THE VIRTUAL CURRENCY REGULATION REVIEW

SECOND EDITION

Editors
Michael S Sackheim and Nathan A Howell

THE LAWREVIEWS

THE VIRTUAL CURRENCY REGULATION REVIEW

SECOND EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in September 2019
For further information please contact Nick.Barette@thelawreviews.co.uk

Editors
Michael S Sackheim and Nathan A Howell

THE LAWREVIEWS

PUBLISHER
Tom Barnes

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGER
Joel Woods

SENIOR ACCOUNT MANAGERS
Pere Aspinall, Jack Bagnall

ACCOUNT MANAGERS
Olivia Budd, Katie Hodgetts, Reece Whelan

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Tommy Lawson

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Tessa Brummitt

SUBEDITOR
Neil Fanning

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC2A 4HL, UK

www.TheLawReviews.co.uk

ISBN 978-1-83862-055-4

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

© 2019 Law Business Research Ltd

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ALLEN & GLEDHILL LLP

AMERELLER

ANDERSON MORI & TOMOTSUNE

ARTHUR COX

BECH-BRUUN

BRANDL & TALOS RECHTSANWÄLTE GMBH

CLIFFORD CHANCE LLP

DENTONS

GERNANDT & DANIELSSON ADVOKATBYRÅ

GTG ADVOCATES

HARNEYS

HENGELER MUELLER PARTNERSCHAFT VON RECHTSANWÄLTEN MBB

JONES DAY

KIM & CHANG

KRAMER LEVIN NAFTALIS & FRANKEL LLP

MARVAL, O'FARRELL & MAIRAL

MVR LEGAL BV

NISHITH DESAI ASSOCIATES

PINHEIRO NETO ADVOGADOS

RUSSELL MCVEAGH

SCHELLENBERG WITTMER LTD

SCHILTZ & SCHILTZ SA

SCHJØDT

SIDLEY AUSTIN LLP

STIKEMAN ELLIOTT LLP

TFH RUSSIA LLC

URÍA MENÉNDEZ

WEBB HENDERSON

CONTENTS

PREFACE

We are pleased to introduce the second edition of *The Virtual Currency Regulation Review* (the *Review*). The increased acceptance and use of virtual currencies by businesses and the exponential growth of investment opportunities for speculators marked late 2018 and early 2019. As examples, in May 2019, it was reported that several of the largest global banks were developing a digital cash equivalent of central bank-backed currencies that would be operated via blockchain technology, and that Facebook was developing its own virtual currency pegged to the US dollar to be used to make payments by people without bank accounts and for currency conversions.

The *Review* is a country-by-country analysis of developing regulatory initiatives aimed at fostering innovation, while at the same time protecting the public and mitigating systemic risk concerning trading and transacting in virtual currencies. On 28 May 2019, the International Organizations of Securities Commissions (IOSCO) published a report titled 'Issues, Risks and Regulatory Considerations Relating to Cryptoassets'. This report provided guidance on the unique issues concerning overseeing cryptoasset trading platforms that provide onboarding, clearing, settlement, custody, market making and advisory services for investors under the umbrella of a single venue. IOSCO advised global regulators of these platforms that their goals should be to ensure that investors are protected, fraud and manipulation are prevented, cryptoassets are sold in a fair way and systemic risk is reduced – the same goals that apply to securities regulation. IOSCO also advised that national regulators should share information, monitor market abuse, take enforcement actions against cryptoasset trading platforms when appropriate and ensure that these venues are resilient to cyberattacks. In the United States, the US Securities and Exchange Commission has not yet approved public offerings of virtual currency exchange-traded funds. The US Commodity Futures Trading Commission (CFTC) has approved of virtual currency futures trading on regulated exchanges and the trading of virtual currency swaps on regulated swap executed facilities. US regulators remain concerned about potential abuses and manipulative activity concerning virtual currencies, including the proliferation of fraudulent virtual currency Ponzi schemes. In May 2019, the US Financial Crimes Enforcement Network issued guidance concerning the application of bank secrecy laws relating to financial institutions with respect to identifying and reporting suspicious activities by criminals and other bad actors who exploit convertible virtual currencies (virtual currencies whose values can be substituted for fiat currencies) for illicit purposes. The CFTC also issued an alert offering potential whistle-blower rewards to members of the public who report virtual currency fraud or manipulation to the CFTC.

Fortunes have been made and lost in the trading of virtual currencies since Satoshi Nakamoto published a white paper in 2008 describing what he referred to as a system for peer-to-peer payments, using a public decentralised ledger known as a blockchain and

cryptography as a source of trust to verify transactions. That paper, released in the dark days of a growing global financial market crisis, laid the foundations for Bitcoin, which would become operational in early 2009. Satoshi has never been identified, but his white paper represented a watershed moment in the evolution of virtual currency. Bitcoin was an obscure asset in 2009, but it is far from obscure today, and there are now many other virtual currencies and related assets. In 2013, a new type of blockchain that came to be known as Ethereum was proposed. Ethereum's native virtual currency, Ether, went live in 2015 and opened up a new phase in the evolution of virtual currency. Ethereum provided a broader platform, or protocol, for the development of all sorts of other virtual currencies and related assets.

Whether virtual currencies will be widely and consistently in commercial use remains uncertain. However, the virtual currency revolution has now come far enough and has endured a sufficient number of potentially fatal events that we are confident virtual currency in some form is here to stay. Virtual currencies and the blockchain and other distributed ledger technology on which they are based are real, and are being deployed right now in many markets and for many purposes. These technologies are being put in place in the real world, and we as lawyers must now endeavour to understand what that means for our clients.

Virtual currencies are essentially borderless: they exist on global and interconnected computer systems. They are generally decentralised, meaning that the records relating to a virtual currency and transactions therein may be maintained in a number of separate jurisdictions simultaneously. The borderless nature of this technology was the core inspiration for the *Review*. As practitioners, we cannot afford to focus solely on our own jurisdictional silos. For example, a US banking lawyer advising clients on matters related to virtual currency must not only have a working understanding of US securities and derivatives regulation; he or she must also have a broad view of the regulatory treatment of virtual currency in other major commercial jurisdictions.

Global regulators have taken a range of approaches to responding to virtual currencies. Some regulators have attempted to stamp out the use of virtual currencies out of a fear that virtual currencies such as Bitcoin allow capital to flow freely and without the usual checks that are designed to prevent money laundering and the illicit use of funds. Others have attempted to write specific laws and regulations tailored to virtual currencies. Still others – the United States included – have attempted to apply legacy regulatory structures to virtual currencies. Those regulatory structures attempt what is essentially 'regulation by analogy'. For example, a virtual currency, which is not a fiat currency, may be regulated in the same manner as money, or in the same manner as a security or commodity. We make one general observation at the outset: there is no consistency across jurisdictions in their approach to regulating virtual currencies. That is, there is currently no widely accepted global regulatory standard. That is what makes a publication such as the *Review* both so interesting and so challenging to assemble.

The lack of global standards has led to a great deal of regulatory arbitrage, as virtual currency innovators shop for jurisdictions with optimally calibrated regulatory structures that provide an acceptable amount of legal certainty. While some market participants are interested in finding the jurisdiction with the lightest touch (or no touch), most legitimate actors are not attempting to flee from regulation entirely. They appreciate that regulation is necessary to allow virtual currencies to achieve their potential, but they do need regulatory systems with an appropriate balance and a high degree of clarity. The technology underlying virtual currencies is complex enough without adding layers of regulatory complexity into the mix.

It is perhaps ironic that the principal source of strength of virtual currencies – decentralisation – is the same characteristic that the regulators themselves seem to be displaying. There is no central authority over virtual currencies, either within and across jurisdictions, and each regulator takes an approach that seems appropriate to that regulator based on its own narrow view of the markets and legacy regulations. We believe optimal regulatory structures will emerge and converge over time. Ultimately, the borderless nature of these markets allows market participants to 'vote with their feet', and they will gravitate toward jurisdictions that achieve the right regulatory balance of encouraging innovation and protecting the public and the financial system. It is much easier to do this in a primarily electronic and computerised business than it would be in a bricks-and-mortar business. Computer servers are relatively easy to relocate; factories and workers are less so.

The second edition of the *Review* provides a practical analysis of recent legal and regulatory changes and developments, and of their effects, and looks forward to expected trends in the area of virtual currencies on a country-by-country basis. It is not intended to be an exhaustive guide to the regulation of virtual currencies globally or in any of the included jurisdictions. Instead, for each jurisdiction, the authors have endeavoured to provide a sufficient overview for the reader to understand the current legal and regulatory environment.

Virtual currency is the broad term that is used in the *Review* to refer to Bitcoin, Ether, tethers and other stablecoins, cryptocurrencies, altcoins, ERC20 tokens, digital, virtual and cryptoassets, and other digital and virtual tokens and coins, including coins issued in initial coin offerings. We recognise that in many instances the term virtual currency will not be appropriate, and other related terms are used throughout as needed. In the law, the words we use matter a great deal, so, where necessary, the authors of each chapter provide clarity around the terminology used in their jurisdiction and the legal meaning given to that terminology.

Based on feedback on the first edition of the *Review* from members of the legal community throughout the world, we are confident that attorneys will find the updated second edition to be an excellent resource in their own practices. We are still in the early days of the virtual currency revolution, but it does not appear to be a passing fad. The many lawyers involved in this treatise have endeavoured to provide as much useful information as practicable concerning the global regulation of virtual currencies.

The editors would like to extend special thanks to Ivet Bell (New York) and Dan Applebaum (Chicago), both Sidley Austin LLP associates, for their invaluable assistance in organising and editing the second edition of the *Review*, and particularly the United States chapter.

Michael S Sackheim and Nathan A Howell
Sidley Austin LLP
New York and Chicago
August 2019

Chapter 1

ARGENTINA

Juan M Diehl Moreno[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

Argentina is a regional leader in the adoption of cryptocurrencies, and is still making in-roads in this regard. As a result of economic instability and foreign exchange restrictions, Argentina became one of the earliest adopters of cryptocurrency in Latin America (and the world) in an effort to protect its savings against inflation and to overcome the prohibition on purchasing and transferring foreign currency abroad.

Cryptocurrencies are not prohibited in Argentina, and are therefore legal. Nevertheless, the government has issued regulations regarding cryptocurrencies related to taxation and the prevention of money laundering and the financing of terrorism.

The government has not implemented specific regulations on the issuance, exchange or, in general, use of cryptocurrencies, instead choosing to observe ongoing developments regarding the impact of cryptocurrencies in the Argentine market.

II SECURITIES AND INVESTMENT LAWS

There is no specific regulation applicable to the sale of cryptocurrencies or other tokens under securities laws or investment laws in Argentina.

Given the lack of a central issuing authority, Bitcoins cannot be classified as securities. Under Argentine law, securities are essentially negotiable instruments into which their issuers incorporate credit rights. Nevertheless, this conclusion may not be extended to other cryptocurrencies (tokens) issued by a centralised entity.

Following the example of securities and exchange commissions in other parts of the world, the National Securities Commission (CNV) issued a communiqué on initial coin offerings (ICOs) to warn investors of their potential risks.

The CNV has clarified that ICOs would not, in principle, be subject to regulations regarding the capital markets. Nevertheless, it has also stated that, depending on their structure and particular characteristics, certain ICOs may be subject to the control of the CNV.

The communiqué further warns investors about the following potential risks associated with ICOs:

a a lack of specific regulations;
b price volatility and liquidity risks;
c the probability of fraud;

1 Juan M Diehl Moreno is a partner at Marval, O'Farrell & Mairal.

d inadequate access to relevant information;
e the early stage of projects;
f the probability of technological and infrastructure failures; and
g the transnational nature of transactions involving ICOs.

Although the CNV states that ICOs are not, in principle, subject to specific CNV control, the communiqué clarifies that claims may be filed with the CNV in cases where there is a suspicion that an ICO could be fraudulent.

Although there are no specific prohibitions, given the current lack of certainty in connection with the possibility of considering certain cryptocurrencies as securities under the Capital Markets Law (CML),[2] regulated entities subject to the CNV's control, such as investment managers, investment advisers and fund managers, tend not to operate with such assets.

Additionally, the formal requirements for the operational activities of such players have not been designed to address cryptocurrencies. Thus, several regulations may act as practical restrictions that hinder the possibility of operating with such digital assets.

III BANKING AND MONEY TRANSMISSION

In Argentina, cryptocurrencies like Bitcoin are defined by the Financial Information Unit (UIF) as a 'digital representation of value that can be digitally traded and functions as a medium of exchange; and/or a unit of account; and/or a store of value, but does not have legal tender status in any jurisdiction and is neither issued nor guaranteed by any government or jurisdiction'.

The Argentine Civil and Commercial Code (the Civil Code) determines that individuals and legal entities are entitled to all the corresponding rights over the assets that are part of their property. In this regard, the Civil Code classifies assets into two categories: tangible and intangible.

As opposed to those that have a physical entity, intangible assets such as intellectual property and, in general, rights do not materialise in the physical sphere. Thus, as a digital representation of value, cryptocurrencies are intangible assets that are able to form part of individuals' and legal entities' property.

Section 765 of the Civil Code determines that only the Argentine fiat currency can be considered as money, thus excluding any possibility of including cryptocurrencies in such category.

In connection to the possibility of considering cryptocurrencies as currency under Argentine law, Section 30 of the Argentine Central Bank's Charter[3] provides a definition that excludes any type of instrument that has no legal tender directly or indirectly imposed by its issuer, or that is not issued with a nominal value lower than 10 times the amount of the highest national money bill in circulation. As such, to date this provision excludes the possibility of considering several cryptocurrencies as currency under Argentine law. Moreover, extensive interpretations of Section 30 of the Charter are prohibited.

In this regard, in May 2014 the Central Bank issued a non-binding press release stating that virtual currencies are not issued by itself or any other international monetary authority,

2 Law No. 26,831.
3 Law No. 24.144.

and thus are not legal tender and are not guaranteed by any government. Nevertheless, there have not yet been any local precedents or governmental decisions or communications in connection with any cryptocurrency issued by foreign authorities.

The UIF differentiates between virtual currency and electronic currency, stating that the latter involves the electronic transfer of legal tender, while virtual currency transactions do not involve legal tender.

IV ANTI-MONEY LAUNDERING

For the time being, the only specific regulations related to cryptocurrencies in Argentina are UIF Resolution 300/2014 (the UIF Resolution), which implements additional reporting obligations for certain obliged subjects (see below) under the Anti-Money Laundering Law (the AML Law)[4] (see Section V) and the Tax Reform Law[5] (see Section IV).

The AML Law lists a number of persons, including financial entities, broker-dealers, credit card companies, insurance companies, public notaries, and certain government registries and agencies, that have, among other things, specific reporting obligations under the AML Law (obliged subjects), and provides for certain general obligations including applying know your customer (KYC) procedures; reporting to the UIF any transaction suspected of money laundering or terrorism financing; and abstaining from disclosing to their clients or third parties activities performed in compliance with that statute.

As explained above, one of the few regulations on cryptocurrencies in Argentina is the UIF Resolution, which requires most obliged subjects under the AML Law to report all the transactions performed with cryptocurrencies, regardless of their amount.

Following the Financial Action Task Force's guidelines, the UIF also warns obliged subjects about the risks involved in transactions using cryptocurrencies. In so doing, the UIF also requires obliged subjects listed in the UIF Resolution to monitor strictly any transactions performed with cryptocurrencies by their clients.

V REGULATION OF EXCHANGES

There are currently no specific regulations on exchange activities. However, anyone wanting to publicly offer securities within the Argentine territory needs to request a public offering authorisation from the CNV.

The trading of securities requires a licence from the CNV. Therefore, the exchange of cryptocurrencies as a permanent activity will require a licence if the cryptocurrency being exchanged is a security.

As previously mentioned, considering the lack of a central issuing authority, cryptocurrencies like Bitcoin cannot be classified as securities. Nevertheless, this conclusion may not be extended to other cryptocurrencies (tokens) issued by a centralised entity.

4 Law No. 25,246.

5 Law No. 27,430.

VI REGULATION OF MINERS

The mining of Bitcoin and other cryptocurrencies is permitted. There are currently no specific regulations regarding such activity.

VII REGULATION OF ISSUERS AND SPONSORS

There are currently no specific regulations on issuers and sponsors. See Section III.

VIII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

There are currently no specific criminal or civil fraud regulations regarding the exchange or issuance of cryptocurrencies; therefore, either the general criminal and civil law should apply, depending on the specific case at stake.

IX TAX

Among the amendments introduced by the Tax Reform Law, the taxable income derived from the commercialisation of digital currencies was incorporated into the Income Tax Law (ITL). One of the main objectives of the tax reform was to tax financial income.

Neither the Tax Reform Law nor the ITL provide a definition of digital currencies, or the scope that this concept comprises. The corresponding regulations of the Tax Reform Law have not been issued yet. We understand that the meaning of this concept should be the same as that applied to virtual currencies as defined by the UIF Resolution, and therefore this Resolution should apply to cryptocurrencies.

The ITL also determines that if an issuer of cryptocurrencies is domiciled in Argentina, then Argentine-sourced income would be generated as a consequence of the exchange thereof. As such, the profit derived from the sale of cryptocurrencies will be considered income and taxed as such at 15 per cent when derived from either Argentine or foreign sources.

Provided that cryptocurrencies fall within the definition of intangible assets, the exchange of cryptocurrencies should not be impacted by value added tax.

In general, and in addition to the aforementioned examples, cryptocurrencies will be taxed like any other intangible asset.

X OTHER ISSUES

There are no border restrictions or obligations to declare cryptocurrency holdings in Argentina.

There are no reporting requirements for cryptocurrency payments made in excess of a certain value. Currently, the only specific reporting requirements in connection with cryptocurrencies are regulated by the UIF Resolution (see Section V) and the Tax Reform Law (see Section IV).

Cryptocurrencies must be treated as intangible assets for the purposes of estate planning and testamentary succession. This may potentially change in the future in connection with tokens issued through ICOs, subject to the CNV's view on their legal nature under the CML.

For corporate purposes, cryptocurrencies may be contributed as capital of an Argentine entity. However, as a contribution in kind, these cryptocurrencies must be appraised in advance. The type and requirements of the appraisal will depend on the type of entity receiving the capital contribution.

On 11 March 2019, the Argentine Executive Branch issued Decree No. 182/2019 (the Decree) regulating the Digital Signature Law No. 25,506 (DSL).The Decree created the figure of the 'trusted third-party service provider'. This figure includes the operation of distributed ledger technologies for the preservation of electronic documents, management of smart contracts and other digital services.

Moreover, these services also include the electronic certification, digital identification and other services detailed by the licensing entity established by the DSL. Individuals, legal entities, consortiums, public entities and non-state public entities may be trusted third-party service providers under the Decree.

The Decree has not been further regulated yet. Hence, specific guidelines in relation to the use of distributed ledger technology by trusted third-party service providers are still pending.

XI LOOKING AHEAD

The continuous development of new technologies gives rise to several economic, legal and financial problems. In this sense, the international community's receptiveness to cryptocurrencies has raised important concerns, and has therefore required different legislation to analyse and study the issue.

In Argentina, the issue is not yet fully developed, and only the Argentine Central Bank and the UIF have issued opinions on the matter. The regulatory authorities have adopted a wait-and-see strategy in connection with cryptocurrencies.

The definition of cryptocurrencies will, without doubt, impact the decision as to whether or not the current legislation in Argentina applies to transactions in which cryptocurrencies are used.

There are currently no sandbox or other programmes intended to promote research and investment in cryptocurrencies. Nevertheless, the Argentine Central Bank has created several research groups, among which there is a group specifically dedicated to cryptocurrencies and blockchain technologies composed of members of both public and private entities with the aim of analysing potential regulatory modifications to enable the use of new technologies within the financial services industry.

Despite the expectations regarding the meeting of finance ministers and central bank governors of the G20 countries in Buenos Aires in March 2018, no regulatory framework or specific guidelines on cryptocurrencies were issued. Discussions mentioned them, providing alerts as to their risks for consumers and investors, but nothing was discussed as to the way cryptocurrencies should be approached by the authorities, except for a call upon international standard-setting bodies to monitor cryptocurrencies and their risks while evaluating a multilateral response, if appropriate.

The government's plan is to regulate transactions with Bitcoins by amending the AML Law to include stock markets, wallets and brokers as entities required to report certain transactions with cryptocurrencies to official entities. Obligations to be complied with would include KYC procedures, the monitoring and reporting of suspicious transactions and the appointment of a compliance officer in charge of implementing due diligence.

Chapter 2

AUSTRALIA

Ara Margossian, Marcus Bagnall, Ritam Mitra and Irene Halforty[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

i Overview

Distributed ledger technologies (DLTs) are regulated in Australia under a range of laws. Like many other jurisdictions, Australian regulators are taking a keen interest in DLTs, and have been reasonably active in seeking to understand how emerging developments in this space will impact existing business models and regulatory frameworks. To date, Australian regulators have largely attempted to address DLT developments through existing frameworks, which they have sought to incrementally adapt and augment through a combination of regulatory guidance notes and targeted changes.

Although the level of token generation events (TGEs) has come off the highs experienced in 2017 to 2018, we expect that the legal and regulatory landscape in Australia will evolve incrementally as DLT-use cases continue to proliferate, and policymakers and regulators seek to establish more sophisticated approaches to addressing the impact of DLTs.

In this chapter, we focus on the legal and regulatory framework that impacts virtual currencies and TGEs.

ii Regulation

The Australian Securities and Investments Commission (ASIC) is Australia's corporate regulator, with broad powers under the Corporations Act relating to providing financial products and a range of fundraising activities that may impact TGEs.[2]

The Australian Transaction Reports and Analysis Centre (AUSTRAC) is Australia's principal anti-money laundering and counter-terrorism financing (AML/CTF) regulator. The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (the AML/CTF Act) subjects digital currency exchanges (DCEs) to mandatory registration and reporting obligations.

Self-regulation

Australia's regulatory environment is also supported by industry self-regulation including by the Australian Digital Commerce Association (ADCA), the industry body representing businesses using blockchain technology that maintains the voluntary Digital Currency Industry Code of Conduct (DCI Code).

---

1 Ara Margossian is a partner, Marcus Bagnall is a senior associate, and Ritam Mitra and Irene Halforty are lawyers at Webb Henderson.

2 Corporations Act 2001 (Cth) (Corporations Act), Chapter 6 and Chapter 7.

iii Taxation

The Australian Taxation Office (ATO) is the principal Australian revenue collection agency responsible for administering Australia's federal taxation system. The ATO has issued guidance regarding how virtual currency and ICO token events, including acquisitions and disposals, are treated from a taxation perspective.

iv Consumer protection

Australian law prohibits various forms of misleading and deceptive conduct. ASIC has powers to investigate and prosecute TGE issuers, sponsors or advisers engaging in misleading and deceptive conduct in breach of the Australian Consumer Law (ACL).[3]

II SECURITIES AND INVESTMENT LAWS

The Corporations Act, Australia's main securities legislation, operates on a technology-neutral basis and has not been changed to specifically accommodate (or prohibit) virtual currencies and TGEs.[4] Instead of establishing a clear regulatory perimeter for virtual currencies or TGEs, ASIC has provided guidance on how existing securities legislation could apply to cryptoassets and TGEs based on their accompanying features and rights.[5] It also warns entities that they could be required to justify to ASIC a conclusion that their virtual currency or TGE does not constitute a financial product, or that an exemption applies to requiring an Australian Financial Services (AFS) licence.[6]

As each virtual currency or TGE is different, its regulatory treatment depends on its structure and the rights attached to it. The fact that a token is described as a virtual currency or utility token does not mean it falls outside regulation under the Corporations Act (e.g., as a financial product) or is not subject to its provisions (e.g., in relation to misleading and deceptive conduct).

Chapters 6D and 7 of the Corporations Act, which regulate fundraising and financial services markets respectively, are the main aspects of the Corporations Act that could potentially apply to virtual currencies and TGEs. The obligations apply also to foreign financial services providers carrying on business in Australia.

i Regulation as a financial product

Whether a virtual currency or TGE is caught by Chapter 7 turns principally on whether it is a financial product.[7] Although ASIC does not consider Bitcoin is a financial product,[8] whether any other virtual currency or TGE constitutes a financial product requires analysing its structure and rights, which can be a challenging process given that emerging use cases often do not fit neatly into traditional categories.

3 On 19 April 2018, ASIC received delegated powers from the ACCC to take action under the ACL relating to cryptoassets and ICOs, regardless of whether it involves a financial product.

4 ASIC Information Sheet 219: Evaluating distributed ledger technology.

5 ASIC Information Sheet 225: Initial coin offerings and crypto-assets (INFO 225).

6 ibid.

7 See Corporations Act Chapter 7, Part 7.1 Division 3.

8 Australian Securities Investments Commission, 'Senate inquiry into digital currency, Submission by the Australian Securities and Investments Commission', December 2014.

Based on recent ASIC guidance, the following are examples of a virtual currency or TGE that may be a financial product:

a it has the characteristics of a security, such as linking to an underlying asset granting rights to voting, dividends or distribution of capital in a body corporate;

b it may be used as a payment method that makes it a non-cash payment facility;

c where DCE transactions do not settle immediately, or the price or a requirement to provide consideration is derived from another asset or index, in a way that makes it a derivative;

d it allows money to be exchanged for tokens and pools contributions to provide financial benefits to token holders, making it a managed investment scheme; or

e entities that are currently licensed to provide financial services or a financial market in respect of a financial product expand their offering to incorporate a virtual currency or TGE.

ii Financial markets

Where a virtual currency or TGE is a financial product, any platform enabling consumers to buy or sell the virtual currency or TGE may constitute a financial market, as described in further detail in Section V. As at 19 June 2019, there were no licensed or exempt platform operators of virtual currency or TGE financial products in Australia.[9]

iii Regulation of managed investment schemes

A managed investment scheme (MIS), also known as pooled or collective investments, is a type of Australian investment scheme where pooled contributions produce financial benefits for scheme members.[10] An MIS must be registered, and cannot be operated unless it is registered, if it meets certain criteria (e.g., it has more than 20 members).[11]

Rights granted to token holders described in white papers and offer documents can potentially constitute an MIS. This is particularly the case where issuers seek to tokenise certain assets or create exposure to a certain asset class or trading activity, such as a venture capital (VC) fund or hedge fund, through issuing a bundle of rights using a blockchain.

In recent regulatory guidance, ASIC states that the rights granted to token holders should be interpreted broadly, such that if the rights and value of the cryptoasset is affected by the pooling of funds from contributors, or the use of those funds under the arrangement, then the arrangement is likely to be an MIS, particularly if the arrangement is offered as an investment.[12]

This follows ASIC's investigation in May 2018 of Neds, an Australian wagering and betting start-up company, proposed to issue NedsCoins, which could be used to place bets on the Neds platform and entitled token holders to receive dividends of 0.25 per cent of the company's quarterly turnover. ASIC investigated the offer and determined that, in addition

9 ASIC Information Sheet 225: Initial coin offerings and crypto-assets (INFO 225).

10 Corporations Act, Section 9.

11 ibid., Section 601ED. Note that an MIS does not need to be registered if all interests issued would not have required a product disclosure statement (PDS) had the scheme been registered.

12 For more information on requirements, see: ASIC Regulatory Guide 133, Funds management and custodial services: Holding assets, July 2018, available at: https://download.asic.gov.au/media/4832070/rg133-published-31-july-2018.pdf.

to potentially misleading statements in the white paper, the offer was an unregulated MIS. Neds, along with other issuers, subsequently halted their ICO and indicated they would make structural changes.[13]

iv Virtual currency and non-cash payment facilities

A non-cash payment (NCP) is a payment made without physically delivering Australian or foreign currency, made through an NCP facility.[14] In May 2018, ASIC stated that a virtual currency or ICO token itself is unlikely to be an NCP facility.[15] However, a virtual currency or TGE may be an NCP facility in certain circumstances,[16] unless an existing exemption applies or ASIC grants relief from the operation of these provisions.[17]

v Fundraising provisions

If a virtual currency or TGE gives token holders rights that are equivalent to a security (e.g., a share) then the disclosure requirements in Chapter 6D will apply to such token offers. For example, tokens giving token holders the right to vote in decisions of the issuer and receive dividends proportionate to their token holdings. Exemption from disclosure is available in certain circumstances, such as for small-scale offerings, or offers to sophisticated investors or through financial services licensees.[18]

III BANKING AND MONEY TRANSMISSION

Virtual currencies and cryptoassets are not currently regulated in Australia as legal tender or money.

The Reserve Bank of Australia (RBA), Australia's principal payments system regulator, has stated that it does not consider virtual currencies to be part of the Australian payments system because:[19]

a they are not widely accepted or used as a payment method;

13 ASIC media release 18-122MR: ASIC takes action on misleading or deceptive conduct in ICOs, https:// asic.gov.au/about-asic/media-centre/find-a-media-release/2018-releases/18-122mr-asic-tak es-action-on- misleading-or-deceptive-conduct-in-icos; Jacobs, S 'ASIC is taking aim at dodgy ICOs as it issues a warning to the sector', Business Insider Australia, 1 May 2018.

14 Corporations Act, Section 763D(1). Examples include the direct debit of a deposit account, gift vouchers or cards, prepaid mobile phone accounts and loyalty schemes.

15 ASIC Information Sheet 225: Initial coin offerings and crypto-assets (INFO 225).

16 Cryptoassets may involve an NCP facility if it includes an arrangement that allows payments of value to be made using a cryptoasset to a number of payees, or allows payments to be made using the cryptoasset and which is then converted to fiat currency to enable the completion of the payment. For more information see: ASIC Information Sheet 225: Initial coin offerings and crypto-assets (INFO 225).

17 For the type of relief that ASIC may order with respect to an individual or class of products or arrangements, see ASIC Regulatory Guide 185: Non-cash payment facilities, RG 185.9. At the time of writing, ASIC has not granted class order relief or declared any virtual currencies or ICO tokens as exempt from Chapter 7 of the Corporations Act.

18 Corporations Act, Section 708.

19 The payments system in Australia refers to arrangements that allow funds transfers between accounts, typically held in financial institutions, through instruments such as cash, credit cards and cheques, and through electronic funds transfer.

b they are not an effective store of value due to large fluctuations and strong speculative influences; and

c they are not commonly used as a unit of account: goods and services in Australia continue to be priced overwhelmingly in Australian dollars.

At the time of writing, linkages in Australia between virtual currencies and the broader financial system remain limited,[20] underlined by financial institutions continuing to take steps to avoid dealing with virtual currencies and intermediaries.[21] The RBA consequently has limited concerns regarding virtual currencies with respect to competition, efficiency or risk to the financial system warranting urgent regulatory intervention, despite token valuation losses occurring.[22]

The RBA has indicated that it does not plan to issue an 'eAUD', and that regulatory intervention can be expected to mitigate any payments system stability risks once virtual currencies mature beyond 'speculative mania' to become an efficient or widely used payment method.[23]

IV ANTI-MONEY LAUNDERING

The concern that virtual currencies may be used by criminals seeking a low-detection risk method to transfer funds has played a prominent role in shaping the initial response of Australia's lawmakers to the growth of virtual currencies.[24]

This has culminated in strengthened AML/CTF measures to safeguard the ability of regulators such as AUSTRAC and law enforcement agencies to detect criminals who would otherwise desire to manipulate the financial sector to obfuscate illegal transactions and funding sources. In accordance with the approach adopted in other advanced economies, the Australian government has sought to focus regulation on DCEs as the primary entry and exit points between the payment systems supporting virtual currencies and fiat currencies.

i Application to digital currency exchanges

The AML/CTF Act regulates DCE services and other digital currency-related services as a designated service; and establishes mandatory registration and reporting obligations on registrable DCE operators.

The AML/CTF Act will only apply to entities that provide services related to digital currencies, which is defined as a digital representation of value that:

a is not issued by or under the authority of a government;

b functions as a medium of exchange, a store of economic value or a unit of account;

20 RBA media release: Payment Systems Board Update: 23 February 2018, https://www.rba.gov.au/media-releases/2018/mr-18-04.html.

21 RBA speech: Cryptocurrencies and distributed ledger technology, Tony Richards, Head of Payments Policy Department, Sydney 26 June 2018, http://www.rba.gov.au/speeches/2018/pdf/sp-so-2018-06-26.pdf, p11.

22 RBA, Submission 19, p. 9; Dr Anthony Richards, Reserve Bank of Australia, Committee Hansard, 7 April 2015, p. 45.

23 RBA Address to 2017 Australian Payment Summit, Governor Philip Lowe, Sydney 13 December 2017 https://www.rba.gov.au/speeches/2017/sp-gov-2017-12-13.html.

24 AUSTRAC typologies and case studies report 2012, http://www.austrac.gov.au/sites/default/files/documents/typ_rprt12_full.pdf.

c is interchangeable with fiat money, and may be used as consideration for the supply of goods or services; and

d is generally available to members of the public without any restriction on its use as a form of consideration.[25]

ii Compliance obligations

The AML/CTF Act applies to reporting entities that provide designated services within Australia or that otherwise have a predefined link to Australia.[26] Reporting entities must meet know-your-customer obligations to properly identify customers before providing DCE services, meet reporting and record-keeping obligations and have an AML/CTF compliance programme.[27]

Reporting obligations require DCEs to submit to regular reporting to AUSTRAC regarding suspicious transactions or transactions above a threshold amount.[28] These measures acknowledge the increasing role played by DCEs to assist the intelligence-gathering efforts of regulatory and law enforcement agencies.

V REGULATION OF EXCHANGES

DCEs are the main touch point between virtual currencies and traditional fiat-based payment systems. There are a growing number of DCEs either in Australia or located outside Australia offering markets in Australian dollars.

The regulatory regimes impacting DCEs operating in Australia include mandatory registration, reporting and compliance obligations under the AML/CTF Act; and potential requirements to obtain and maintain a licence to offer a financial service or financial market under the Corporations Act, depending on whether the DCE operator is offering a financial product: see Section II.

i AML/CTF requirements

A DCE operator that is a reporting entity providing a designated service must comply with the reporting entity obligations under the AML/CTF Act: see Section IV.

All registrable DCE operators must enrol and register with AUSTRAC on the Digital Currency Exchange Register (DCE Register) before providing DCE services, and must renew their registration every three years.[29] While AUSTRAC does not currently publish the DCE Register, several Australian DCE operators have announced their successful registration with AUSTRAC to demonstrate their regulatory compliance to the market. AUSTRAC may also publish the names of persons whose DCE registration has been cancelled.[30]

25 The AML/CTF Act does, however, provide for methods for certain activities to be declared through the rules made under ibid., Section 229. See, for example, the definition of stored value card: ibid., Section 5.

26 ibid., Section 6.

27 ibid., Parts 2, 3, 4, 7 and 10.

28 ibid., Part 3. At the time of writing, the reportable transaction threshold is A$10,000.

29 ibid., Section 76A. It is an offence for a registrable DCE operator to provide DCE services without being registered on the DCE Register: ibid., Section 76A(3). AUSTRAC can also refuse, suspend or cancel a registration on certain grounds, such as where the DCE poses an unacceptable money laundering, terrorism financing or other serious crime risk: ibid., Part 6A Division 3.

30 ibid., Section 76J(4).

ii Licensing requirements

An entity must obtain a licence to authorise any financial services or financial markets offered or provided in relation to financial products. ASIC has indicated the following DCE-related activities are not financial products, financial services or financial markets requiring a licence:

a the immediate exchange and settlement of virtual currency transactions and operating a DCE;
b software that facilitates virtual currency transfers between wallets;
c virtual currency automated teller machines; and
d escrow facilities supporting DCEs.

At the time of writing, no major Australian DCE operator has obtained an AFS licence for their DCE activities. However, DCE operators will need an AFS if their exchange lists a cryptoasset that is a financial product or for other activities involving a financial product. For example, CoinJar, in addition to providing DCE services, provides CoinJar Swipe, which is an electronic funds transfer at point of sale (EFTPOS) card allowing consumers to convert virtual currency to Australian dollars to make purchases at EFTPOS terminals in Australia. The CoinJar Swipe product is a financial product issued under an AFS licence,[31] which is distinct from the DCE services offered by CoinJar.

VI REGULATION OF MINERS

See Section IX for information on how mining activities are treated under taxation legislation.

No obligations otherwise apply specifically to miners, other than the general obligations described throughout this chapter.

VII REGULATION OF ISSUERS AND SPONSORS

See Section II regarding the application of the Corporations Act to virtual currency and ICO token issuers and sponsors.

See Section VIII regarding virtual currency and ICO token issuer and sponsor consumer protection obligations for issues such as making market representations.

VIII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

Several laws regulate enforcement activities relating to the marketing and selling of virtual currencies and ICO and STO tokens in Australia. Regulators' investigative and enforcement powers include seeking substantial civil, and in some cases criminal, penalties for breaches.

The main regulatory focus is currently on TGEs, pursuant to which issuers, advisers and promoters alike can be held liable for engaging in illegal conduct. Separately, AUSTRAC is focusing on registration and reporting compliance obligations for DCEs, as described in Section V.

31 Emerchants eftpos prepaid debit card PDS: https://s3-ap-southeast-2.amazonaws.com/coinjar-assets/swipe/eftpos-pos-20160101.pdf.

i Misleading and deceptive conduct

Under Australian law, misleading or deceptive conduct is prohibited in the course of business[32] and under the securities law in connection with financial services and in relation to financial products.[33] In May 2018, ASIC announced it would issue inquiries to ICO issuers and advisers where it identifies conduct or statements that may be misleading or deceptive, noting that 'regardless of the structure of the ICO, there is one law that will always apply: you cannot make misleading or deceptive statements about the product. This will be a key focus for us as this sector develops'.[34]

ASIC has also issued guidance noting specific examples of potentially misleading and deceptive conduct for ICOs, which would likely extend to TGEs generally:[35]

a falsely stating or conveying the impression that the TGE or underlying token is a financial product;

b falsely stating or conveying the impression that a cryptoasset trading platform does not quote or trade financial products;

c using social media to artificially inflate public interest in a TGE;

d undertaking or arranging for a group to engage in trading strategies to generate the appearance of greater buying and selling activity levels for a virtual currency or ICO or STO token;

e failing to disclose adequate information about a TGE; or

f suggesting that a TGE is a regulated product or that the regulator has approved a TGE, if that is not the case.

According to ASIC, the most prevalent legal issues experienced by ICOs are the use of misleading or deceptive statements in marketing, the operation of illegal managed investment schemes, and failing to hold an AFS licence.[36] For example, in one case, ASIC cited fundamental concerns regarding the ICO's structure and overly optimistic business growth forecasts in its white paper disclosure.[37]

Remedies available to consumers, regulators and courts in respect of misleading and deceptive conduct (including for making false or misleading representations) include maximum pecuniary penalties ranging between A$945,000 (for individuals), and the greater of A$10 million, three times the value of the benefit received by the corporation as a result

32 ACL, Section 18.

33 Corporations Act Section 1041H; Australian Securities and Investments Commission Act 2001 (Cth) (the ASIC Act), Section 12DA.

34 ASIC media release 18-122MR: ASIC takes action on misleading or deceptive conduct in ICOs, https://asic.gov.au/about-asic/media-centre/find-a-media-release/2018-releases/18-122mr-asic-takes-action-on-misleading-or-deceptive-conduct-in-icos/.

35 ASIC Information Guide 225: Initial coin offerings and crypto-assets (INFO 225).

36 ASIC media release 18-274MR: ASIC acts against misleading Initial Coin Offerings and crypto-asset funds targeted at retail investors, https://asic.gov.au/about-asic/news-centre/find-a-media-release/2018-releases/18-274mr-asic-acts-against-misleading-initial-coin-offerings-and-crypto-asset-funds-targeted-at-retail-investors/.

37 ASIC Media Release: 18-122MR, ASIC takes action on misleading or deceptive conduct in ICOs, https://asic.gov.au/about-asic/news-centre/find-a-media-release/2018-releases/18-122mr-asic-takes-action-on-misleading-or-deceptive-conduct-in-icos/.

of the conduct, or where the benefit cannot be calculated, 10 per cent of the annual turnover in the preceding 12 months (for corporations) or 10 years' imprisonment,[38] and injunctions (such as an injunction blocking a TGE),[39] compensation for damages and other orders.

ii Product intervention power

From April 2019, ASIC received further powers to make a product intervention order in relation to conduct where a product has, will or is likely to result in significant consumer detriment,[40] which would apply to virtual currencies or TGEs to the extent they are a financial product or a credit product. In its current draft regulatory guide regarding enforcement of its product intervention powers, ASIC indicates that the factors that make significant consumer detriment more likely include:[41]

a the extent and operation of any conflicts of interest;
b the complexity or opacity of the product and circumstances of its sale; and
c how choices and processes are presented to consumers that influence their take-up and use of the product (the choice architecture).

iii Unlicensed financial products and markets

Penalties for breaching the licensing and registration requirements under the Corporations Act include fines of up to A$105,000 or five years' imprisonment for individuals and up to A$525,000 for corporations, depending on the breach.

At the time of writing, there has not been a successful ICO involving a financial product in Australia. ASIC has otherwise successfully acted to prevent a number of ICOs raising capital without the appropriate investor protections, with some of these put on hold or restructured to comply with applicable securities and investments laws.[42] For example, on 13 September 2018, ASIC issued a final stop order on a PDS issued by Investors Exchange Limited for 'units' in the New Dawn Fund. ASIC considered that the New Dawn Fund was an unregulated 'crypto-asset managed investment scheme' as it proposed to invest in a range of cryptocurrency assets on behalf of New Dawn Fund 'unit' owners.[43]

Given the current and growing regulatory and governmental scrutiny of Australia's financial services sector (including ASIC's role), penalties for unlicensed financial products and markets will likely increase.[44]

38 See ACL, Section 224(3); ASIC Act Section 12DB; Corporations Act Schedule 3 Item 310.

39 ACL, Section 232.

40 Corporations Act, Part 7.9A.

41 ASIC draft regulatory guide: Product Intervention Power (attachment to CP 313), June 2019, https://download.asic.gov.au/media/5165180/attachment-to-cp313-published-26-june-2019.pdf.

42 ASIC acts against misleading Coin Offerings and crypto-assets funds targeted at retail investors, 18-247MR, Thursday, 20 September 2018, available at: https://asic.gov.au/about-asic/news-centre/find-a-media-release/2018-releases/18-274mr-asic-acts-against-misleading-initial-coin-offerings-and-crypto-asset-funds-targeted-at-retail-investors/.

43 ASIC acts against misleading Coin Offerings and crypto-assets funds targeted at retail investors, 18-247MR, Thursday, 20 September 2018, available at: https://asic.gov.au/about-asic/news-centre/find-a-media-release/2018-releases/18-274mr-asic-acts-against-misleading-initial-coin-offerings-and-crypto-asset-funds-targeted-at-retail-investors/.

44 See Treasury Department, ASIC Enforcement Review Taskforce Report: https://treasury.gov.au/review/asic-enforcement-review/r2018-282438; Treasury Department, Australian Government response to the ASIC Enforcement Review Taskforce Report, https://treasury.gov.au/publication/p2018-282438.

iv AML/CTF breaches

Failure by a registrable DCE operator to comply with AUSTRAC's registration requirements, including providing unregistered DCE services and breaching registration conditions, can result in up to two years' imprisonment or a A$105,000 fine, or both. The penalty can increase to up to seven years' imprisonment or A$420,000, or both, for repeat offenders and for failing to comply with undertakings.

AUSTRAC has historically sought significant penalties to deter breaches of the laws it administers, and DCE operators should expect the same treatment under the AML/CTF Act. For example, in 2018, the Commonwealth Bank of Australia agreed with AUSTRAC a settlement involving a A$700 million penalty for over 53,000 breaches of the AML/CTF Act, which included failing to comply with its AML/CTF programme in respect of 778,370 bank accounts.

On 8 March 2019, AUSTRAC reiterated that it will continue to monitor compliance with AML/CTF requirements that came into full effect on 2 October 2018.[45] At the time of writing, AUSTRAC's DCE enforcement activities have included 11 investigations, suspending two DCE registrations owing to involvement with organised crime, and refusing two DCE registration applications.[46]

v Taxation

The ATO announced on 30 April 2019 that it will be collecting records from Australian virtual currency service providers and matching them against ATO data to identify taxpayers who are failing to adequately disclose their income details.[47]

According to the National Tax Liaison Group, the ATO's agenda for virtual currencies in 2019 will:

a continue to focus on releasing guidance, with further updates expected in October 2019;

b focus on compliance and engagement activities (including the use of data matching) to promote compliance among virtual currency providers and brokers; and

c strengthen international engagement, in particular with the Joint Chiefs of Global Tax Enforcement (J5).[48]

45 AUSTRAC Media Release, Cybercrime Squad and AUSTRAC remind digital currency exchanges of reporting obligations, http://www.austrac.gov.au/media/media-releases/cybercrime-squad-and-austrac-remind-digital-currency-exchanges-reporting.

46 AUSTRAC, Digital currency exchange provider actions, http://www.austrac.gov.au/enforcement-action/digital-currency-exchange-provider-actions.

47 ATO media release, ATO receives cryptocurrency data to assist tax compliance, https://www.ato.gov.au/Media-centre/Media-releases/ATO-receives-cryptocurrency-data-to-assist-tax-compliance/; see also ATO, Cryptocurrency: 2014–15 to 2019–20 financial years data matching program protocol, https://www.ato.gov.au/General/Gen/Cryptocurrency-2014-15-to-2019-20-financial-years/.

48 Australian Taxation Office: National Tax Liaison Group key messages 4 March 2019, QC58590, https://www.ato.gov.au/General/Consultation/In-detail/Stewardship-groups-minutes/National-Tax-Liaison-Group/National-Tax-Liaison-Group-key-messages-4-March-2019/.

IX TAX

The range of potential structures for virtual currencies and TGEs lends a degree of uncertainty regarding their tax treatment for issuers and holders. The ATO has provided some guidelines and commentary regarding virtual currency treatment under Australia's taxation regime, specifically Bitcoin.[49] The ATO views virtual currencies such as Bitcoin as assets with tax consequences, rather than money or currency. The main tax considerations are:

a income tax;
b capital gains tax;
c goods and services tax (GST); and
d fringe benefits tax.

i Income tax

Australia's income tax regime is principally set out under the Income Tax Assessment Act 1936 (Cth) and the Income Tax Assessment Act 1997 (Cth). If a person carries on a business (e.g., for commercial reasons, in a business-like manner) that involves transacting with virtual currency,[50] any virtual currency held by the business (whether as part of an incorporated entity or not) will likely be treated as trading stock. This means that proceeds from the sale of a virtual currency will be treated as ordinary income and assessed accordingly, while the costs and outgoings of carrying on the business (such as virtual currency mining costs) are deductible.[51]

ii Capital gains tax

The ATO has issued guidance clarifying that capital gains tax may apply where virtual currency is sold or gifted, traded or exchanged, converted to fiat currency, or used to obtain goods or services.[52] In circumstances where one virtual currency is disposed of to acquire another, the capital gain (or loss) arising from the disposal is worked out using the market value of the original virtual currency when it is disposed of.

Whether capital gains tax applies to a virtual currency disposal depends on whether it is held as an investment, or as a personal use asset kept primarily to purchase items for personal use or consumption:

a if held as an investment, any capital gains from a virtual currency disposal will be added to an individual's assessable income provided that, if the individual held the virtual currency for at least 12 months prior to its disposal, any capital gain is eligible for a 50 per cent discount; and
b if held as a personal use asset and acquired for less than A$10,000, a virtual currency will generally be exempt from capital gains tax; however, any capital losses from its disposal cannot be used to offset any capital gains.

49 Australian Taxation Office: Tax treatment of crypto-currencies in Australia – specifically bitcoin, QC42159, https://www.ato.gov.au/misc/downloads/pdf/qc42159.pdf.

50 Examples include virtual currency traders, miners, exchange operators and virtual currency automated teller machine operators.

51 Australian Taxation Office: Tax treatment of crypto-currencies in Australia – specifically bitcoin, QC42159, https://www.ato.gov.au/misc/downloads/pdf/qc42159.pdf, p. 7.

52 ibid., p. 7.

ATO has provided the following guidance on how capital gains tax will be applied to virtual currency chain splits, where a holder of virtual currency receives new virtual currency in addition to their existing holdings:[53]

a if held as an investment, the initial receipt of the new virtual currency is not earned as income nor is a capital gain made; in determining the capital gain on a disposal of that new virtual currency, the cost base will be zero; and

b if held as part of a business, it will be treated as trading stock (see Section IX.i).

iii GST

Since 1 July 2017, the sale and purchase of digital currencies[54] or its use as a payment is not subject to GST (i.e., Australia's value added tax regime), unless a person is carrying on a business in relation to the virtual currency, as described above.

iv Fringe benefits tax

If an employee has a valid salary sacrifice arrangement with its employer (i.e., to receive a virtual currency as remuneration for work performed instead of Australian dollars), the payment of the virtual currency may be a fringe benefit, making the employer subject to fringe benefits tax. Employers must pay tax at on the taxable value of fringe benefits provided to employees, such as cars and mobile phones, and, in this case, virtual currencies. If there is no valid salary sacrifice arrangement, the virtual currency will be deemed to have been earned as ordinary salary or wages, and the employer must meet its pay as you go tax obligations on the Australian dollar value of the virtual currency it pays to the employee.

X OTHER ISSUES

The DCI Code was published by the ADCA in February 2016 following the recommendation of the 2015 Senate Economics References Committee Report on Digital Currencies regarding the development of a self-regulatory model in consultation with government agencies.[55]

The DCI Code may be voluntarily adopted by virtual currency businesses that are located or provide services in Australia.[56] Businesses certified by the ADCA as DCI Code-compliant must be independently audited and adhere to certain best practice standards.[57]

The DCI Code also requires certified members to:

a apply data security systems and processes to protect customer data, including virtual currency identifiers, wallet addresses and user credit card information; and

b adopt, maintain and comply with an AML/CTF and sanctions compliance programme addressing a risk assessment framework, employee due diligence processes, governance controls and AML/CTF compliance.[58] See Section IV regarding AML/CTF obligations and Section V regarding virtual currency exchange regulation.

53 ibid., p. 6.

54 As defined in Section 195.1 of A New Tax System (Good and Services Tax) Act 1999 (Cth).

55 Recommendation 3, Digital Currency – game changer or bit player, Senate Economics Reference Committee, 4 August 2015 at [5.64].

56 DCI Code Clause 3.2, ADCA, http://adca.asn.au/home-2/code-of-conduct.

57 ibid., Clause 4, ADCA, http://adca.asn.au/home-2/code-of-conduct.

58 ibid., Clause 4.3.2, ADCA, http://adca.asn.au/home-2/code-of-conduct.

XI LOOKING AHEAD

As with many jurisdictions, Australia's legal and regulatory landscape for DLTs is in its early stages, and will continue to evolve as DLT-use cases continue to develop.

Virtual currencies and TGEs have represented the main initial use cases for DLTs, and consequently have been the main area of focus for regulators to date. As DLT-use cases expand over the next few years and the business models become more diverse, we expect the legal and regulatory landscape will continue to evolve as policymakers and regulators seek to grapple with these developments and realign the legal and regulatory landscape in response.

i Higher levels of enforcement action likely in the short term

Despite the significant decrease in the ICO market in 2019 compared with 2017–2018, ASIC's enforcement approach to ICO enforcement activities is likely to continue to focus its enforcement priorities on fraud and misleading conduct, consumer protection and more egregious breaches of local securities law. We expect AUSTRAC to closely monitor the sector for DCE compliance failures given the end of the AML/CTF Act policy principles period on 2 October 2018. We also expect the ATO to continue to expand its compliance programme to prevent further leakages from the Australian tax base owing to cryptoassets.

ii Experimentation with DLT by traditional institutions will continue

We are continuing to see banks and other traditional financial institutions continuing to experiment with DLTs. For example, in July 2019, three major Australian banks formed a consortium with IBM and a shopping centres operator to launch a live pilot for Lygon, a digital platform underpinned by DLT designed to streamline and reduce the risk of fraud in connection with obtaining and managing bank guarantees.[59] This pilot points to the growing interest by Australian banks in using DLT where it offers advantages to manage its risk, or otherwise to help improve organisational understanding of DLT and the future possibilities for its integration into business.

In April 2019, the operator of the Australian Securities Exchange (ASX) launched a sandbox for a proposed DLT-based replacement of its exchange settlement and clearing system. ASX announced that the April software drop into the sandpit was one of seven drops planned at regular intervals over the following 12 months, aimed at allowing customers to interrogate business functionality and assess options. The ASX plans to roll out the DLT-based platform in March 2021, after it announced in September 2018 a delay to the initial roll-out target of Q4 2020, highlighting the complexity of replacing entrenched legacy systems with the new DLT-based platform.

iii Facebook

In June 2019, Facebook announced in a white paper its plans to introduce Libra, a new decentralised blockchain, virtual currency and smart contract platform aimed at creating new opportunities for 'responsible financial services innovation'.[60] Given Facebook's position and

59 ANZ: Banks, IBM and Scentre launch Lygon blockchain to transform bank guarantee process, https://media.anz.com/posts/2019/07/banks--ibm-and-scentre-launch-lygon-blockchain-to-transform-bank?adobe_mc=MCMID%3D75708814272297219856107743574585734039%7CMCORGID%3D67A216D751E567B20A490D4C%2540AdobeOrg%7CTS%3D1562544000.

60 Facebook, Libra White Paper, https://libra.org/en-US/white-paper/.

reach, Libra could be the catalyst to bring virtual currencies mainstream. However, regulatory scrutiny is likely to remain high and will probably require regulators to look long and hard at whether existing banking and financial regulations are fit for purpose. We also expect that ventures such as Libra may raise questions regarding the ongoing relevance of some other virtual currencies, and precipitate a greater need for interoperability between DLTs to maximise adoption.

iv STOs will become more prominent as tokenisation moves into more traditional asset classes

Entities that wish to undertake TGEs are becoming more sophisticated in their approaches, which have started to better account for the requirements of securities and other legislation and the stated concerns of regulators.

We see the rise of STOs as the next big step in the use of DLTs as a fundraising tool. This will extend the benefits of tokenisation beyond the creation of virtual currencies and utility tokens into new areas.

There are a range of factors that are driving the shift to STOs over time:

a greater levels of regulator-led scrutiny and enforcement against unregulated offerings;

b the application of tokenisation and fractional ownership techniques to new asset classes (e.g., illiquid assets) and business models (e.g., crypto VC funds and hedge funds) that need to be structured to comply with local securities law;

c the entry of more traditional funding sources into crypto markets, such as VC funds, family offices and large financial institutions; and

d the greater use of technology to remove the costs associated with the launch of regulation-compliant securities across several markets.

The shift to STOs is also likely to be accompanied by a shift to a compliant by default approach to TGEs, where the underlying rights associated with the relevant token are treated as a security or financial product.

Unlike traditional funding mechanisms, such as initial public offerings, which have significant costs and risks that cannot otherwise be avoided, the availability of standardised regulation-compliant security token platforms will play a significant role in facilitating the more cost-efficient delivery of STO-based fundraising. Several platforms have already started to emerge globally in this space and we expect these platforms to be used to drive fundraising activity across several jurisdictions in parallel as a means of increasing the investor pool in a manner that complies with the securities, taxation and AML/CTF legislation in each jurisdiction. Australia will not be immune to these developments.

Chapter 3

AUSTRIA

Nicholas Aquilina and Martin Pichler[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

i Definition of virtual currencies

Although there has been a steady increase in the public awareness of, and attention from the legislature and the administration about, virtual currencies (and cryptocurrencies based on blockchain technology in particular) in Austria over the past few years, mainly owing to the rise of Bitcoin and the popularity of initial coin offerings (ICOs) and initial token offerings (ITOs), the momentum has subsided. Various industries have long used virtual currencies tailored for their respective purposes, such as online gaming and social gaming, where operators often use self-created currencies or currency units for placing stakes or making certain payments inside a game, albeit in most cases not based on blockchain technology.[2] Over the past three years, there have been several ICOs and ITOs, but the market has since calmed.

The Austrian legislature has continued to focus on the matter, but virtual currencies have still not been incorporated as a concept in Austrian law. However, the definition of virtual currencies as set out in Article 1(2)(d) of the Amendments to the Fourth EU Anti-Money Laundering Directive[3] (often referred to as the Fifth AML Directive) will soon be introduced into the Austrian legal system in the course of the implementation of the Amendments to the Fourth EU Anti-Money Laundering Directive into Austrian law. Apart from this new definition based on supranational EU law, virtual currencies may be classified by using the existing legal definitions in Austrian legislation, both under general civil law as well as under regulatory legislation, and in particular in the sectors of banking and financial services regulation and capital markets regulation.

The legislative definition set by the Amendments to the Fourth EU Anti-Money Laundering Directive will soon be implemented into the Austrian Financial Markets Anti-Money Laundering Act (FM-GwG) as follows:

> *Virtual currencies: a digital representation of value that is not issued or guaranteed by a central bank or a public authority, and is not necessarily attached to a legally established currency, and does not possess a legal status of currency or money, but is accepted by natural or legal persons, as a means of exchange, and which can be transferred, stored and traded electronically.*[4]

---

1 Nicholas Aquilina is an attorney and Martin Pichler is a senior associate at Brandl & Talos Rechtsanwälte GmbH.

2 Rericha/Aquilina, 'Initial Coin Offering: Ein Fall für die FMA?', *ecolex* 2017, 1116.

3 Directive (EU) 2018/843 amending Directive (EU) 2015/849 (Amendments to the Fourth EU Anti-Money Laundering Directive).

4 Section 2 Paragraph 21 Ministerial Draft on the Federal Act amending the Financial Market Anti-Money Laundering Act; Article 1(2) Letter d of Directive (EU) 2018/843 amending Article 3(18) of Directive

This definition is based on function, and does not make a distinction as to whether virtual currencies are generated using blockchain technology.

Cryptocurrencies are commonly understood to be special forms of virtual currencies. Payment systems and the storage and management of cryptocurrencies are organised by a decentralised computer protocol: protection is ensured by cryptographic signature sequences. However, there may be blockchain-based coins, often referred to as tokens, that are not created by a decentralised network of miners by solving complex mathematical problems, but rather issued by an individual or company in the course of an ICO or ITO. During 2017, there was increased activity in Austria in this sector, and a number of companies (in particular start-ups) have started evaluating or have successfully completed ICOs or ITOs, including some that have been reviewed by the Austrian Financial Markets Authority (FMA). At the end of 2018, the FMA for the first time also reviewed and approved a security token that confers 'real' profit participation rights to its holders (see Section II.ii).

There are numerous questions from a legal perspective that need to be considered and (should) influence business decisions when it comes to conducting or setting up a business involving virtual currencies. Solid legal advice is key to conducting virtual currency businesses and transactions (including ICOs and ITOs) successfully and preventing sanctions (e.g., for failing to observe banking and financial services licensing obligations).

ii Virtual currencies and general civil law

Starting from a very general perspective, the Austrian Civil Code (ABGB) distinguishes only between the notions of persons and objects. Section 285 ABGB states very generically that anything that is not a person (qualified as such from a legal perspective) is an object. As virtual currencies obviously cannot be qualified as persons, they must be qualified as objects. Within the term 'objects', a distinction is made between movable and immovable on the one hand, and physical and non-physical on the other. According to Section 292 ABGB, physical objects are those that are perceptible by sense. This is understood to include objects that have a certain spatial delimitation, because only then can an object be physically controlled.[5] According to the ABGB, any objects that are not considered physical qualify as non-physical objects.

If, inter alia, data, formulae, codes and software are not placed in or on a physical object (e.g., data saved on a USB stick), they are considered non-physical objects.[6] This concept can be illustrated by using Bitcoin as an example. An item consisting of several individual objects (whether physical, non-physical or both) (Section 302 ABGB), such as a storage medium on which an entire blockchain, and thus also the private key of a Bitcoin owner, is stored, is qualified as a physical object according to Section 302 ABGB if it is regarded as a single unit in legal transactions. Therefore, a card containing a blockchain and a digital key of Bitcoin could be regarded as *universitas rerum*, and therefore as a physical object. However, as a digital key, which may be temporarily stored on a physical storage medium, but can also be transferred separately (i.e., digitally), Bitcoin shall be qualified as a non-physical object pursuant to Section 292 ABGB, and not within the meaning of Section 302 ABGB as

(EU) 2015/849 (Amendments to the Fourth EU Anti-Money Laundering Directive).

5 Kisslinger in Fenyves/Kerschner/Vonkilch (Hrsg), *Großkommentar zum ABGB – Klang Kommentar* – Sections 285 to 352 ABGB Sachenrecht I, third edition (2011) Section 292(1).

6 Eccher/Riss in Koziol/Bydlinski/Bollenberger (Hrsg), *Kurzkommentar zum ABGB*, fifth edition (2017) Section 292(1).

universitas rerum.[7] Virtual currencies may also be qualified as non-physical objects by using the following line of argument: virtual currencies constitute data records in an account book. These data records determine which address contains which certain value.[8] As neither a data record nor an account book is (necessarily) a physical object, virtual currencies are classified as non-physical objects under general civil law.

iii Virtual currencies and the term money

The mainstream use and understanding of the word currency in terms of virtual currencies implies that – at least under certain circumstances – virtual currencies could be considered as money from a legal perspective. However, the legal definition of currencies is legal tender recognised by the state that is subject to compulsory acceptance, also referred to as fiat currencies.[9] Money as qualified by Austrian law is created by a sovereign act in which the state determines a certain currency and raises it to the status of legal tender.[10] Money is further considered as a means of payment recognised by the state and carrying an obligation to be accepted as legal tender.[11] The Euro Act further qualifies what is considered as legal tender.[12]

Virtual currencies, on the other hand, are (generally) not a state product, but are either created decentralised and online (as in the case of Bitcoin), or issued by a non-governmental person, company or agency (e.g., a company that carries out an ICO). Virtual currencies (generally) lack an official act of a state government, which is why they are generally not regarded as money.

As virtual currencies are not qualified as money (or legal tender or currency), transactions involving the exchange of virtual currencies are therefore generally not subject to the special civil law rules on making a purchase, but rather are subject to the more general rules of exchange in kind (i.e., qualified as exchanging one object for another).[13] Under Section 1053 ABGB, through a purchase agreement, one item is given by one person to another person for a certain amount of money. As a virtual currency is not qualified as money, exchanging such virtual currency for another object (e.g., another virtual currency, such as a coin or token issued in the course of an ICO, being exchanged for Ether) is subject to an exchange-in-kind contract rather than a purchase contract.[14] This also corresponds to the definitions of the Amendments to the Fourth EU Anti-Money Laundering Directive and the Austrian Ministerial Draft on the Federal Act amending the FM-GwG (the Ministerial Draft), which

7 Aquilina/Stadler, 'E-Commerce-Transaktionen im B2C Bereich' in Eberwein/Steiner (Hrsg), *Bitcoins*, 98–99.

8 Völkel, 'Privatrechtliche Einordnung virtueller Währungen', *ÖBA* 2017, 385 (387).

9 Rericha/Aquilina, 'Initial Coin Offering: Ein Fall für die FMA?', *ecolex* 2017, 1116 (1117).

10 Falschlehner/Klausberger, 'Zur finanzmarktrechtlichen Einordnung von Bitcoins' in Eberwein/Steiner (Hrsg), *Bitcoins*, 38–39.

11 Welser, *Fachwörterbuch zum bürgerlichen Recht*, 219–220.

12 Section 1 Euro Act covers banknotes denominated in euros as well as coins and collector coins denominated in euros or cents.

13 Aquilina/Stadler, 'E-Commerce-Transaktionen im B2C Bereich' in Eberwein/Steiner (Hrsg), *Bitcoins*, 103–104.

14 Aicher in Rummel/Lukas, *ABGB*, fourth edition, Section 1046(3) (status: 1 May 2017, rdb.at).

refer to virtual currencies as means of exchange[15] accepted by natural or legal persons.[16] According to Section 1045 ABGB, an exchange in kind is a contract whereby one object is exchanged for another object. The difference in the special form of purchase contracts becomes clear by reading Section 1046 ABGB: money is not an object of an exchange-in-kind contract. However, it follows that in the case of exchanging virtual currencies for fiat money (such as the euro), the transaction is considered a purchase contract.

II SECURITIES AND INVESTMENT LAWS

The following provides a brief overview of the applicability of the Austrian Alternative Investment Fund Managers Act and the Austrian Capital Markets Act to virtual currencies.

i Alternative Investment Fund Managers Act

In accordance with Section 2(1)(1) of the Alternative Investment Fund Managers Act (AIFMG), any collective investment undertaking (including its sub-funds) that collects funds from a number of investors to invest them for the benefit of those investors in accordance with a specified investment policy shall be deemed to be an alternative investment fund (AIF) as long as the funds directly serve the operational activity and the fund is not an undertaking for collective investments in transferable securities (UCITS) pursuant to the UCITS Directive.[17] The management of an AIF requires a licence as alternative investment fund manager (AIFM) to be issued by the FMA.

Virtual currencies may also be part of the assets of an AIF. The explanatory notes to the AIFMG expressly emphasise that the AIFMG should apply to all AIFMs that manage the full range of funds not covered by the UCITS Directive.[18] An Austrian AIF can thus be used to implement any investment strategy in which (also) virtual assets are invested.[19] Whether the investment of virtual currencies is subject to the AIFMG has still not been entirely clarified by the Austrian authorities. However, the FMA has now taken the view that business models requiring participation in the mining of cryptocurrencies such as Bitcoin may constitute an AIF and may therefore fall within the scope of the AIFMG.[20] Consequently, such business models may be subject to a licence issued by the FMA.[21]

ii Capital Markets Act

According to Section 2 of the Capital Markets Act (KMG), the public offering of securities or investments is only permitted if a prospectus has been published, at the latest one banking

15 In Section 2(21) of the Ministerial Draft on the Federal Act amending the Financial Market Anti-Money Laundering Act, virtual currencies are referred to as 'Tauschmittel'.

16 Article 1(2)(d) of Directive (EU) 2018/843 amending Article 3(18) of Directive (EU) 2015/849 (Amendments to the Fourth EU Anti-Money Laundering Directive); Section 2(21) Ministerial Draft on the Federal Act amending the Financial Market Anti-Money Laundering Act.

17 Directive 2009/65/EC.

18 Explanatory notes to the AIFMG (ErläutRV 2401 BlgNR XXIV. GP 3).

19 Majcen, 'Bitcoins und andere virtuelle Währungen . . . bald eine neue Anlageklasse im modernen Asset Management?', *ÖBA* 2017, 691 (695).

20 FMA FAQ on the application of the AIFMG (status: August 2018).

21 Gorzala/Hanzl, 'Mining – Bergbau oder doch alternatives Investment in das Schürfen von Kryptowährungen?', *ÖBA* 2018, 560.

day prior to the launch of the offer. With respect to securities as qualified by the KMG, the European and national legislators understand transferable securities in accordance with the Markets in Financial Instruments Directive II.[22] These mainly include equities and equity-type securities, as well as non-equity securities, such as debt securities and other securitised debt securities.[23] Whether virtual currencies qualify as securities pursuant to the KMG is controversial: as the KMG also subjects the public offer of investments to the prospectus requirement, even if taking the view that virtual currencies do not constitute securities, it is still necessary to assess whether they fall under the definition of investments pursuant to Austrian law. Differences between securities and investments basically only exist with regard to the specifications by which the prospectus has to be prepared. Otherwise, the differences are negligible.

In accordance with Section 1(1)(3) KMG, investments are uncertificated property rights (rights to claims, membership rights or rights *in rem*)[24] for the direct or indirect investment of several investors who carry the risk, either alone or jointly with the issuer, and that investors do not administer themselves. The term investment includes uncertificated profit participation rights, limited partnerships and silent participations.[25] Prospectuses for investments do not follow the scheme of the Prospectus Regulation,[26] but those according to the annexes provided in the KMG.

A precondition for the existence of an investment is that it is issuer-based (i.e., that property rights are mediated through an issuer). Coins designed as decentralised virtual currencies (such as Bitcoin) are exempt as investments because they do not have an issuer who acts as a mediator.[27] Coins are created by a large number of users on the basis of protocol calculations (mining). Moreover, with genuine cryptocurrencies such as Bitcoin or Ether, the essential factors that are decisive for an investment pursuant to the KMG are not present: thus, although there is a property right in the broadest sense, there is no investment in cryptocurrencies. Genuine cryptocurrencies such as Bitcoin do not convey membership-like rights to a company, and investors do not invest funds with the aim of having a third party invest, or otherwise invest the funds at the risk of multiple investors for the purpose of multiplication. There is, therefore, a lack of the community aspect or joint risk in an investment about cryptocurrencies as required for the concept of investments. The income derived from the mining or sale of genuine cryptocurrencies is rather generated by the transfer of an asset, and the price or resale price for such transactions is formed by the rules of supply and demand. Genuine cryptocurrencies are non-physical objects that can be exchanged for other goods or legal tender. Such coins are therefore an asset or a product (see also Section I.ii).[28] The public offering of a commodity is not a public offer of a security or an investment that requires the issuing of a prospectus.[29]

22 Directive 2014/65/EU.

23 Lorenz/Zib in Zib/Russ/Lorenz (Hrsg), *Kapitalmarktgesetz* (2008) Section 1(37) ff.

24 Zib/Russ/Lorenz in Zib/Russ/Lorenz (Hrsg), *Kapitalmarktgesetz* (2008) Section 1(30).

25 Kalss/Oppitz/Zollner, *Kapitalmarktrecht*, second edition (2015) Section 11(17).

26 Regulation (EU) 2017/1129.

27 Paulmayer, 'Initial Coin Offerings (ICOs) und Initial Token Offerings (ITOs) als prospektpflichtiges Angebot nach KMG?', *ZFR* 2017, 532.

28 Piska/Völkel, 'Kryptowährungen reloaded – auf dem Weg aus dem Bermuda-Dreieck', *ecolex* 2017, 816 (816 f).

29 Federal Administrative Court decision of 29 July 2014, W148 2000409-1 = ZFR 2015/119.

A distinction must be made between genuine decentralised cryptocurrencies such as Bitcoin and Ether, and those coins and tokens that can be created centrally by a certain individual or company in any number and are not open to mining by other users, such as generally is the case with ICOs or ITOs.[30] Such cases must be evaluated individually as to whether there is an investment pursuant to the KMG. If a coin or token represents a value attached to a project or company (and the coin or token thus has an intrinsic value), there is a considerable risk that it will meet the requirements for a prospectus requirement under the KMG.[31] In cases where coins or tokens confer affiliate rights or economic ownership or are an investment in a company or project, or it is apparent that several investors have invested or managed a common account[32] in which the invested funds have been used for profit maximisation, such cases may constitute an investment subject to the regulations of the KMG.

Issuers have to decide from an *ex ante* consideration at the time of an ICO or ITO whether the token or coin to be issued fulfils the requirements for a prospectus obligation according to the KMG. If the issuer comes to the conclusion that the ICO or ITO qualifies as an investment as per the KMG and the issuer wants to avoid creating a prospectus, the issuance of the coin or token must be designed so that it meets one of the exceptions of Section 3 KMG (e.g., the offer of tokens or coins for a minimum of €100,000; an offer to qualified investors only; or an offer to fewer than 150 persons per Member State of the European Economic Area who are not qualified investors). In these cases, a prospectus will not be required.

If there is an investment as per the KMG, the issuer's other legal obligations also depend on the issuance volume. If the issuance volume of the ICO or ITO is less than €250,000, it is excluded from the scope of the obligations as per the KMG. For issuance volumes from €250,000 to €2 million, the provisions of the Alternative Financing Act (AltFG) apply, but not the requirements of the KMG with regard to a prospectus. In this case, the issuer must prepare an information sheet in accordance with the AltFG. For issuance volumes from €2 million to €5 million, the issuer may draw up a simplified prospectus according to Scheme F of the KMG. For issuance volumes from €5 million onwards, a KMG brochure according to Scheme C is required.

In addition to ICOs and ITOs, the FMA had to examine a security token for the first time in late 2018. A security token is a tokenised security, based on the blockchain. Pursuant to the FMA's previous legal opinion, the security token was subject to the prospectus requirement of the KMG and the FMA approved the prospectus published by the issuers.[33] This is to be seen as the first approval for tokenised securities in Europe. However, the reason for the mandatory prospectus was that the respective profit participation right was classified as a security, not that it was issued via blockchain. It is nevertheless expected that this will be of great relevance for issuing other securities in the future (i.e., shares or bonds).

30 Paulmayer, 'Initial Coin Offerings (ICOs) und Initial Token Offerings (ITOs) als prospektpflichtiges Angebot nach KMG?', *ZFR* 2017, 532.

31 ibid.

32 Lorenz in Zib/Russ/Lorenz (Hrsg), *Kapitalmarktgesetz* (2008) Section 1(31) f.

33 FMA FinTech Navigator on ICO (https://www.fma.gv.at/querschnittsthemen/fintechnavigator/initial-coin-offering/; accessed on 24 June 2019).

III BANKING AND MONEY TRANSMISSION

i Banking Act

All banking transactions subject to the Banking Act (BWG) are defined by the exhaustive list in Section 1(1) BWG. The most relevant transactions for virtual currencies are Section 1(1)(1) (deposit business), Section 1(1)(6) (issuing and managing means of payment) and Section 1(1)(7) (trading in foreign cash and financial instruments).

Deposit business (Section 1(1)(1) BWG)

Deposit business pursuant to Section 1(1)(1) BWG is the receipt of external funds for administration (first case) or as a deposit (second case).

Funds are accepted within the meaning of Section 1(1)(1) BWG for administration (first case) if the recipient has a 'certain degree of discretion' with regard to these funds in order to use them as agreed in the interest of the depositor.[34] The depositor thus has an unconditional claim for repayment of the amount remaining under contractually agreed administration. The realisation of an administrative activity does not conflict with the fact that the depositor can decide for him- or herself in individual cases or intervene with instructions, as long as the recipient has 'the power of limited independent action'. However, in cases where the depositor specifies in each case how the funds shall be invested, and thus the receiving institution lacks any discretionary power, money is not considered as being accepted for administration. In addition, if the repayment claim depends on the economic condition of the company in which the investor participates by acquiring company shares, this is not considered a deposit business.[35]

According to prevailing opinion, the acceptance of repayable funds from the public that are used as a means of investment is considered a deposit subject to Section 1(1)(1) BWG (second case), if such business is undertaken not only occasionally, but rather as a regular business model.[36] A deposit pursuant to Section 1(1)(1) BWG (second case) is subject to the depositor having an unconditional claim for repayment with respect to the money deposited.[37] A conditional repayment claim, which also includes a loss participation of the depositor, therefore does not qualify as a deposit within the meaning of the law.[38]

The issuance of genuine virtual currencies shall not be qualified as a deposit business according to Section 1(1)(1) BWG. As there is no issuer for such virtual currencies, users also have no repayment claim. The situation may be different with centrally issued virtual currencies. In the case of ICOs and ITOs in particular, the receipt of funds for administration (first case) may be fulfilled if the investor can return the coins or tokens after the expiration of a certain time to the issuer, so that these coins or tokens have a term and an attainable repurchase price (e.g., depending on financial key figures of a company issuing the coins or tokens), or the development of a particular project is funded by the coin or token proceeds.

34 Supreme Administrative Court decisions of 22 February 2006, 2005/17/0195; 4 September 2008, 2008/17/0034.

35 Waldherr/Ressnik/Schneckenleitner in Dellinger (Hrsg), *Bankwesengesetz* (8. Lfg 2016) Section 1(23).

36 Waldherr/Ressnik/Schneckenleitner in Dellinger (Hrsg), *Bankwesengesetz* (8. Lfg 2016) Section 1(25).

37 Oppitz in Chini/Oppitz (Hrsg), *BWG – Bankwesengesetz* Section 1(10); Schrank/Meister, 'Cash Pooling im Lichte des BWG', *ZFR* 2013, 257.

38 Oppitz in Chini/Oppitz (Hrsg), B*WG – Bankwesengesetz* Section 1(10).

Issuing and managing means of payment (Section 1(1)(6) BWG)

The term means of payment generally comprises accepted monetary surrogates in circulation that are accepted by a larger group of persons, such as credit cards, travellers cheques and e-money. Thus, the issuance of vouchers or regional currencies, as well as the issuance of coins or tokens created within the framework of an ICO or ITO, may well be subject to the provisions of Section 1(1)(6) BWG. ICOs regularly focus on applying the exception of the limited network pursuant to Section 1(1)(6) BWG, according to the prevailing administrative practice used within the meaning of Section 2(3)(1) of the Austrian E-Money Act (E-GeldG), if the means of payment issued only has a limited amount of points of acceptance (such as a limited number of service providers accepting the coin, or in cases where a coin is only accepted for the acquisition of a limited selection of goods), so that there is no means of payment recognised by the general public and, in particular, the coin issued in the ICO does not create a parallel currency posing a systemic risk to the legal tender in use.[39]

Section 1(1)(7) BWG refers to trading in foreign legal tender and financial instruments. As the FMA does not (currently) qualify Bitcoin or similar virtual currencies as financial instruments or means of payment, the aforementioned activity does not fall under Section 1(1)(7) BWG.

ii Securities Supervision Act

Advice about and brokerage and administration of virtual currencies

Transactions involving the acquisition and sale of virtual currencies are currently not subject to a licence obligation or to a trade licence in Austria, as virtual currencies are not considered financial instruments.[40] All activities referred to in Section 3(2) of Securities Supervision Act requiring a licence issued by the FMA are based on the term financial instruments: investment advice in relation to financial instruments; portfolio management by managing portfolios on an individual basis with the discretion under a power of attorney of the client, if the client portfolio contains one or more financial instruments; and acceptance and transmission of orders if these activities are related to one or more financial instruments.

iii E-Money Act

Virtual currencies are currently not legal tender in Austria (see Section I.iii). Section 1(1) E-GeldG defines e-money as any electronically (including magnetically) stored monetary value in the form of a claim against an e-money issuer issued against payment of a sum of money. Therefore, there must at least be the possibility of a three-party relationship (issuer–buyer–third point of acceptance).[41] The criteria must be cumulative.[42] However, virtual currencies are different from e-money because a virtual currency, unlike e-money, does not express capital in conventional units of account (e.g., euros) but in virtual units of account.[43] Decentralised cryptocurrencies such as Bitcoin or Ether also do not have a single

39 Rericha/Aquilina, 'Initial Coin Offering: Ein Fall für die FMA?', *ecolex* 2017, 1116 (1119) with further references.

40 Seggermann in Brandl/Saria (Hrsg), *WAG 2018,* 2nd edition, Section 1(86).

41 Leixner, *Zahlungsdienstegesetz/E-Geldgesetz* 2010 (2011) Section 1(5).

42 Rericha/Aquilina, 'Initial Coin Offering: Ein Fall für die FMA?', *ecolex* 2017, 1116 (1117).

43 Majcen, 'Bitcoins und andere virtuelle Währungen bald eine neue Anlageklasse im modernen Asset Management?', *ÖBA* 2017, 691.

issuer, but are created in the network via a specific algorithm; they also do not create a claim against an issuer. The situation may, of course, be different in the case of virtual currencies issued in the course of an ICO or ITO. Frequently, participants in an ICO acquire only a claim against the issuer for the transfer of the respective volume of coins or tokens to a wallet. In general, this requirement is immediately fulfilled by transferring coins or tokens to a participant's wallet. In ICOs, there may thus be cases in which an issuer would require a licence as an e-money institution pursuant to the E-GeldG if the exceptions from the licence obligation – such as found in the case of a limited network (see also Section III.i) for the acceptance of the issued coins or tokens – are not met.

iv Payment Services Act

The commercial provision of payment services may trigger a concession obligation, in particular if a virtual currency is qualified as a means of payment within the meaning of the BWG (see Section III.i) or as a payment instrument. A payment instrument within the meaning of Section 4(14) of the Payment Services Act (ZaDiG) is any personalised instrument, such as a credit card including the cardholder's code or signature, or any personalised procedure agreed between the payment service user and the payment service provider that can be used by the payment service user to issue a payment order, such as the access code of the payment service user and the transaction numbers and transaction codes in online banking.[44] Owing to the lack of personalisation, virtual currencies frequently do not constitute payment instruments pursuant to the ZaDiG, as they are usable and are transferable by anybody. Furthermore, the FMA also applies the limited network exception to the ZaDiG (Section 3(3)(11) ZaDiG; see also Section III.i).

IV ANTI-MONEY LAUNDERING

Under Austrian criminal law, concealing or disguising the origin of assets resulting from certain criminal activities is classified as money laundering. In addition to penal provisions (Section 165 Austrian Criminal Code (StGB)), various laws and regulations exist in this context to prevent money laundering.

The main Austrian law on preventing money laundering is the FM-GwG. This federal Act was passed to implement the EU's Fourth Anti-Money Laundering Directive, and is essentially intended to prevent money laundering and the financing of terrorism in the banking and financial services sectors. The Ministerial Draft implements the Amendments to the Fourth EU Anti-Money Laundering Directive, and for the first time expressly refers to virtual currencies and includes a definition thereof (see also Section I.i). In the course of the public consultation, various stakeholders issued critical statements regarding the Ministerial Draft.[45]

44 Rericha/Aquilina, 'Initial Coin Offering: Ein Fall für die FMA?', *ecolex* 2017, 1116 (1119).

45 For example, Völkel (1/SN-137/ME XXVI. GP – Comment on Ministerial Draft) criticises that virtual currency is defined as the representation of a value that is 'accepted' as a means of exchange. This definition would only be based on actual acceptance, as is the case with Bitcoin or Ether. However, a coin issued during an ICO would not be accepted and therefore not be covered by this definition. A similar argument can be made as regards the representation of a 'value' as it may also be questionable whether coins issued at the very beginning of an ICO already have a value.

According to Section 1 FM-GwG, the obligations stated in the FM-GwG are directed at credit institutions and financial institutions; the Ministerial Draft also includes certain providers of services with regard to virtual currencies.[46] The planned definition includes not only providers of wallets and exchanges but also service providers who offer the transfer of virtual currencies and the provision of financial services for the issuance and sale of virtual currencies into the scope of obliged entities.[47] Further to this, a number of Austrian laws and regulations refer to the FM-GwG when it comes to the anti-money laundering (AML) and counter-terrorist financing (CTF) rules applicable to certain obliged entities. This is the case, inter alia, in the sports betting Acts of Austria's nine provinces, and also in the AIFMG, the E-GeldG and the BWG. However, other Austrian legislation beyond the FM-GwG may also include specific requirements and obligations aimed at the prevention of money laundering and the financing of terrorism.

The FM-GwG provides for various obligations to be met by the respective obliged entities. Insofar as an entity involved in doing business with virtual currencies is considered an obliged entity pursuant to the FM-GwG, it has to subject transactions to its obligations under the FM-GwG, including customer due diligence (know your customer), checking the source of funds and a risk assessment. The Ministerial Draft also contains a registration obligation with the FMA for providers of services with regard to virtual currencies. In the course of registration, a service provider must disclose, inter alia, the name or company name of the service provider, the managing director, the company's registered office, a description of the business model, a description of the internal control system to comply with the requirements of the FM-GwG, and the identity of the owners and the amount of their shareholding in the service provider. The FMA shall refuse registration in case of doubts as to whether the requirements of the FM-GwG can be met or if the FMA has doubts as to the personal reliability of a person who wishes to become a service provider with regard to virtual currencies. The lack of such registration could result in the FMA prohibiting the service provider from performing its activities. The FMA should, however, first take less restrictive measures.

According to Section 4 FM-GwG, obliged entities must prepare an internal risk assessment regarding money laundering and terrorist financing. Furthermore, the FM-GwG provides that certain due diligence obligations towards customers must be applied, with enhanced due diligence measures applying in certain cases. Pursuant to Section 5 FM-GwG, customer due diligence is required in the following cases, irrespective of whether the transaction or business relationship is performed by using virtual currencies or fiat money, whereby the thresholds set by the FM-GwG in euros will apply by using exchange rates as in the case of transactions with foreign fiat money (non-euro):

a establishing a business relationship;

b execution of all transactions that do not fall within the scope of a business relationship (occasional transactions) if either:
- the amount of the transaction exceeds €15,000; or
- the transaction is processed electronically by a payment service provider and the amount exceeds €1,000;

c the deposit or disbursement of saving deposits if the amount exceeds €15,000;

46 Section 1 Ministerial Draft.

47 Section 2(22) Ministerial Draft.

d if it is suspected that a customer is a member of a terrorist group, or is involved in transactions that serve money laundering or terrorist financing; and

e in the case of doubts about the authenticity or appropriateness of previously obtained customer identification data.

If one of the above-mentioned cases occurs, the due diligence obligations pursuant to Section 6 FM-GwG, or the simplified or increased obligations pursuant to Section 8 or Section 9 FM-GwG, respectively, must be complied with. The obligations are aimed at depriving customers of the advantage of anonymity; therefore, the most important tasks are to ascertain the best possible identification of a customer and his or her relevant assets, which includes virtual currencies. Customers can be identified, for example, by presenting certain identification documents. Various documents relating to a customer's business activities or financial circumstances can be used to prove the legal origin of assets. Appropriate due diligence measures will also have to be undertaken in the case of handling transactions involving virtual currencies, whereby there are no specific measures that the FM-GwG stipulates as regards transactions involving virtual currencies. The degree of the due diligence methods applied depends on the result of the internal risk assessment, which will need to take the specifics of virtual currencies, in particular as regards traceability and potential anonymity, into account, in particular in terms of checks into the source of funds and wealth.

Moreover, the FM-GwG also provides for certain reporting obligations: according to Section 16 FM-GwG, an obliged entity must report to the Financial Intelligence Unit when there is a suspicion that a customer is using or attempting to use funds resulting from a criminal act listed in Section 165 StGB, or if there is a suspicion that a transaction is related to a criminal organisation, terrorist organisation or terrorist financing. The Financial Intelligence Unit (Money Laundering Reporting Office) is an agency established at the Federal Criminal Police Office. Transactions that create a reporting obligation must not be carried out subject to instructions from the Money Laundering Reporting Office.[48]

The FM-GwG in its current form is the implementation of the Fourth Anti-Money Laundering Directive. Amendments to the Fourth Anti-Money Laundering Directive entered into force on 9 July 2018, and Austria is in the process of implementing these into national law. The Ministerial Draft has not yet entered into force as the legislative procedure is ongoing (see also Section X).

V REGULATION OF EXCHANGES

There is no specific regulation of exchanges in Austria yet, and – subject to the business model of exchanges not falling under specifically regulated activities pursuant to Austrian banking and financial services regulations – they are generally not subject to licensing by the FMA. At an EU level, amendments to the Fourth Anti-Money Laundering Directive for the first time include exchanges as obliged entities, and thus operators of exchanges will also be subject to AML/CTF legislation in Austria once the Ministerial Draft enters into force (see Sections IV and X).

48 Section 17(1) FM-GwG.

VI REGULATION OF MINERS

Mining currently does not fit into any regulatory or supervisory structure. On 22 May 2018, the FMA published an update to its FAQ catalogue on the application of the AIFMG. In these FAQs, the FMA takes the view that certain business models in connection with the mining of cryptocurrencies may constitute an AIF.[49] The most important consequence of the applicability of the AIFMG to these business models is the inadmissibility of distribution to private consumers, as such business models do not meet the requirements of Section 48 or 49 AIFMG.[50] However, it remains to be seen whether the FMA will eventually prevail with this view (see also Section II.i).

VII REGULATION OF ISSUERS AND SPONSORS

There are no explicit regulations regarding issuers and sponsors. The European Parliament and the Ministerial Draft both define virtual currencies as 'a digital representation of value that is not issued or guaranteed by a central bank or a public authority'.[51] However, new units of genuine cryptocurrencies are created by mining, and there are no issuers in the area of typical cryptocurrencies such as Bitcoin or Ether.

In comparison, there are virtual currencies that are generated within an ICO or ITO. Tokens are basically digital coupons whose functions can vary depending on the ITO in question. In most cases, they serve as the currency for a project financed with them, and companies that give out such tokens to finance their project can therefore be considered as issuers. The initial issuance of coins or tokens by a company to potential investors against the payment of a cryptocurrency (especially Bitcoin or Ether) or money has become a popular financing model in the past year. It is therefore necessary to examine the banking and investment supervisory classification of ICOs (see Sections II and III).

VIII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

Given that they are considered as objects under civil law, virtual currencies are qualified as a person's assets under Austrian criminal law. Therefore, both civil and criminal law apply to virtual currencies, notwithstanding the more complicated regulatory law situation. As a result, the full scope of criminal law applies to criminal conduct involving cryptocurrencies just as it would if the offence involved legal tender: for example, the embezzlement of a virtual currency or any fraudulent behaviour to elicit virtual currency is prosecuted under Austrian criminal law, and virtual currencies can be the subject matter of civil or criminal proceedings.

There are, however, certain factual difficulties both in criminal and civil procedural law, in particular when it comes to enforcement. Besides the obvious – such as the anonymity immanent to many cryptocurrencies, which leads to difficulties when trying to recover elicited or embezzled assets – there are difficulties in confiscating virtual currency in criminal procedures, and also in executing civil adjudications. At the moment, Austrian authorities have no means to

49 Piska/Völkel, 'Mining als Alternativer Investmentfonds? Angenommen, die FMA hat Recht . . .', *ecolex* 2018, 703.

50 Rirsch/Tomanek/Wintersberger, 'Mining von Kryptowährungen im Anwendungsbereich des AIFMG', *ecolex* 2018, 699 (702).

51 Article 1(2)(d) of Directive (EU) 2018/843 amending Article 3(18) of Directive (EU) 2015/849 (Amendments to the Fourth EU Anti-Money Laundering Directive); Section 2(21) Ministerial Draft.

seize virtual currencies other than forcing their owners to transfer a virtual currency to a wallet in the authorities' disposal. This is done via inflectional punishments (monetary punishments and, if necessary, detention) that are limited quantitatively and qualitatively.

Inflectional punishments cannot be inflicted upon suspects under Austrian criminal procedure law, as they are in conflict with the *nemo tenetur se ipsum accusare* principle, prohibiting the authorities from forcing any person accused of a criminal offence to incriminate him- or herself in any way. This principle is construed widely, prohibiting any means to force a suspect to support the authorities in criminal proceedings against a suspect itself. Therefore, if a suspect is not cooperating, it currently is largely impossible to find, seize and confiscate assets in the form of virtual currencies from suspects under Austrian criminal procedure law.

IX TAX

According to Section 23 No. 1 of the Austrian Income Tax Act (EStG), income from a trade or business that is undertaken with the intention of making a profit can be characterised as a participation in a general economic activity.

Where cryptocurrencies are created by mining, this constitutes a commercial activity. The creation of cryptocurrencies is treated like the production of commodities. The operation of a virtual currency exchange, through which virtual currencies can be exchanged for other virtual currencies or purchased for fiat money, is considered a commercial activity, and thus any income derived from such business is subject to income tax. This also applies to virtual currency automated teller machines through which virtual currencies can be purchased, for example, by inserting euro banknotes.

The income tax treatment of virtual currencies held as private assets depends on whether they are interest-bearing. In that case, virtual currencies are qualified as assets pursuant to Section 27(3) EStG. For non-interest bearing assets, virtual currencies are subject to taxation according to Section 31 EStG in cases where the period between the acquisition and the disposal does not exceed one year. In cases of different units of a virtual currency having been acquired at different points in time but all being held in the same wallet, the units acquired first are treated as being disposed of first (the 'first in, first out' principle).

As regards value added tax (VAT), the exchange of fiat money for Bitcoin or other similar virtual currencies and vice versa is not subject to VAT. The Court of Justice of the European Union confirmed this in its landmark ruling in the Swedish *Hedqvist* case, which is transferrable to Austria due to the harmonisation of the VAT legislation across the European Union.[52] According to the Austrian tax authorities, mining is also not subject to VAT owing to the lack of an identifiable beneficiary.[53]

With regard to using virtual currencies for paying for goods or services, in general the same tax rules apply as when using legal tender. The basis for the tax assessment is determined by the value of the virtual currency.

52 CJEU, 22 October 2015, C-264/14, *Hedqvist*.

53 Ponesch-Urbanek/Beer, 'Kryptowährungen im Experten-Check', *ögwthema* 2017 H 4, 16; CJEU, 22 October 2015, C-264/14, *Hedqvist*.

X LOOKING AHEAD

Recently, changes concerning the regulation of virtual currencies have also been considered at the national level. In March 2018, the Federal Minister of Finance, Hartwig Löger, proposed stricter regulations for cryptocurrencies.[54] Specifically, Mr Löger mentioned a reporting obligation to the Money Laundering Reporting Office for transactions exceeding €10,000. He also proposed subjecting trading platforms for cryptocurrencies to the supervision of the FMA. As regards ICOs, which were extremely popular in Austria in late 2017 and early 2018, and thus also created relatively widespread media attention, Mr Löger stated that he favours introducing an obligation to produce a 'lightweight prospectus'. To review and implement these proposals, he convened a FinTech Regulatory Council to make proposals for appropriate legal framework conditions. The Council's priorities are the creation of the new lightweight prospectus law for ICOs and the regulation of virtual currencies similar to gold or derivatives.[55] The Council is set to meet once every two months. It shall draft proposals, including recommendations and concrete measures that could be undertaken, with a particular focus on data protection and consumer protection.[56] Mr Löger had initially set the deadline that by the end of 2018, the FinTech Regulatory Council should have defined concrete measures and presented concrete results in this area. Furthermore, he promised that 'by the end of this year [2018], there will be a circular letter from the FMA in which the insights of the Council can already be fixed in a legal adaptation area that will then also be valid'.[57] So far, however, no documentation of the Council has been made publicly available.

Furthermore, Doris Margreiter, a member of the Social Democratic Party, submitted a formal written inquiry in Parliament to Mr Löger regarding her view of 'ICOs as partly unregulated high-risk businesses' on 7 September 2018. By way of example, the inquiry covers the following questions: will the government's efforts to regulate ICOs be intensified in the coming years? Is a change in the law on this subject planned within the next two years? And is it planned to implement a new law that is fully prepared for the online financial market of the 21st century? The deadline for dealing with this inquiry was 7 November 2018. The answers to these questions largely referred to the tasks of the FinTech Regulatory Council.

In early 2019, the Federal Ministry of Finance created a proposal for an Amendment of the Financial Market Authority Act introducing a regulatory sandbox.[58] This concept – on the basis of a similar concept introduced by the British Financial Conduct Authority – enables fintech companies to test their business models under the supervision of the FMA. After receiving a licence for the regulatory sandbox, licences required for the actual exercise of the business model can be applied for separately. The FMA will provide support during this process. This enables business models from the cryptocurrency sector to be tested in advance in a protected environment. Miners, as well as exchanges, could use the regulatory sandbox to test their business model in compliance with regulatory requirements and by receiving assistance from the FMA. The proposal has not entered into force yet as the legislative procedure is ongoing.

54 Austrian Ministry of Finance, https://www.bmf.gv.at/presse/LoegerKryptowaehrungen.html (accessed on 29 August 2018).

55 Austrian Ministry of Finance, https://www.bmf.gv.at/presse/fintech_beirat.html (accessed on 29 August 2018).

56 'Anfragebeantwortung des Bundesministers für Finanzen', *AB* 382 XXVI. GP 2.

57 Stenographic record of the National Council, XXVI.GP, 31st Meeting, 14 June 2018, p. 120.

58 Austrian Ministry of Finance, https://www.bmf.gv.at/presse/FinTech.html (accessed on 24 May 2019).

Chapter 4

AZERBAIJAN

Ulvia Zeynalova-Bockin[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

The rise of virtual currencies and the underlying blockchain technology in recent years have presented regulators around the world with an interesting challenge: striking a delicate balance between regulating this nascent phenomenon of decentralised currency, while avoiding overzealous regulation so as not to stifle innovation. Azerbaijani regulators are no exception.

Although it has been recognised that the use of virtual currencies and blockchain technology represents an emerging global trend,[2] and despite real concerns about fraud, money laundering and other illicit activities potentially involving the use of virtual currencies, there is no specific regulation of virtual currencies in Azerbaijan. There are, of course, regulations in place that would potentially be applicable to virtual currencies, but the real challenge seems to be how to classify virtual currencies, as they possess the characteristics of various types of assets (e.g., a unit of account, a commodity or a security), thus eluding traditional regulatory definitions.

For this reason, any discussion on how virtual currencies ultimately will be regulated in Azerbaijan inevitably becomes an exercise in educated conjecture, taking into account the current understanding on the classification of virtual currencies and regulatory parameters. Depending on how virtual currencies are ultimately classified by the Azerbaijani regulators (as a unit of account, a commodity or a security), different regulations may potentially be applicable, as outlined below.

II BANKING AND MONEY TRANSMISSION

Generally, the Banking Law attributes the activity of monetary transmission (money transfer services or payment instruments) to be a licensable banking activity.[3] Further, the Law on Currency Regulation regards foreign currency exchange activities (i.e., engaging in

---

1 Ulvia Zeynalova-Bockin is counsel at Dentons. The author would like to acknowledge the invaluable editorial guidance of James E Hogan, managing partner at Dentons, and Ophelia Abdullayeva for her input on taxation-related matters.

2 The State Programme on the Expansion of Digital Payments in the Republic of Azerbaijan for 2018–2020, approved by Decree of President of the Republic of Azerbaijan, No. 508, dated 26 September 2018, Republic of Azerbaijan Collection of Legislation 2018, No. 09, Item 1893 (in Azerbaijani), Article 4.6. Available at http://e-qanun.gov.az/framework/40164.

3 Law of the Republic of Azerbaijan 'On Banks', No. 590-IIQ, dated 16 January 2004, Republic of Azerbaijan Collection of Legislation 2004, No. 03, Item 130 (in Azerbaijani), Article 32. Available at http://e-qanun.gov.az/framework/5825.

the business of buying or selling foreign currencies) as an additional licensable activity in Azerbaijan in which only local banks, branches of foreign banks, certain licensed post offices and entities holding foreign currency exchange licences may engage.[4]

The Law on Currency Regulation defines foreign currencies as money in the form of banknotes, treasury notes and coins in circulation that are legal tender in the territory of a foreign state or group of states. Although unlikely, it is possible that virtual currencies will be classified as a foreign currency, especially if they are recognised as legal tender in a foreign country.[5]

Therefore, entities wishing to engage in the above-mentioned activities involving a virtual currency within Azerbaijan or, potentially, Azerbaijani residents, are likely to be prevented from doing so, unless the relevant licence has been obtained.

III ANTI-MONEY LAUNDERING

When it comes to money laundering and terrorism financing, Azerbaijani law does not seem to make any material distinction between transactions carried out using a fiat currency or a virtual currency (although the latter is not specifically mentioned). For instance, any transactions involving funds received from or transferred to anonymous accounts located outside Azerbaijan or transactions where the parties cannot be accurately identified, or in cases where the submission of identification information about a customer or beneficiary is denied, as well as where identification information about a customer or beneficiary is discovered to be false, are required to be reported to the Financial Monitoring Service.[6]

The current anti-money laundering regime in Azerbaijan covers, among other regulated entities, monitoring subjects, the definition of which includes financial institutions, institutions engaged in money transmission services, investment companies, investment funds and investment fund managers.[7] It is these monitoring subjects that have the obligation to report the foregoing transactions.

Given the potential for abuse of the anonymity present in transactions using virtual currencies and the possible implications for the enforcement of anti-money laundering legislation, this is an area where specific regulations are very likely to be enacted.

IV TAX

Given the broad definition of income under the Azerbaijani Tax Code, revenues generated by residents from trading virtual currencies are likely to be subject to taxation. As no special regime for the taxation of capital gains exists in Azerbaijan, these revenues are likely to be

4 Law of the Republic of Azerbaijan 'On Currency Regulation', No. 910, dated 21 October 1994, Supreme Council of the Republic of Azerbaijan Information [Bulletin] 1995, No. 07, Item 116 (in Azerbaijani) (Law on Currency Regulation), Article 3. Available at http://e-qanun.gov.az/framework/9238.

5 id., Article 1.7-1 and 1.7-2, and Article 3.

6 Law of the Republic of Azerbaijan 'On the Prevention of the Legalization of Criminally Obtained Funds or Other Property and the Financing of Terrorism', No. 767-IIIQ, dated 10 February 2009, Republic of Azerbaijan Collection of Legislation 2009, No. 02, Item 58 (in Azerbaijani) (Law on the Prevention of the Legalization of Criminally Obtained Funds or Other Property and the Financing of Terrorism), Article 7. Available at http://e-qanun.gov.az/framework/16347.

7 id., Article 4.

subject to personal income tax at a 14 per cent marginal rate (in relation to individuals not registered as entrepreneurs), simplified tax (applicable to certain individual entrepreneurs) or corporate profit tax (applicable to certain individual entrepreneurs, enterprises with revenues exceeding a certain threshold and those not qualified to become simplified taxpayers). General taxation principles would apply to transactions using a virtual currency.[8]

It is not clear what the tax authorities' approach to enforcement would be given that, currently, the assessment of taxes on income received from abroad is largely dependent on self-declaration. However, there is a general, and rather vague, provision in the Law on Currency Regulation requiring residents of Azerbaijan to repatriate earned foreign currency reserves received from foreign economic activities, which are likely to include funds received from virtual currency trading once they are converted into fiat currency.[9]

Failure to comply with the repatriation rules may result in significant administrative fines (of up to 50 per cent of such foreign currency reserves)[10] or, potentially, criminal liability for the management officials of the company where the funds exceed the equivalent of 20,000 Azerbaijani manats.[11]

V OTHER ISSUES

i Legal tender

The 1995 Azerbaijan Constitution (the Constitution), which was adopted in a nationwide referendum, proclaims the Azerbaijani manat as the official currency of Azerbaijan and the only monetary unit that is recognised as legal tender within the territory of Azerbaijan.[12] The Constitution recognises the exclusive authority of the Central Bank of Azerbaijan (the Central Bank) to issue banknotes and mint coins.[13]

The Civil Code, the cornerstone of commercial law, goes even further by requiring that contractual monetary obligations between residents be denominated in Azerbaijani manats.[14] Finally, wages may also only be paid in Azerbaijani manats.[15]

8 Tax Code of the Republic of Azerbaijan, approved by Law of the Republic of Azerbaijan No. 905-IQ, dated 11 July 2000, Republic of Azerbaijan Collection of Legislation 2000, No. 08, Item 583 (in Azerbaijani). Available at http://e-qanun.gov.az/code/12.

9 Law on Currency Regulation, Article 7.2.

10 Code of Administrative Offenses of the Republic of Azerbaijan, approved by Law of the Republic of Azerbaijan No. 96-VQ, dated 29 December 2015, Republic of Azerbaijan Collection of Legislation 2016, No. 02, Item 202 (in Azerbaijani), Article 483. Available at http://e-qanun.gov.az/code/24.

11 Criminal Code of the Republic of Azerbaijan, approved by Law of the Republic of Azerbaijan No. 787-IQ, dated 20 December 1999, Republic of Azerbaijan Collection of Legislation 2000, No. 04, Item 251 (in Azerbaijani), Article 208. Available at http://e-qanun.gov.az/code/11.

12 Constitution of the Republic of Azerbaijan, adopted at a nationwide referendum on 12 November 1995, Republic of Azerbaijan Collection of Legislation 1997, No. 03, Item 159 (in Azerbaijani), Article 19.I and 19.III. Available at http://e-qanun.gov.az/framework/897.

13 id., Article 19.II.

14 Civil Code of the Republic of Azerbaijan, approved by Law of the Republic of Azerbaijan No. 779-IQ, dated 28 December 1999, Republic of Azerbaijan Collection of Legislation 2000, No. 04, Item 250 (in Azerbaijani), Article 439.1. Available at http://e-qanun.gov.az/code/8.

15 Labour Code of the Republic of Azerbaijan, approved by Law of the Republic of Azerbaijan No. 618-IQ, dated 1 February 1999, Republic of Azerbaijan Collection of Legislation 1999, No. 04, Item 213 (in Azerbaijani), Article 174.4. Available at http://e-qanun.gov.az/code/7.

As such, virtual currencies are not, and are very unlikely to become, legal tender in Azerbaijan. In fact, recognising them as such would likely require amendments to the Constitution to be adopted in a nationwide referendum. It is not clear that the authority of the Central Bank to issue banknotes and mint coins would include minting electronic coins for a cryptocurrency protocol backed by the Central Bank.

So far, the Central Bank has not expressed any intention to engage in the minting of electronic coins, and has described its position regarding the virtual currency as conservative. In remarks made during discussions on the 2018 State Budget in Parliament, the Chair of the Central Bank, Mr Elman Rustamov, described cryptocurrencies as an instrument for investing rather than an alternative means of payment.[16]

ii Currency controls

Under the Law on Currency Regulation,[17] residents may carry out currency operations related to the movement of capital (such as, for instance, the purchase of securities expressed in foreign currency), subject to the regulations[18] specified by the Central Bank. These rules apply both to residents (generally, legal entities registered in Azerbaijan and Azerbaijani citizens) and non-residents (generally, legal entities registered outside Azerbaijan, and their branches and representative offices in Azerbaijan), and they set forth an exhaustive list of grounds for remittances in foreign currency, as well as related documentary requirements.

These regulations may hinder the ability of Azerbaijani residents to invest in virtual currency as, even though they expressly permit residents and non-residents to remit funds for the purposes of investing in securities (including those denominated in foreign currency),[19] no express permission exists in relation to remittances for the purposes of investing in virtual currency.

VI LOOKING AHEAD

In January 2018, it was reported that a working group had been established in Azerbaijan to develop a draft law on the regulation of trade in virtual currencies.[20] However, it seems that no progress has been made to date. In all likelihood, and based on various public statements

16 Anvar Mammadov, 'CBA head comments on use cryptocurrency in Azerbaijan', Trend News Agency (21 November 2017), accessed on 8 August 2018, https://en.trend.az/business/economy/2824191.html (in Azerbaijani).

17 Law on Currency Regulation, Article 8.2.

18 Rules of the Central Bank of the Republic of Azerbaijan 'On Conducting Foreign Currency Transactions by Residents and Transactions of Non-Residents in Foreign and National Currency in the Republic of Azerbaijan' No. 45/1, dated 28 November 2016 (in Azerbaijani) (Currency Regulations), Article 4.3. Available at http://e-qanun.az/framework/34248.

19 Currency Regulations, Article 4.3.13.2.

20 Lada Evgrashina, 'Azerbaijan takes up crypto-currencies: the bill is being prepared, the country will be visited by co-founder Ethereum', 1news.az (29 January 2018), accessed on 12 July 2019, http://www.1news.az/news/azerbaydzhan-vzyalsya-za-kriptovalyuty-gotovitsya-zakonoproekt-stranu-posetit-so-osnovatel-ethereum (in Russian).

of local officials, Azerbaijani regulators are likely to continue to monitor[21] the virtual currency space and assess regulatory measures adopted by other countries before any specific regulation is adopted.

The experiences of countries that share a common legal heritage with Azerbaijan, such as other (larger) countries in the Commonwealth of Independent States, are closely monitored. It is possible that Azerbaijan will follow the lead of Russia and adopt legislation similar to the Second Draft Law on Digital Financial Assets (which, at the time of writing, is being discussed in the Russian parliament).[22] This Law is expected to, among other things:

a regulate relations arising out of the creation, issuance, storage and circulation of digital financial assets, digital tokens and the specific activities of the operators of information systems (within which digital financial assets are issued) and those of the operators of digital financial asset exchanges; and

b provide detailed definitions of certain cryptocurrency-related terms, including for digital financial assets, digital tokens and distributed ledgers, and classify them.

The absence of specific regulations on virtual currencies and their underlying technology in Azerbaijan may contribute to uncertainty and potentially stifle innovation in their implementation. For this reason, and in the interest of encouraging innovation in this sphere, the adoption of a separate law would be a welcome legislative development.

A great deal of care should be given to striking the correct balance in regulating virtual currency-related activities and providing clear guidance to market players, while at the same time avoiding unintended consequences of overzealous regulation, which is a difficult, but not impossible, task. It remains to be seen if the Azerbaijani regulators will take up this challenge any time soon.

21 Samuel Haig, 'Azerbaijan rejected Crypto as means of Payment', Cryptofame (4 December 2017), accessed on 12 July 2019, https://news.bitcoin.com/azerbaijan-rejects-crypto-as-means-of-payment/.

22 Second Draft of the Federal Law of the Russian Federation 'On Digital Financial Assets', Consultant.ru (21 March 2019), accessed on 11 July 2019, http://static.consultant.ru/obj/file/doc/pr_fz210319_2.rtf (in Russian).

Chapter 5

BELGIUM

Michiel Van Roey and Louis Bidaine[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

i Virtual currencies

Virtual currencies are defined by the European Central Bank (ECB) as 'a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money'.[2] It clarifies that even though they can be used as an alternative to money, virtual currencies are not money or currency from a legal perspective.[3] It provides further clarification by proposing three subcategories of virtual currencies that are classified according to their interaction with legal tender (or similar instruments) and on their ability to be used to purchase tangible goods and services.[4] These three subcategories are:

a Closed virtual currencies schemes: these are virtual currencies that have no interaction with the physical world. They cannot be obtained using legal tender (or similar instruments), nor can they be exchanged back into legal tender, and they cannot be used for purchasing goods and services in the physical economy. An example given by the ECB is World of Warcraft (WoW) gold, an in-game virtual currency that WoW players can use to better equip their avatars to reach higher levels in the game.

b Virtual currencies schemes with unidirectional flow: these are virtual currencies that can be purchased using fiat currency but cannot be converted back into fiat currency. Examples are Facebook credits or air miles in frequent flyer programmes.

c Virtual currencies schemes with bidirectional flow: these are virtual currencies that users can buy and sell according to an exchange rate with fiat currency, and that can be used to purchase physical goods and services. The most notable example of bidirectional virtual currencies are cryptocurrencies, which form the main subject of this chapter considering their increasing influence and controversy in today's economy.

---

1 Michiel Van Roey, representing MVR Legal BV, is general counsel and ICO legal adviser at Profila GmbH and Belux legal counsel at Cisco Systems, and Louis Bidaine is legal and ICO project manager for Profila GmbH.

2 European Central Bank (2015), 'Virtual Currency Schemes – a further analysis', https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, p. 4.

3 'From an economic perspective, the virtual currencies currently known about do not fully meet all three functions of money defined in economic literature: (i) medium of exchange, [. . .], (ii) store of value [. . .], 3) unit of account', European Central Bank (2015), o.c., 23. This opinion is shared by the Advocate-General of the Belgian Court of Cassation, André Henkes (https://datanews.levif.be/ict/actualite/il-faut-une-legislation-sur-les-crypto-monnaies/article-normal-885869.html?cookie_check=1562445348).

4 European Central Bank (2015), o.c., 6.

ii Cryptocurrencies and tokens[5]

Although Bitcoin[6] is still by far the most well-known cryptocurrency with the highest market capitalisation, altcoins have emerged in the past few years, and they are bringing innovation to the first generation Bitcoin protocol. Several second (and even third[7]) generation cryptocurrencies and tokens have emerged over the past few years. One well-known example is Ether, the cryptocurrency for operating the distributed application platform Ethereum, an open-source, blockchain technology-based software platform that runs smart contracts. Ether has many uses; it provides software developers with incentives to write smart contracts and compensates them for their attributed resources;[8] it can be used for executing smart contracts and for paying for goods and services on the Ethereum network. Ethereum, as a platform, is further used to develop other cryptocurrencies and tokens (i.e., ERC20 tokens such as Tron (TRX), Omisego (OMG), Icon (ICX)[9]) through initial coin offerings (ICOs) (see Section VII).

Recent years have shown the incredible potential of virtual currencies and tokens. Just as every new technology does, virtual currencies face obstacles and uncertainties that affect their market price substantially. As discussed in this chapter, the uncertainty about the legal framework that applies to virtual currencies and tokens is still a major hindrance to their development and adoption in the market.

II SECURITIES AND INVESTMENT LAWS

i Financial market regulators

The financial market in Belgium is regulated by two autonomous supervisory bodies, namely the Financial Services and Markets Authority[10] (FSMA) and the National Bank of Belgium (NBB).[11] The FSMA and NBB are in charge of supervising and monitoring companies operating in the Belgian financial market, and they each have clearly defined roles.

5 The term cryptocurrency often (wrongly) serves as a collective term for different crypto instruments, covering both those that are meant as a means of payment (the actual 'coins' or 'cryptocurrencies', such as Bitcoin) as well as crypto instruments that have a utility or an investment function. For the purpose of this chapter, the latter utility and investment instruments are referred to as 'tokens'. For a more detailed overview of the difference and reasoning behind the distinction between cryptocurrencies and tokens, see A Snyers and K Pauwels, 'De ITO: A new kid on the block in het kapitaalmarktenrecht', *TBH* 2019, Vol. 2, 179.

6 On 17 December 2017, Bitcoin's market capitalisation attained an all-time high of US$332 billion.

7 Third generation cryptocurrencies such as Cardano (ADA) are considered to be more sustainable, interoperable and scalable. https://steemit.com/cryptocurrency/@ramsteem/cardano-ada-3rd-generation-of-cryptocurrency.

8 'Ether, the crypto-fuel for the Ethereum network', see https://www.coindesk.com/information/what-is-ether-ethereum-cryptocurrency.

9 Ethereum Request for Comment, a technical standard or universal language used for smart contracts on the Ethereum blockchain that implement tokens and that cause them to be traded with other tokens on the Ethereum network, https://cointelegraph.com/explained/erc-20-tokens-explained.

10 See https://www.fsma.be/en.

11 See https://www.nbb.be/en.

The FSMA protects the interests of Belgian financial consumers, and is responsible for supervising financial products, financial information published by companies and financial service providers.[12]

The NBB is responsible for overseeing individual financial institutions (e.g., credit institutions, investment firms, payment institutions, electronic money institutions, insurance companies) and the proper functioning of the financial system as a whole.

ii Regulatory framework governing financial markets

As there is no virtual currency-specific legislation on securities and investment laws in Belgium, we elaborate on the existing framework that applies to securities and investments laws. This framework governs financial instruments, investment instruments and financial products, and assesses if and to what extent it applies to virtual currencies and its market participants.

Regulatory framework governing financial instruments and investment services

The Belgian legislation on financial instruments consists of the Act of 21 November 2017 regarding the infrastructures of the market for financial instruments, which transposes Directive 2014/65 into national law (the Act on Financial Instruments), and the Act of 25 October 2016 on access to investment services companies, and on the legal status and supervision of portfolio management and investment advice companies (the Act on Investment Services). The Act on Financial Instruments and the Act on Investment Services are the national laws implementing the second Markets in Financial Instruments Directive (MiFID II).[13] This MiFID-based legal framework aims to foster investor protection and to cope with new trading technologies, practices and activities.

Virtual currencies as financial instruments

MiFID II and the above-mentioned Acts implementing it apply to certain types of entities (such as investment firms or credit institutions) that offer investment services and activities[14] relating to financial instruments. The core of this legislation revolves around the notion of financial instruments.[15] The term financial instruments covers a range of instruments, including transferable securities and derivative products.[16]

It is essential for market participants to assess whether virtual currencies fall under the concept of financial instrument. For this assessment, the distinction made earlier between unidirectional scheme virtual currencies and bidirectional scheme virtual currencies is relevant. The first two categories of virtual currencies, namely the closed and unidirectional

12 This also covers supervising currency exchange offices and intermediaries in banking and investment services, see https://www.fsma.be/en.

13 Directive 2014/65/EU of 15 May 2014 on markets for financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.

14 Defined as 'a service or activity detailed hereafter that relates to financial instruments' and includes eight different services and activities, including the 'reception and transmission of orders in relation to one or more financial instruments', 'execution of orders on behalf of clients' or 'operating a multilateral trade facility', Article 2(1) Act on Investment Services.

15 See Article 4, 15° MiFID II, which refers to Section C of Annex I, in which the list of financial instruments is detailed. See Article 3, 16° Act on Financial Instruments, which refers to Article 2, 1 Belgian Act of 2 August 2002 on the supervision of the financial sector and financial services.

16 Article 2(24) MiFID II.

scheme ones, should not be considered financial instruments. Closed scheme virtual currencies cannot be obtained using legal tender, and unidirectional scheme virtual currencies, although they can be obtained using legal tender, cannot be converted back into legal tender or similar instruments.[17] Their (limited) transferability does not qualify them as investment.[18]

The situation for bidirectional scheme virtual currencies is less straightforward because not all virtual currencies that fall in this category have the same characteristics. Below, we distinguish the three different characteristics of bidirectional scheme virtual currencies. They are used:

a as a means of payment (coins or cryptocurrencies, allowing the owner to use them to pay for certain goods and services that are purchased on the internet (e.g., using Bitcoin to make an online purchase of a wellness session or appointment));

b as a means of investment (investment tokens, granting the owner an economic interest in the company behind the token, linked to the performance of the company); or

c for a utilitarian purpose (utility tokens, granting the owner access to certain goods or services that are offered on the platform of the issuer).[19]

In some specific cases, a token can even have a hybrid function: for example, Ether can be used in many ways on the Ethereum network, but it also functions as a means of payment for buying other tokens in the process of ICOs.[20]

If a bidirectional scheme virtual currency constitutes a means of payment only or has only a utility function, it seems unlikely that it can be considered a financial instrument under Belgian law. Cryptocurrencies and utility tokens are not included in the list of financial instruments in the Act on Financial Instruments, nor do they seem to fall under the scope of transferable securities, as they do not represent a certain right on the company that issued the token.[21] However, the problem with cryptocurrencies and utility tokens is that apart from their principal use, they are being traded on virtual currency exchanges, and fluctuate in price just as other virtual currencies do, and therefore also seem to have some investment function. This can be illustrated by Siacoin.

Siacoin is a utility token that can be used on the Sia storage platform, a decentralised storage platform that:

a leverages under-utilised hard drive capacity around the world to create a data storage marketplace;

b allows users to obtain Siacoins when they make their laptops' hardware available for the benefit of the platform; and

c allows users to store files by paying Siacoins in return.[22]

17 N Vandezande, *Virtual Currencies: A Legal Framework*, Cambridge, Intersentia, 2018, 321.

18 ibid., 322.

19 This distinction between payment, utility and asset tokens is used by the FSMA (Communication No. FSMA_2017_20 of 13 November 2017 on (initial coin offerings), see https://www.fsma.be/sites/default/files/public/content/EN/Circ/fsma_2017_20_en.pdf, p. 2, as well as by other financial market authorities such as the Swiss Financial Market Authority (FINMA), see https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/; A Snyers, K Pauwels, 'ICOs in Belgium: Down the Rabbit Hole into Legal No Man's Land? Part 1', *International Company and Commercial Law Review*, 2018, Issue 8, 491.

20 A Snyers, K Pauwels, o.c., 487.

21 T Spaas and M Van Roey, 'Quo Vadis Bitcoin?', *Computerrecht* 2015/84, June 2015, ed. 3, 118.

22 See https://sia.tech/.

There is no doubt that Siacoin is a utility token, but a person that bought US$1,000 of Siacoins on 7 January 2016 at a rate of US$0.000017 (to obtain roughly 59 million Siacoin tokens) and sold that same amount of utility tokens two years later on 7 January 2018 at US$0.09715 would have made approximately US$5.7 million in profit in just two years' time.[23] Even if the primary purpose of Siacoin is utilitarian, it has been functioning in practice as a means of investment.

Apart from this example, it is undeniable that certain bidirectional scheme virtual currencies can serve primarily as investments, especially if such currency is issued by a private company in the framework of an ICO and has characteristics that entitle investors to a share in the profits of the blockchain-based company that issues the virtual currency, that carries voting rights or that gives right to some kind of interest revenue.[24] In these scenarios, the tokens convey a certain right to the issuer (as per transferable securities), and their value is linked to the success of the company's business. It seems likely that virtual currencies with these characteristics would be considered a financial instrument under Belgian law.

Obligations under the Act on Financial Instruments and the Act on Investment Services

If bidirectional scheme virtual currencies were considered financial instruments under Belgian law, virtual currency market players providing investment services and activities[25] relating to virtual currencies would have to comply with the certain obligations on transparency or licensing, or both,[26] that are imposed by the above-mentioned financial legislation, which includes obligations regarding rules of conduct:[27] to act in an honest, fair and professional way that best serves the customer's interest; to provide customers with information that is clear, fair and not misleading; and to offer services specifically tailored to the customer's situation.

The regulatory framework governing investment instruments

The legal framework governing investment instruments consists of the Prospectus Act of 2018 (the Prospectus Act).[28] The Prospectus Act requires that a prospectus for a public offer[29] of investment instruments be drafted. A list of such instruments can be found in Article 3(1) of the Prospectus Act. Its scope of application is very broad because investment instruments cover a catch-all category of 'all other instruments that enable carrying out a financial investment, regardless of the underlying assets'.[30] Because virtual currencies are all traded on

23 See https://coinmarketcap.com/currencies/siacoin/.

24 See https://cointelegraph.com/explained/ico-explained; A Snyers, K Pauwels, 'ICOs in Belgium: Down the Rabbit Hole into Legal No Man's Land? Part 1', *International Company and Commercial Law Review*, 2018, Issue 8, p. 489.

25 The Belgian Act on Investment Services, implementing into Belgian law certain provisions of MiFID II, is aimed to arrange access to and the provision of investment services, which it defines as 'a service or activity detailed hereafter that relates to financial instruments' and includes the following eight services and/or activities, see Article 2(1) Belgian Act on Investment Services.

26 For example, Article 6 Belgian Act on Investment Services reads 'investment firms governed by Belgian law must, before taking up their activities, obtain one of the following authorisations from the supervisory authority, irrespective of the place where they will carry on their activities [. . .]'.

27 See 'Subpart 9, 'Market rules', Articles 30–34 Act on Financial Instruments.

28 Act of 11 July 2018 regarding public offers of investment instruments and the admission of investment instruments on a regulated market (Prospectus Act), Belgian State Gazette, 20 July 2018.

29 See Article 4(2) Prospectus Act for the definition of public offer.

30 Article 3 §1, 11° Prospectus Act.

exchange platforms, and because their highly volatile nature leads to market speculation, it could be argued that bidirectional scheme virtual currencies would all fall under the scope of investment instrument within the meaning given to the term under the Prospectus Act.[31] Hence, companies offering these virtual currencies to the public and certain intermediaries that act on their behalf would have to comply with the prospectus requirement under certain circumstances.[32]

FSMA guidance and FSMA regulation on financial products

The FSMA has taken a rather neutral approach to virtual currencies, putting the onus on market participants to self-assess whether a given virtual currency would fall under the above-mentioned financial legislation. The FSMA mentions that this assessment should be based on the specific characteristics of the virtual currency, and states that the regulatory status of virtual currencies is to be assessed on a case-by-case basis.[33]

Apart from the neutral stance of the FSMA in relation to virtual currencies and the absence of any virtual currency-specific legislation in Belgium, the FSMA has adopted a regulation that applies to financial products (which are to be considered a subsection of the financial instruments as discussed earlier). This regulation prohibits the 'distribution, in Belgium, as a professional activity, to one or several retail customers of a financial product whose return depends directly or indirectly on a virtual money'.[34] This ban on the distribution of financial products, which are defined as savings, investment or insurance products,[35] applies to virtual money, which is, in its turn, defined as 'any form of unregulated digital currency that is not legal tender'. This ban would apply to derivatives if return depends directly or indirectly on a virtual currency. This would mean, for example, that exchange-traded funds (ETFs),[36] which would invest the money of investors only in virtual currencies, would be banned from offering their services in Belgium. This is highly topical considering the multiple requests for virtual currency ETFs that are currently pending before the United States Securities and Exchange Commission (SEC). The SEC must give its decision on these requests by 18 October 2019.[37]

In the explanatory note accompanying the regulation, the FSMA describes various risks associated with virtual money, from hacking of trade platforms to lack of authority

31 A Snyers, K Pauwels, 'ICOs in Belgium: Down the Rabbit Hole into Legal No Man's Land? Part 1, *International Company and Commercial Law Review*, 2018, Issue 8, p. 499.

32 Article 7 Prospectus Act.

33 See https://www.fsma.be/sites/default/files/public/content/EN/Circ/fsma_2017_20_en.pdf, p.2.

34 Article 2(2) FSMA regulation of 3 April 2014, which was approved by a Royal Decree of 24 April 2014, published in the Belgian Official Gazette on 20 May 2014; for the full text, see https://www.fsma.be/sites/default/files/public/sitecore/media%20library/Files/fsmafiles/wetgeving/reglem/en/reglem_24-04-2014.pdf.

35 Article 2, 39 Belgian Act of 2002 on the supervision of the financial sector and on financial services.

36 'An exchange-traded fund (ETF) is a passive investing instrument that tracks underlying benchmark indexes (such as the NASDAQ-100 Index, S&P 500, Dow Jones, and others), commodities, bonds, or portfolios of assets and replicates their performances. ETFs can be traded like a common stock on exchanges, combining the diversified holdings of a fund with the low cost and tradability of a share': https://cryptoren.com/wiki/exchange-traded-fund-etf-meaning/.

37 'Bitwise Files With US Securities and Exchange Commission to Launch Crypto ETF', see https://cointelegraph.com/news/bitwise-files-with-us-securities-and-exchange-commission-to-launch-crypto-etf; https://cointelegraph.com/news/sec-postpones-vaneck-bitcoin-etf-yet-again-should-we-expect-an-approval-in-2019.

supervision and price volatility. The FSMA also describes several dishonest practices that have been identified in relation to derivative cryptocurrency products where the distribution of such derivative financial products to consumers has led to significant losses to the investors in question. This clearly indicates that the FSMA intends to use this regulation to protect small retail customers and investors against these very complicated financial products.

III BANKING AND MONEY TRANSMISSION

i Electronic money directive

The Act of 11 March 2018 regarding, inter alia, the emission of electronic money (e-money) (the E-money Act),[38] which is the Belgian law implementing the provisions of the E-money Directive,[39] aims to facilitate the emergence of new, innovative and secure e-money services as well as to encourage effective competition between all market participants.

The E-money Act defines e-money as 'electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued upon receipt of funds for the purpose of making payment transactions [. . .] and that is accepted by a natural or legal person other than the electronic money issuer'.[40] Only bidirectional scheme virtual currencies[41] might have some resemblances to this definition of e-money, that is, they are both stored electronically and some virtual currencies are accepted as a means of payment by other parties than the e-money issuer. However, virtual currencies should not be considered e-money under the E-money Act. The main argument supporting this is that virtual currencies are not issued upon receipt of funds because a virtual currency is created digitally.[42] The requirement that e-money needs to be issued upon receipt of funds means that the e-money issuer cannot just create new e-money units, because only central banks have a monopoly over money creation.[43] However, this is just what a virtual currency issuer does: digitally creating a certain amount of virtual currencies through software development. In addition, virtual currencies usually do not create a claim on the issuer, with the exception

38 Article 1 Section 3, 3°–4° Belgian E-money Act.

39 Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (E-money Directive), see https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32009L0110.

40 Article 2(2) E-money Directive and Article 2, 77° Belgian E-money Act.

41 As closed scheme virtual currencies cannot be obtained using legal tender or exchanged back into legal tender, they fall outside the definition of e-money (which needs to be 'issued upon receipt of funds'). The same applies for unidirectional scheme virtual currencies, which have a limited transferability and cannot be redeemed back into legal tender. Although see the definition of e-money in N Vandezande, *Virtual Currencies: A Legal Framework*, Cambridge, Intersentia, 2018, 222–223.

42 N Vandezande, o.c., 272; according to Zeeshan Feroz CEO of Coinbase UK, Coinbase will be allowed to issue e-money and to provide payment services, see https://cryptoslate.com/coinbase-issued-e-money-license-uk-europe/.

43 N Vandezande, o.c., 218.

of certain bidirectional scheme virtual currencies that could be considered to be a means of investment.[44] Consequently, virtual currencies fall outside the scope of the Belgian legal framework concerning e-money.[45]

ii Payment service directive

Payment services are regulated at EU level by the Payment Services Directive II (PSD II),[46] which has been transposed into Belgian law through the adoption of the Act of 11 March 2018[47] (the Payment Services Act). PSD II and the Payment Services Act aim to govern payment services and payment service providers, and to harmonise consumer protection and the rights and obligations for payment providers and users.

Although the Payment Services Act does not regulate the emission of virtual currencies per se, the question arises of whether certain virtual currency market players provide services that could be considered payment services, and whether these players can be seen as part of a certain limited number of payments service providers[48] that have a monopoly over the provision of such services in Belgium.[49] If so, a licence needs to be obtained from the NBB before any payment service provider can offer payment services in Belgium to consumers.[50]

The Payment Services Act defines payment services as any payment service set out in Annex I, which lists eight different payment services, including the execution of payment transactions, money remittance, payment initiation services and account information services.[51] This definition seems very broad, but this broadness is mitigated by several

44 See Section II, 'virtual currencies as financial instruments or investment services'.

45 As a side note, the E-money Directive and the E-money Act put into place a system of e-money licences that institutions can obtain only if they fulfil certain requirements. Even though virtual currencies are not considered e-money, it is interesting to see that some actors, such as the exchange platform Coinbase, have taken a proactive stance towards the regulatory framework on e-money. On 21 March 2018, Coinbase obtained an e-money licence from the United Kingdom Financial Conduct Authority, which means Coinbase is looking to expand its offering beyond virtual currencies, or is anticipating changes in e-money legislation, see https://support.coinbase.com/customer/en/portal/Articles/2928609-e-money-license?b_id=13521.

46 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC, and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, see https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32015L2366.

47 Act of 11 March 2018 on the legal status and the supervision of payment institutions and electronic money institutions, access to the activities of payment service providers and the issuance of electronic money, and access to payment systems. Article 107 PSD II provides for full harmonisation, namely that 'member states can neither keep nor introduce provisions that are different from those contained in the Directive', which entails that EU legislation in relation to payment services is fully harmonised throughout the EU.

48 That is, credit institutions; e-money institutions; bpost; NDD; ECB; federal, regional, community and local Belgian authorities, when they are not acting as a public authority; and payment institutions.

49 Article 1 PSDII and corresponding Article 1 Payment Services Act.

50 Article 6 Payment Services Act.

51 '1. Services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account; 2. Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account; 3. Execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider: (a) execution of direct debits, including one-off direct debits; (b) execution of payment transactions through a payment card or a similar device; (c) execution of credit transfers, including standing orders; 4. Execution of payment transactions where the funds are covered by a credit line for a payment

exemptions in Article 3 of the Payment Services Act. For example, according to the limited network exemption, services based on a payment instrument 'allowing the holder to acquire goods or services only in the premises of the issuer [. . .]' or 'that can be used only to acquire a very limited range of goods or services' fall outside the scope of the Payment Services Act.[52]

Based on this latter exemption, closed scheme virtual currencies and (most) unidirectional scheme virtual currencies can be excluded directly based on their (absence of or limited) transferability. This exemption could even apply to certain bidirectional scheme virtual currencies if their use is limited according what is described above.[53] Whether virtual currency service providers will fall within the scope of the Payment Services Act will have to be assessed on a case-by-case basis taking into account the factual circumstances of each case.

IV ANTI-MONEY LAUNDERING

At the EU level, the Fourth Anti-Money Laundering Directive (AMLD4),[54] transposed into Belgian law through the adoption of the Act of 18 September 2017 on the prevention of money laundering and terrorism funding (the AML Act),[55] aims to intensify efforts to effectively combat money laundering and terrorism financing. It does so by imposing certain risk assessment obligations and obligations to identify customers (know your customer (KYC)), and putting in place transaction monitoring procedures for obliged entities (i.e., certain financial and credit institutions as well as certain legal entities and natural persons in the exercise of their professional activities).

The AML Act applies to goods and property derived from criminal activity and to funds used in terrorism financing.[56] Although virtual currencies could be seen as both goods or property and funds, the AML Act only imposes reporting obligations on obliged entities.[57] These types of entities are listed exhaustively, but no virtual currency market participant is mentioned. Therefore, adding virtual currencies to the concepts of goods or property and funds would not have any actual effect, given that they are not considered to be obliged entities that need to report on any anti-money laundering (AML) or terrorism-funding activities.[58]

service user: (a) execution of direct debits, including one-off direct debits; (b)execution of payment transactions through a payment card or a similar device; (c) execution of credit transfers, including standing orders; 5. Issuing of payment instruments and/or acquiring of payment transactions; 6. Money remittance; 7. Payment initiation services; 8. Account information services.'

52 Article 3(k) Payment Services Act; N Vandezande, *Virtual Currencies: A Legal Framework*, Cambridge, Intersentia, 2018, 258.

53 N Vandezande, *Virtual Currencies: A Legal Framework*, Cambridge, Intersentia, 2018, 272.

54 Directive 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No. 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

55 Articles 2, 3 and 5 AML Act.

56 Article 3 AML Act.

57 Article 4, 18 AML Act.

58 N Vandezande, Virtual Currencies: A Legal Framework, Cambridge, Intersentia, 2018, 298.

The EU legislature amended AMLD4 through the adoption of the Fifth AMLD (AMLD5).[59] With AMLD5, the European Commission specifically adds certain players in the virtual currency industry to the list of obliged entities, namely providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet providers.[60] If and when those amendments are adopted and implemented in Belgian law, it will limit the existing pseudo-anonymity or anonymity[61] of virtual currencies[62] even further. These new obliged entities in the virtual currency space will be compelled to take 'appropriate steps to identify and assess the risks of money laundering and terrorist financing',[63] and to put in place policies, monitoring and procedures to mitigate and manage effectively the risks of money laundering and terrorism-financing. They will also have a reporting obligation when they know, suspect or have reasonable grounds to suspect that certain activities are linked to money laundering.[64]

Although AMLD5 will provide more transparency in the market and will discourage illegal activity to some extent, it only addresses certain service providers of bidirectional scheme virtual currencies. For example, the definition of a custodial wallet provider is limited to 'an entity that provides services to safeguard private cryptographic keys on behalf of its customer, to hold, store, and transfer virtual currencies'.[65] This definition might affect multi-currency desktop wallet providers such as Exodus,[66] Jaxx[67] or MyEtherWallet,[68] but virtual currency owners (including those involved in criminal activities) have a wide range of cold wallets and hardware wallets at their disposal (such as Ledger[69] or Trezor[70]) through which only they, as owner, have access to the private cryptographic keys. There are, therefore, still numerous ways to hold, store and transfer virtual currencies without becoming subject to the KYC or transaction monitoring procedures conducted by the new obliged entities under AMLD5. This Directive might therefore only have limited effect, and additional legislative efforts will be necessary to effectively tackle criminals using virtual currencies.

AMLD5 has not yet been transposed into Belgian law: Belgium has until 10 January 2020 to do so.[71] In the meantime, it seems that the Belgian Executive Branch (in particular, the

59 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive 2015/849 on the prevention of the use of the financial systems for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

60 New Article 2(1)(3) (g) and (h) AMLD4, see Article 1 AMLD4 Amendment.

61 Take Bitcoin as an example: the information in the blockchain does not allow users to access it directly, but contains the exact time and size of each transaction as well as the Bitcoin addresses of the payer and the payee. Together with other information that is stored outside of the Bitcoin protocol, certain transactions can therefore be properly traced back to identifiable persons. The anonymity that Bitcoin and certain other virtual currency offer is only partially anonymous; it is better to speak of a pseudo-anonymous than an anonymous one system: T Spaas and M Van Roey, 'Quo Vadis Bitcoin?', Computerrecht 2015/84, June 2015, ed. 3, 114.

62 New Article 13. 4 AMLD5, see Article 1 AMLD4 Amendment.

63 New Article 8.1, 4A AMLD5, see Article 1 AMLD4 Amendment.

64 New Article 8.2 and Article 47 Section 1 AMLD5, see Article 1 AMLD4 Amendment.

65 New Article 3(19) the AMLD5, see Article 1 AMLD4 Amendment.

66 See https://www.exodus.io/.

67 See https://jaxx.io/.

68 See https://www.myetherwallet.com/.

69 See https://www.ledgerwallet.com/.

70 See https://trezor.io/.

71 Article 4 AMLD4 Amendment.

Minister of Finance responsible for combating tax fraud), in cooperation with the FSMA and NBB, is taking a proactive stance on the issue and is considering adopting Belgian legislation that would oblige virtual currency exchange platforms to formal registration and other AML requirements.[72]

V REGULATION OF EXCHANGES

Virtual currency exchanges play a key role. They offer exchange services to users, and allow them to acquire virtual currencies with fiat money or other virtual currencies.[73] Currently, no specific legislation exists that regulates the business activities of a virtual currency exchange. However, the following is a brief overview of whether virtual currency exchanges would fall under one of the following Belgian laws:

i AML Act

Virtual currency exchanges currently do not fall under the AML Act, but some of them will be seen as obliged entities within the scope of AMLD5, which will be implemented into Belgian law before 10 January 2020. The amended AML Act will not apply to all virtual currency exchanges, however, as it lists only providers engaged in exchange services between virtual currencies and fiat currencies as obliged entities. Virtual currency exchanges such as Binance,[74] which only allow users to buy and sell virtual currencies using Bitcoin or Ether, will not be subject to the AML obligations.

ii E-money Act

Since virtual currencies fall outside the scope of the EU and Belgian legal framework concerning e-money, the E-money Act does not apply to virtual currency exchanges.

iii Act on Financial Instruments and Belgian Act on Investment Services

These two pieces of legislation could apply to exchanges if a certain bidirectional scheme virtual currency was seen as a financial instrument, and if a virtual currency exchange offers investment services or activities in relation to this financial instrument: for example, the reception and transmission of orders in relation to one or more financial instruments. Although no guidance from the FSMA or NBB has been given on the issue, it is likely that certain virtual currency trading platforms, exchange services and virtual currency investment companies already provide such activities, so they could fall within the scope of these two laws. The fact that the virtual currency exchange Blocktrade.com sought approval from the European Financial Market Authority under MiFID II seems to indicate that some exchanges do consider that they are subject to financial legislation.[75]

72 Response by the Minister of Finance, who is charge of combating tax fraud dated, 28 November 2017, to certain parliamentary questions posed by Mr Gilles Foret (MR politician) on 4 October 2017 (Bulletin No. B134, q. 1856), https://www.lachambre.be/kvvcr/showpage.cfm?section=qrva&language=fr&cfm=qrvaXml.cfm?legislat=54&dossierID=54-b134-902-1856-2016201718654.xml.

73 Coinbase is one of the numerous exchangers on the marketplace https://www.coinbase.com/join.

74 See: https://www.binance.com.

75 'New Cryptocurrency Exchange Targets European Regulatory Compliance', Forbes.com, 30 July 2018, see https://www.forbes.com/sites/heatherfarmbrough/2018/07/30/new-fully-regulated-cryptocurrency-exchange-launches/#efe578c335d9. Because of the lack of clarity as to which legislation applies to virtual

The Belgian crypto exchange Bit4you SA, on the other hand, has a different view on the matter. On its website, Bit4you states that its 'first activities launched on 29 August 2018 are not subject to any licence under the current Belgian and European legislation'. In its terms and conditions, it does, however, proactively implement AML and KYC procedures, even though, as explained above, virtual currency exchange platforms are (currently) not subject to the AML Act.[76]

Although Bit4you mentioned during its launch that it obtained the approval of the FSMA and NBB, the latter quickly rectified such statement. Both institutions admit to having spoken to the company, but concluded that the services offered by Bit4you fall outside their respective competences considering that the direct purchase or sale of virtual currencies is not regulated in Belgium.[77]

VI REGULATION OF MINERS

Miners play an important role in virtual currencies networks. The core activity of miners is validating virtual currency transactions by solving a cryptographic puzzle for which they use specialised mining hardware. In return for this, or as a reward, they get a sum of newly mined virtual currencies. In some cases, miners can earn additional transaction fees from users that require faster confirmation of a transaction.

There is no specific Belgian legislation that regulates miners' activities. Nevertheless, any natural person or legal entity that earns money through mining activities could still be subject to Belgian tax law, and might have to pay personal or corporate income taxes.[78]

VII REGULATION OF ISSUERS AND SPONSORS

i Initial coin offerings, initial token offerings and token generating events

In the first quarter of 2018, more than US$6.3 billion was invested in virtual currency companies worldwide via the sale of crypto instruments and digital tokens.[79] These public sales have different names and are referred to as initial coin offerings (ICOs), initial token offerings (ITOs) and token generating events (TGE). For the sake of this chapter and taking into account the wide adoption of the term ICO, we will collectively refer to the different kind of public sales of crypto instruments as ICOs.

According to the FSMA, ICOs are operations through which 'project developers offer digital tokens to the public via the internet as a way of funding the development of the

currency exchanges, they seem to take a very cautious stance. On the website of Kraken, the exchange states that 'Bitcoin's legal status is still being defined, but Kraken takes a highly proactive and informed approach to ensuring legal compliance', and 'our approach is to operate conservatively, entirely within the bounds of current law, and to constantly monitor regulatory developments so that we can anticipate changes before they occur'.

76 Terms and conditions of Bit4you SA, available via the URL: https://www.bit4you.io/terms-and-conditions.

77 See https://trends.knack.be/economie/bedrijven/geen-groen-licht-voor-belgisch-bitcoinplatform/article-normal-1191265.html.

78 See Section IX.

79 https://www.coindesk.com/6-3-billion-2018-ico-funding-already-outpaced-2017/.

project'. Although ICOs resemble initial public offerings and crowdfunding campaigns to a considerable degree, ICOs are still largely unregulated and are often carried out by companies without any proven track record or a viable product, which makes them risky investments.[80]

It should be underlined that the success of virtual currency companies in Belgium is very relative compared to other jurisdictions such as Switzerland or Germany. To date, there has not yet been an ICO conducted out of Belgium, although the increase in ICO activity and in virtual currency awareness will definitely affect Belgium in the coming years.

ii Regulatory framework in Belgium that applies to ICO issuers

At present, there is no specific legislation aimed at ICOs, so there are no ICO-specific regulatory requirements for companies that are planning a token sale in Belgium. However, existing legislation often has a wide scope that might apply to ICOs.[81] As mentioned in Section II, financial legislation might apply to certain bidirectional scheme virtual currencies, depending on the specific characteristics of the virtual currencies issued (i.e., whether they are a means of payment, investment or utility). This is the current stance of the FSMA, and also that of other financial market authorities throughout the world.[82]

On 13 November 2017, the FSMA issued a communication on ICOs in which it warned ICO issuers that their operations might fall under the scope of application of various EU and Belgian legislation.[83] This communication makes clear the FSMA's cautious position regarding the applicable legal framework on ICOs in Belgium. The FSMA did not want to exclude any law a priori.

At first sight, not all Belgian laws to which the FSMA refers in its communication seem inapplicable to ICO issuers. For example, ICO issuers fall outside the scope of application of the AML Act, despite the Belgian legislature's adoption of the AMLD5 amendments that consider (only) virtual currency exchange platforms and custodian wallet providers to be obliged entities.[84] In addition, it is not clear how ICO issuers would fall within the scope of the Belgian Crowdfunding Act,[85] as this Act applies to crowdfunding service providers that

80 Instead, these companies promise to develop a certain blockchain-based product or service in the future, funded by the money they acquired via the ICO. In consideration for the money they receive from the token sale (which can be up to US$1.7 billion for one ICO), these companies will provide tokens that grant the holders with some benefit in the future (access to a platform, discounts to products or services to be developed, etc.). 'Telegram raised $1.7 billion through its two private pre-sales, making it the largest ICO ever. The popular messaging tool is reportedly planning to build an ecosystem of token-based services constructed inside the messenger app, such as distributed file storage and micropayments for peer-to-peer transactions', see https://cryptoslate.com/most-successful-icos-of-2018-so-far/.

81 A Snyers, K Pauwels, o.c., 484.

82 The same goes for the United States, Japan, the United Kingdom, France, Germany, Switzerland, Hong Kong, among others. See Autonomous Next, using analysis from Bloomberg, as of 19 March 2018, Thomas Reuters, Latham & Watkins LLP, pp. 98–106, see https://www.lw.com/thoughtLeadership/crypto-utopia-autonomous-next.

83 In its communication, the FSMA warns ICO issuers that their operations could fall within the scope of various EU directives, including MiFID II, AMLD4, the Alternative Investment Fund Managers Directive and the Prospectus Directive, as well as numerous Belgian laws, including AMLD4 and the Act on AML, the Prospectus Act and the Royal Decree of 24 April 2014 on the commercialisation ban on offering financial products to consumers without professional occupation (as discussed in Section II.iii).

84 See Section IV.

85 Act of 18 December 2016 regulating the recognition and delineation of crowdfunding and containing various financial provisions (Crowdfunding Act).

organise alternative investments via an alternative investment platform. Under the existing law, these alternative investments are defined as 'the service consisting of marketing investment instruments via a website or any other electronic means issued by corporate issuers'.[86] In our view, an ICO issuer does not market such alternative investment services, especially not if the ICO relates to a cryptocurrency or a utility token. In addition, in most cases, it is not the ICO issuer but rather an intermediary third-party company (e.g., Blockstarter, Coinlaunch, Coinlist) that will launch the cryptocurrency or token on the market.[87]

In conclusion, it seems that the principal legislation that ICO issuers should comply with when launching a virtual currency that could be considered an investment instrument on the Belgian market is the Prospectus Act. Under the current Prospectus Act, a prospectus must be drafted for every public offer of investment instruments having a total value of €5 million[88] or more. This prospectus document must be approved by the FSMA before it is made available to the public.[89] Both the form and the contents of the prospectus are regulated. It should notably include a 'short description of the risks related to the investment concerned and the essential characteristics of this investment, including all rights attached to securities' and 'the reasons behind the offer and the intended use of the funds collected'.[90]

VIII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

Virtual currencies are susceptible to misuse as part of criminal activities, and the exponential increase in the value of virtual currencies has not gone unnoticed by cybercriminals. In Belgium alone, there were more than 300 cases of Bitcoin-related scams or thefts during 2017, a number that was surpassed in the first five months of 2018 with more than 329 complaints.[91] Criminal activity, specifically against virtual currency users, can happen on virtual currency exchanges,[92] during virtual currency transactions[93] or when merely holding virtual currencies in a user's wallet.[94] Additionally, the certain degree of anonymity offered by virtual currencies such as Bitcoin (BTC), Monero (XMR) and Zcash (ZEC) makes virtual currencies attractive for transferring illegally obtained funds.

86 Article 4, 2° Crowdfunding Act.

87 For example of such intermediaries, see http://blockstarter.tech/; https://coinlaunch.co/.

88 Article 22 Section 1 Prospectus Act; Exceptions to this principle are listed in Article 3 Section 2 Prospectus Act.

89 Article 23 Prospectus Act.

90 Article 24 Section 2 b) and d) Prospectus Act.

91 'Kris Peeters met en garde contre une fraude aux cryptomonnaies en plein essor', see https://www.rtbf.be/info/economie/detail_kris-peeters-met-en-garde-contre-une-fraude-aux-cryptomonnaies-en-plein-essor?id=9936983; see https://www.hln.be/geld/dit-jaar-al-voor-minstens-2-2-miljoen-euro-aan-fraude-met-cryptomunten~a2e03709/?referer=https%3A%2F%2Fwww.google.com%2F.

92 The famous Mt Gox theft in which hackers stole around US$473 million worth of cryptocurrencies, and the DAO hack, which led to a loss of around US$70 million worth of cryptocurrencies, https://coincodex.com/Article/51/5-biggest-crypto-hacks-of-all-time/.

93 'Hacker Makes Over $18 Million in Double-Spend Attack on Bitcoin Gold Network', see https://www.bleepingcomputer.com/news/security/hacker-makes-over-18-million-in-double-spend-attack-on-Bitcoin-gold-network/.

94 The hacking of virtual currency wallets, which can be held online, locally on a computer's hard drive, a USB stick or even offline in cold wallets, is certainly one of the most sensitive issues. For more information on virtual currency wallets and security risks, see T Spaas and M Van Roey, 'Quo Vadis Bitcoin?', *Computerrecht* 2015/84, June 2015, ed. 3, 114.

To date, no specific criminal legislation concerning virtual currencies has been adopted in Belgium. Unlike other jurisdictions, the legal use of those currencies is not prohibited in Belgium.[95] Nevertheless, certain illegal use of virtual currencies or illegal activity relating to virtual currencies must still comply with the general provisions of Belgian criminal law or specific legislation in relation to computer-related infractions (see subsection ii).

i General provisions of Belgian criminal law

Under the general Belgian law provisions, there are at least three criminal infractions that could apply to illegal activity relating to virtual currencies.[96]

The first criminal offence is common theft, which is covered by Article 461 of the Belgian Criminal Code, which states that 'anyone who fraudulently appropriates anything that does not belong to him is guilty of theft'. Theft of virtual currencies, just as theft of any other form of asset or good, is punishable by prison sentences of up to five years and a fine of up to €4,000.[97]

The second criminal offence is a scam as prohibited under Article 496 of the Criminal Code, which could also be very relevant with respect to virtual currencies. A scammer is defined as a person who:

> *with the intention of appropriating property belonging to another person, takes or receives money, movable property, commitments, discharges, debt liberations [. . .], either by the use of false names or false capacities or by the use of cunning tricks to make one believe that false companies of an imaginary power or of an imaginary credit exist, to expect or cause a successful outcome, an accident or any other mysterious event, or to otherwise abuse trust or credulity.*

This description covers a wide range of situations that could apply to the rigged sale of virtual currencies, and to fake trading platforms and virtual currency exchanges. As an example of this wide coverage, the FSMA, following numerous complaints from Belgian citizens, published a blacklist of virtual currency trading platforms that are suspected of scamming people into investing money for virtual currencies via an exchange where those people never really received any virtual currencies in return or their money back.[98] Another form of scam

95 For example, Ecuador banned virtual currencies and Bitcoin in particular as early as 2014, see https://www.ibtimes.co.uk/ecuador-reveals-national-digital-currency-plans-following-Bitcoin-ban-1463397.

96 Apart from theft and scams, money laundering of virtual currencies that are illegally obtained is a significant criminal activity as well, which can be punishable under certain conditions under the rather broadly described criminal offence of fencing, set out in Article 505 Belgian Criminal Code, which reads: 'a penalty of 15 days to 5 years prison sentence and/or a fine of €26 to €100,000 shall be imposed on the following individuals: 1. Those who have unlawfully received some or all of the items taken, diverted, or obtained by means of a crime or other offense [. . .].'

97 Article 263 Criminal Code mentions up to €500, which has to be multiplied by a factor of eight for criminal sanctions. The Act of 25 December 2016 amending the Act of 5 March 1952 on the surcharges on criminal fines stipulates that as from 1 January 2017, criminal fines are to be multiplied by a factor of eight instead of six.

98 'Belgian Financial Services Markets Authority Warns of Fraud in Cryptocurrency Trading Platforms, Publishes List of Alleged Fraudulent Cryptocurrency Exchanges', see https://www.crowdfundinsider.com/2018/02/128731-belgian-financial-services-markets-authority-warns-fraud-cryptocurrency-trading-platforms-publishes-list-alleged-fraudulent-cryptocurrency-exchanges/.

could be a fraudulent ICO involving a natural person or legal entity that convinces investors to buy tokens, which happen to be fake, and the person or entity suddenly disappears with the investors' money.

Scams in relation to virtual currencies, just as any other form of asset, are punishable by a prison sentence of up to five years and a fine of up to €24,000.[99]

The third criminal offence relates to money laundering as prohibited under Article 505 of the Criminal Code. This provision states notably that a penalty of 15 days' to 5 years' imprisonment or a fine of €26 to €100,000 (or both) shall be imposed on 'those who will have bought, received in exchange for free, possessed, kept, managed the goods referred to in Article 42,3° [pecuniary benefits directly derived from a crime, or the goods and value which have been substituted to them and income from benefits invested] while they knew or should have known the origin of those goods at the beginning of those operations' as well as 'those who will have converted or transferred goods referred to in Article 42.3°, with the aim of concealing or disguising their illicit origin or to help any person entangled in a crime from where those goods stem from, to escape the legal consequences of their actions'.

Given the advantages that virtual currencies (notably their relative anonymity) represent for criminals in conducting their illegal activities, Article 505, and the seizures of assets it can lead to, is one of the most useful provision of the Criminal Code to fight illegal uses of those currencies.

ii Specific legislation regarding computer-related infractions

The Belgian legislature enacted specific pieces of legislation regarding computer-related infractions that are actually more suitable for prosecuting any criminal activity involving virtual currencies.[100]

First, the infraction known as unauthorised access to computer systems (also known as hacking) can apply if a person accesses a computer system and he or she knows that the access was unauthorised (Article 550 *bis*, first paragraph, Criminal Code). Hacking is punishable under criminal law by a prison sentence of up to two years and a fine of up to €200,000.[101]

Second, the hacker might commit the infraction known as concealment of data (Article 550 *bis*, third paragraph, Criminal Code) at the same time if he or she processes or transfers data that was stored on a third-party computer system or that was treated or transmitted by the third-party computer system. Concealment of data under Belgian law is punishable by prison sentence up to two years and a fine of up to €200,000.[102]

A third infraction under Belgian law is computer-related fraud, which applies to anyone who, with fraudulent intent, obtains an unfair economic advantage while altering, changing

99 Article 496 Criminal Code mentions up to €3,000, which has to be multiplied by a factor of eight for criminal fines.

100 Article 504 *quater*, and Article 550 *bis* and *ter* Criminal Code.

101 Article 550 *bis*, Section 1 Criminal Code mentions up to €25,000, which has to be multiplied by a factor of eight for criminal fines; a computer system is understood as 'any system for storage, processing or transmission of data'.

102 Article 550 *bis*, 3° Criminal Code mentions up to €25,000, which has to be multiplied by a factor of eight for criminal fines.

or deleting data that is stored on or transmitted by a computer system. Computer-related fraud is punishable under Belgian law by a prison sentence of up to five years and a fine of up to €800,000.[103]

To illustrate, the above-mentioned infractions could apply to a hacker who gains unauthorised access to a virtual currency user's personal computer and virtual currency wallet (unauthorised access to computer systems or hacking) for the purpose of copying the virtual currency user's private key (concealment of data) to ultimately transfer the virtual currencies stored in the user's wallet to the hacker's personal wallet, which would amount to computer-related fraud (computer-related fraud).

iii Seizure of virtual currencies after criminal activity has been committed

Belgian authorities can confiscate virtual currencies that have been illegally obtained in the course of criminal infractions, just as they can confiscate other illegally obtained assets.[104] The government already has in custody a certain amount of Bitcoins that it has seized during criminal investigations,[105] although the value thereof has not been disclosed.[106] In the framework of a criminal investigation in Belgium, brought before the Court of Appeal of Antwerp on 10 November 2016, the police confiscated 3.54 Bitcoins from a drug dealer.[107] To put this in perspective, the US Federal Bureau of Investigation (FBI) is currently the second-largest Bitcoin owner in the world, with a stunning total of 144,000 Bitcoins, which were worth approximately US$2.8 billion during the all-time high of their value in December 2017.[108]

The question that arises is what can or should a government do with such sum of virtual currencies? Should they be forfeited, and, if so, when should they be sold? On 2 March 2018, Koen Metsu asked the Ministry of Justice how many Bitcoins the government has confiscated since January 2015 and whether the government made a loss on the confiscated Bitcoins after confiscating them.[109] Considering the volatility of virtual currencies, this is an important question, given that the US$2.8 billion worth of Bitcoin from the FBI has lost more than 60 per cent of its value since December 2017.

According to the Ministry of Justice, the Belgian Public Prosecutor is handling hundreds of files concerning virtual currencies, and in at least 10 cases virtual currencies have been seized. However, the Ministry of Justice's response to the parliamentary question did not mention the actual forfeiture of such virtual currencies, but only that 'the law on the missions and composition of the Central Organisation for Seizure and Confiscation (COIV), voted on 18 January 2018, provides that the COIV can manage confiscated virtual values'.[110] Apart

103 Article 504 *quater* Criminal Code mentions up to €100,000, which has to be multiplied by a factor of eight for criminal fines.

104 Article 39 *bis*, Law of 17 November 1808 on the Code of Criminal Procedure (Code of Criminal Procedure).

105 C Conings, 'Beslag op Bitcoins', *Computerrecht* 2015, 79.

106 On 2 March 2018, Mr Koen Metsu (NVA politician) asked several questions on virtual currencies in Belgium to the Minister of Justice, Koen Geens, including the quantity of Bitcoins that the government has confiscated since January 2015; this question has not yet been answered by the cabinet of Minister Koen Geens (Bulletin nN. B152, q. 2531).

107 Court of Appeal, Antwerp, 10 November 2016, not published.

108 These Bitcoins were confiscated in the course of the *Silk Road* investigation, see https://steemit.com/Bitcoin/@loryon/fbi-is-global-stakeholder-in-cryptocurrency-currently-owns-largest-Bitcoin-wallet.

109 See footnote 113.

110 Response by the Belgian Ministry of Justice dated 9 May 2018 to the questions asked by M Brecht Vermeulen (N-VA (New Flemish Alliance) politician) on 26 April 2018 (Bulletin No. B154, q. 2576).

from this new piece of legislation, it would also be possible to forfeit virtual currencies based on Article 28 *octies* and 61 *sexies*, Section 2 of the Code of Criminal Procedure, which allows the forfeiture of certain assets that are exchangeable (whose value can be easily determined) and whose retention would lead to value reduction.[111]

IX TAX

The number of cryptocurrency owners is drastically increasing, and it is estimated that around 20 million users own Bitcoins. Because of significant price fluctuations in particular, cryptocurrency owners might make considerable gains on their initial investment. For example, someone who bought one Bitcoin on 1 January 2017 at €950 and sold it for €11,050 on 31 December 2017 would have made a €10,100 gain. Cryptocurrencies raise important taxation issues, especially in relation to personal income tax and VAT.

i Personal income tax

Capital gains made by a Belgian resident from the sale of cryptocurrencies are not dealt with specifically in the Belgian Income Tax Code 1992. The existing rules allow the tax administration to tax cryptocurrency gains as either professional income (Article 23 Income Tax Code) or miscellaneous income (Article 90, 1°, Income Tax Code).

If a person's professional occupation is trading cryptocurrencies, the profits generated from this occupation will be taxed as professional income, and will therefore be subject to the progressive tax rates that range between 25 and 50 per cent in Belgium.[112]

If, to the contrary, a Belgian resident makes gains on cryptocurrency transactions outside of the scope of his or her professional activity, he or she will benefit from a tax exemption on those gains, but only on condition that the transaction is realised within the boundaries of the normal management of his or her private estate. Article 90, 1° of the Income Tax Code indeed provides for a general tax exemption for capital gains made on private assets of the taxpayer (which include securities or currencies, such as cryptocurrencies, as well as tangible assets and real estate) on condition that they result from the normal management of his or her private wealth. The question on whether a transaction is considered to be realised within that normal management is one based purely on facts. The Belgian courts generally describe normal management' as a conservative, risk-averse and unsophisticated management.

If gains resulting from cryptocurrency investments are made outside the scope of this normal management or derive from speculative transactions, they will be taxed as miscellaneous income, hence at a fixed rate of 33 per cent. It would probably be excessive to conclude that an investment in cryptocurrencies is always speculative because it is volatile, and as such, it implies a certain level of risk. The speculative nature of an investment in cryptocurrencies should always be assessed having regard to all the facts on a case-by-case basis. Indicators of speculation could be, for instance, the very short term of investments, the repetition of cryptocurrency transactions, the financing of the cryptocurrency investment

111 S Royer, 'Bitcoins in het Belgische strafrecht en strafprocesrecht', RW 2016–17, 26 November 2016, No. 13, 497.

112 Article 23 Income Tax Code: 'Professional income is income derived directly or indirectly from activities of every kind [and assimilated income], in particular: 1° profit; 2° benefits; 3° profits and benefits from a previous professional activity; 4° remunerations; 5° pensions, interest and allowances applicable as such'; Article 130 Belgian Income Tax Code lists the progressive tax rates between 25 and 50 per cent.

through loans or the investment of large sums of money (compared to the value of a Belgian resident's entire estate). On the other hand, if a Belgian resident invested a sum of €1,000 in cryptocurrencies and sold them five years later, making a big capital gain on this occasion, arguments could be put forward to sustain the notion that the transaction was made, as a good pater familias, within the boundaries of the general management of his or her private estate. Needless to say, situations are never as straightforward in practice.

As there is a large grey area between the speculative world and the normal management of a person's estate, in practice, taxpayers often apply for tax rulings to obtain legal certainty on the tax treatment of the gains made on their private assets (such as shares). The same applies for cryptocurrency gains. As a practical example, the Belgian Ruling Commission rendered a decision on 5 December 2017 regarding the tax treatment of the capital gains made by a student who developed a software application that automatically traded cryptocurrencies. The Ruling Commission held that the gains made from the sale of Bitcoins through a developed software application 'should not be considered as professional income within the meaning of Article 23 Belgian Income Tax Code but, in view of their speculative nature, are taxable as miscellaneous income within the meaning of Article 90(1) Belgian Income Tax Code'.[113] The Ruling Commission recently shed additional light on the tax treatment of cryptocurrency gains. It published a virtual currency questionnaire to be filled in by a taxpayer when he or she applies for a pre-filing request in relation to transfers of virtual currencies. The list contains 17 detailed and diverse questions, from the sum invested in virtual currencies to the frequency of the transactions and the current professional occupation of the taxpayer, as well as the reporting on social media of his or her activity on virtual currency groups.[114] From the answers provided by a taxpayer, the Ruling Commission will assess whether a cryptocurrency investment can be considered to have been made in the scope of the normal management of his or her private estate.

At this time, considering that the information on virtual currency acquisitions and trading activities can only be found online on a user's cryptocurrency exchange account or cryptocurrency wallet (instead of a bank account), the tax administration will most certainly encounter some practical difficulties in obtaining this information or assessing whether a taxpayer fully disclosed all the relevant information.

ii VAT

On 22 October 2015, the Court of Justice of the European Union (CJEU) rendered a judgment in response to a request from the Swedish Supreme Administrative Court seeking clarification on the question of whether transactions on an online virtual currency exchange platform to exchange a traditional currency for a Bitcoin virtual currency, or vice versa, were subject to VAT.

The CJEU first clarified that the exchange of different means of payments constitutes a supply of services (Article 24 VAT Directive).[115] Secondly, it stated that an

113 Anticipated decision by Ruling Commission No. 2017.852, 15/12/2017, news DVB 2018, p. 3, No. 1.3, available in Dutch, see https://www.ruling.be/sites/default/files/content/download/files/nieuwsbrief_dvb_3_nl.pdf.

114 https://www.ruling.be/sites/default/files/content/download/files/liste_de_questions_crypto-monnaies_0.pdf.

115 The CJEU first clarified that the exchange of different means of payments constitutes a supply of services within the meaning of Article 24 VAT Directive, since Bitcoins cannot be characterised as tangible property as referred to in Article 14 VAT Directive. The CJEU went on to recall that the supply of services is affected for consideration only if there is a direct link between the services supplied and the consideration received.

exchange transaction involving a Bitcoin constitutes a supply of services for consideration (Article 2(1)(c) VAT Directive).[116] Subsequently, it focused on the question of whether this supply of services for consideration could fall under one of the VAT exemptions. It held that the exemption in Article 135(1)(e) of the VAT Directive applied. According to the Court, this exemption for transactions involving currency, bank notes and coins used as legal tender also applies to non-traditional currencies. The Court emphasised that to interpret this provision as including only transactions involving traditional currencies would go against the context and aims of Article 135(1)(e) of the VAT Directive, because transactions involving non-traditional currencies that have been accepted by the parties to a transaction are also financial transactions. Applying this judgment to this case, the Bitcoin transaction has no other purpose than to be used as a means of payment.

In this decision, the CJEU paved the way for a positive future for Bitcoin purchases at Bitcoin exchanges in the European Union. Following this decision, Europeans can continue to buy Bitcoins using traditional currency without paying any VAT on these transactions.[117] Considering that VAT is an EU form of tax, any transactions involving virtual currencies should be treated in line with the CJEU's decision, including transactions carried out in Belgium. We hope that this approach will become adopted by countries outside the European Union, thereby further harmonising the taxation approach towards virtual currency transactions.

X OTHER ISSUES

Since the General Data Protection Regulation (GDPR)[118] entered into force, certain academics and commentators have emphasised the fundamental paradox between GDPR and blockchain technology. Whereas GDPR aims to protect EU citizens from privacy and data breaches, blockchain technology was designed so that data could be stored on a distributed ledger in an incorruptible way, and accessible for the public to see. The articulation of GDPR and blockchain technology raises several compatibility questions.

One question centres around certain data subject access rights. Pertaining to the right to be forgotten, the GDPR reads that 'the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her',[119] and the right to rectification, which reads that 'the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her'.[120] The question in this context is how can a person exercise these rights if his or her personal data is stored on a blockchain, since it is designed to be immutable? It is thus possible that personal data contained in smart contracts or virtual currency transactions cannot be erased or rectified, thereby violating the data subject's rights under the GDPR.

116 According to the CJEU, it is clear that the exchange of traditional currency for units of Bitcoin, in return for payment of a sum equal to the difference between the price paid by the operator to purchase the currency and the price at which he or she sells the currency to his or her clients, constituted a supply of services for consideration within the meaning of Article 2(1)(c) VAT Directive.

117 M Van Roey, C Bihain, 'European Court of Justice considers the exchange of traditional currencies for Bitcoins exempt from VAT', Stibbe ICT Newsletter, December 2015, No. 52, see https://www.stibbe.com.

118 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

119 Article 17 GDPR.

120 Article 16 GDPR.

A second question relates to personal data transfers to a place outside the European Economic Area (EEA). Article 44 of the GDPR states that personal data can only be transferred to a country outside the EEA if the rights under GDPR are safeguarded in that country. How can this obligation be complied with if virtual currency transactions using distributed ledger technology are to be verified by other users (nodes) that could be located outside the EEA, and the information on the blockchain can be accessed by anyone with an internet connection from anywhere in the world?[121]

Although both GDPR and blockchain technology are promising initiatives, certain obligations under GDPR could pose some challenges to companies deploying blockchain technology or to virtual currency companies. However, we are hopeful that the necessary (technical) solutions will be adopted in time to resolve these challenges.

XI LOOKING AHEAD

Whenever legal uncertainty hinders the development and adoption of legislation on virtual currencies, authorities and market regulators should provide the necessary clarification, or adopt new regulations that balance the rights and interests of all virtual currency market participants. As discussed throughout this chapter, the Belgian authorities have not (yet) implemented specific legislation on virtual currencies; nor did the FSMA provide clear guidance on how virtual currencies fit within existing legislation.[122]

It could be argued that this legislative inertia is attributable to the very limited interest that Belgian investors have shown regarding Bitcoin and other virtual currencies compared to investors in other fintech-friendly jurisdictions such as Switzerland and Germany. Nevertheless, this position is gradually changing considering the increasing number of parliamentary questions relating to virtual currencies that have been filed in recent years and that have been discussed in more detail throughout this chapter.[123]

Given the transnational nature of virtual currencies as a global phenomenon, we believe that virtual currencies are best regulated by transnational or international instruments. While the EU, through AMLD5, has already taken actions with regard to AML, initiatives on a broader scale are required. Virtual currencies were discussed in March 2018 by G20 members, and several reports have been commissioned. Some G20 countries even identified virtual currencies regulation as a priority for 2018, and this position was reaffirmed at the 2019 G20 summit in Japan.[124] Future regulatory actions regarding virtual currencies are thus to be expected and desired.[125]

121 See https://cryptobriefing.com/gdpr-vs-blockchain-technology-against-the-law/.

122 However, the FSMA issued a regulation prohibiting the sale of derivatives on virtual currencies. See Section II.iii or the following link: http://www.etaamb.be/fr/arrete-royal-du-24-avril-2014_n2014011323.html.

123 Those questions relate to, inter alia, taxation systems, the regulation of exchangers or criminal activities related to Bitcoins. See parliamentary questions No. 1856 (Bulletin No. B134); No. 2016 (Bulletin No. B145); No. 2531 (Bulletin No. B152); No. 2576 (Bulletin No. B154), see http://www.dekamer.be/.

124 https://cointelegraph.com/news/g20-leaders-reaffirm-position-on-cryptocurrencies-in-statement.

125 See https://www.independent.co.uk/life-style/gadgets-and-tech/news/Bitcoin-regulation-latest-south-korea-trading-ban-how-happen-price-what-happen-rise-drop-a8183136.html.

Chapter 6

BRAZIL

Fernando Mirandez Del Nero Gomes, Tiago Moreira Vieira Rocha, Alessandra Carolina Rossi Martins and Bruno Lorette Corrêa[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

i Introduction

The boom experienced in users' adoption of virtual currencies[2] has also reached the Brazilian market, which has given local law practitioners, legislators and regulators a lot to discuss. Traditionally, technology and business innovation comes ahead of regulation, and this is also proving to be the case with virtual currencies businesses.

The virtual currencies industry is both globalised and localised, and the growth of its ecosystem has given grounds for discussions that range from local mining activities to global exchanges, with services and products that defy the limits of banking, payment and capital markets laws and regulations on a daily basis. This is the case in Brazil.

The first official communication by the Brazilian Central Bank (the Central Bank) regarding virtual currencies occurred in 2014. In this statement, the Central Bank clearly stated that virtual currencies are not considered legal currency in Brazil, and thus would not be subject to Central Bank scrutiny. It also stated that although it would follow the development of this market closely, the volume of transactions was not yet large enough to pose a threat to the soundness of the Brazilian financial system.

The 2017 boom in the virtual currencies market brought virtual currencies back into the spotlight and resulted in the Central Bank and the Brazilian Securities Exchange Commission (CVM) releasing more comprehensive communications to the market stating their position regarding new virtual currencies businesses in light of the existing Brazilian laws and regulatory framework.

In parallel, the Brazilian Congress has started a series of public hearings to hear regulatory authorities, market players and specialists as part of discussions regarding a bill of law[3] aimed at regulating virtual currencies in Brazil.

ii Legal and regulatory framework applicable to virtual currencies

Although virtual currencies are capable of having the economic functionality traditionally attributed to currencies, they do not fall within the legal definition of a currency for the purposes of Brazilian law. The legal currency in Brazil is the real as provided by Decree-Law 857/69 and Law 10192/01.

---

1 Fernando Mirandez Del Nero Gomes is a partner, and Tiago Moreira Vieira Rocha, Alessandra Carolina Rossi Martins and Bruno Lorette Corrêa are associates, at Pinheiro Neto Advogados.

2 Also known as digital currencies or virtual currencies.

3 No. 2303/15.

According to Law 10192/01, all payment obligations enforceable in Brazil must be determined in reais, and all agreements or other documents that in any form constrain or refuse the use of the legal currency are void. These provisions are referred to as the 'legal course' of the real.

As a result, despite being able to be used as a means to carry out exchanges, a unit for the purposes of accountancy or even as reserve of value, virtual currencies do not have legal course, and therefore do not fall within the legal definition of legal currency.

Considering that virtual currencies are not currency in Brazil, they are generally classified as assets subject to the general regimen established by the Civil Code.[4]

Nevertheless, similarly to most jurisdictions, the legal treatment of virtual currencies in Brazil may vary according to the intrinsic characteristics of each virtual currency, including its purpose and usage, existence of remuneration, and distribution and issuance methods. Thus, a given virtual currency may end up being subject to certain banking and securities laws and regulations. To fully and properly understand the legal and regulatory framework that may apply to virtual currencies, it is important to have a general overview of the banking and securities legal and regulatory framework existing in Brazil.

iii General overview of the banking and securities legal and regulatory framework

General aspects of the Brazilian financial system

The basic legal framework of the financial system is provided by the Brazilian Constitution of 1988[5] along with the Banking Law.[6]

The Banking Law, although dated prior to the Constitution, remains the main law establishing the current format of the financial system, and sets forth the ground rules for its infrastructure and regulatory framework.

It assigns the authority to regulate and oversee local financial institutions, defines the regulatory policy of the Brazilian Monetary Council (CMN) and created the Central Bank. In addition to the CMN and the Central Bank, the financial system is also composed of the national council of private insurance, the private insurance authority and the CVM, which are subject to specific legal diplomas. Other laws complement the legal framework applicable to the financial system, among which are the Capital Markets Law,[7] the Securities Law,[8] the Anti-Money Laundering Law[9] and the E-payments Law.[10]

In 2013, the enactment of the E-payments Law enlarged the scope of the regulatory authority of the CMN and Central Bank. The E-payments Law was enacted to regulate the industry of electronic payments in Brazil by bringing the CMN and Central Bank's scope of oversight to the rendering of payment services in the context of the Brazilian payments system. The E-payments Law sets the ground rules of the regulatory framework applicable to payment arrangements (i.e., the set of rules governing a payment scheme, such as credit or debit card transactions) and payment agents (i.e., any agent that issues a payment instrument or acquires a merchant for payment acceptance).

4 Law 10406/02.

5 Article 192 of the Federal Constitution of 1988, as amended.

6 Federal Law 4595/64.

7 Law 4728/65.

8 Law 6385/76.

9 Law 9613/98.

10 Law 12865/13.

General aspects of the Brazilian banking and e-payment system

The banking system is highly regulated. The main piece of legislation is the Banking Law, which places the CMN as the highest authority in the financial system. It is responsible for establishing the monetary and financial policies in Brazil, and is in charge of the overall supervision of the Brazilian monetary, credit, budgetary, fiscal and public debt policies, as well as operating the Brazilian payments system (SPB).

The primary objectives of the CMN's policies are to:

a adjust the monetary supply to the needs of the Brazilian economy and its development process;

b regulate the domestic value of the real to prevent or correct inflationary or deflationary trends of internal or external origin, economic depressions or other imbalances arising from sudden events;

c regulate the value of the real outside of Brazil and regulate the Brazil's balance of payments to make better use of foreign currency resources;

d improve the quality of the resources of financial institutions and of financial instruments so as to make the payments system and the mobility of funds more efficient; and

e monitor the liquidity and solvency of financial institutions and payment institutions.

The Central Bank is responsible for implementing the monetary and credit policies established by the CMN, as well as to regulate public and private financial institutions per se, payment arrangements, payment arrangements institutors and payment institutions, applying, when needed, the sanctions stipulated in the rules applicable to such entities. It is also responsible, among other activities, for exercising control over credit and foreign capital, receiving mandatory payments and voluntary demand deposits made by financial institutions, engaging in rediscount transactions and providing loans to financial institutions, and exercising the function of a depository of official gold and foreign currency reserves.

In this sense, the CMN is responsible for regulating the criteria for the organisation, operation and inspection of financial institutions and payment arrangements and agents, while the Central Bank is responsible for effectively authorising the operations of financial institutions in Brazil and supervising their activities.

The regulatory authority of the CMN is exercised by the issuance of resolutions creating the basic regulatory framework applicable to financial institutions as per the mandate and pursuant to the limits provided by the Banking Law and E-Payments Law. The Central Bank, in its role as the regulatory and supervising authority, issues regulations aimed at implementing CMN resolutions. While CMN resolutions set the policies and guidelines for the financial and payments systems, Central Bank regulations serve to establish the technical details for implementation of CMN resolutions.

General aspects of the Brazilian capital markets

The Brazilian capital markets system is also highly regulated. The main piece of legislation is the Capital Markets Law, which created the CVM, and the Securities Law, which establishes the scope of the CMN and the Central Bank in the capital markets.

The CVM is responsible for regulating, supervising and inspecting the securities market and its participants. It is also responsible, among other things, for overseeing the exchange and organised over-the-counter markets, publicly-held corporations, the commodities,

futures, derivatives and securities markets, and the intermediation and custody of such assets. Its regulatory authority also extends to banks engaged in investment banking and securities activities, and to other participants in the securities market.

The regulatory authority of the CVM is exercised by the issuance of rulings and opinions that are binding on participants in the securities market and any parties involved in transactions involving securities. There are also some CMN resolutions and Central Bank regulations that apply to financial institutions and other specific capital markets participants subject to such authorities' oversight.

II SECURITIES AND INVESTMENT LAWS

Discussions on the treatment of virtual currencies in light of the Capital Markets Law and the potential characterisation of virtual currencies as securities in Brazil have gained relevance owing to the growth in interest in virtual currencies and other virtual assets throughout 2017, especially in initial coin offerings (ICOs).

ICOs consist of making an offer to the public of virtual currencies or virtual assets (financial or otherwise). The market has conventionally named these tokens or coins, as they are created within a blockchain or distributed ledger technology.

Virtual currencies offered through an ICO may represent any type of asset or instrument, from a share to a feature to access a certain platform. In this sense, as mentioned above, a given virtual currency may be subject to a specific legal and regulatory framework depending on the intrinsic characteristics of each virtual currency, including its purpose and usage, existence of remuneration, and distribution and issuance methods. If a new virtual currency created in the scope of an ICO has characteristics that match the requirements to classify as a security in Brazil, it will be subject to the Brazilian capital markets legal and regulatory framework.

In light of the growth in the number of ICOs in 2017, the CVM published two notices to the market confirming that any given virtual currency may or not be subject to the Capital Markets Law and CVM regulatory framework and scrutiny depending on whether or not it is classified as a security in light of the concept of security provided by the Capital Markets Law, and the analysis should be made on a case-by-case basis.

The concept of securities under the Capital Markets Law is composed of a list of instruments that expressly classify as securities under Brazilian law:

a shares, debentures and subscription bonus;
b coupons, rights, subscription receipts and certificates of unfolding of coupons, rights and subscription receipts;
c certificates of deposit of securities;
d debenture notes;
e quotas of investment funds in securities or investment clubs in any assets;
f commercial notes;
g futures, options and other derivative contracts, which underlying assets are securities;
h other derivative contracts, regardless of the underlying assets; and
i when publicly offered, any other securities or collective investment contracts that generate share, partnership or remuneration rights, including those resulting from the provision of services, whose income comes from the efforts of the entrepreneur or third parties.

Along with the list of instruments that are expressly considered securities (listed in points (a) to (h) above), the Capital Markets Law also provides an open-ended definition whereby any collective investment contracts that are open to public offering, generate a share, partnership or remuneration right, and whose income results from the efforts of the entrepreneur or third parties, are considered a security.

Thus, it is indeed possible to characterise some virtual currencies as securities under the terms of the Capital Markets Law depending on the economic context of its issuance and the rights conferred on investors.

In cases where a virtual currency is classified as a security in Brazil, an ICO for issuance of this virtual currency will be subject to the legal treatment of public offerings of securities in Brazil.

The main concern of the CVM is to ensure that the issuance and public offering of these securities (i.e., their large-scale offering) is carried out in a manner that ensures that the investors concerned are properly educated about the potential risks and benefits involved. Therefore, as a general rule, the public offering of securities depends on the registration by the issuer of the securities offered at the CVM, registration of the offer with the CVM and completion of the public offering through an intermediary authorised by the CVM (investment bank or others).

Public offerings of securities are currently carried out under the general public offerings regimen set forth by CVM Ruling 400/03, which requires the registration of an offer with the CVM, as mentioned above. Alternatively, public offerings of securities may be carried out under the specific regimen set forth by CVM Ruling 476/09 for offerings with restricted efforts (that is, a direct offering to a limited number of qualified investors) and the specific regimen set forth for investment crowdfunding in CVM Ruling 588/17. In both cases, the offerings do not require prior registration with the CVM but are subject to specific limitations.

Additionally, the CVM has issued specific opinions dealing with offerings of securities using the internet that occurred abroad whereby the authority has stated that an offering made using the internet is generally considered public, and that even if a certain public offering occurs abroad, in cases where it targets Brazilian investors it will be subject to Brazilian capital markets laws and regulation. In this sense, an ICO is for all purposes a public offering as it uses the internet as the main distribution method, and even if the public offering is occurring elsewhere, it should observe Brazilian capital markets laws and regulation if Brazilian investors are targeted.

As a result, the CVM may administer the applicable sanctions and penalties in the event of offers of virtual currencies that fit the definition of security in disregard of the capital markets applicable regulation, an understanding that has already been publicly confirmed by the CVM.

The same applies to the trading rules. Securities may only be traded in markets authorised by the CVM (stock exchanges and over-the-counter markets) and, therefore, virtual currencies that are classified as securities can only be traded in such markets, being prevented from listing in non-regulated environments: that is, virtual currency exchanges (see Section V).

In early 2019, the CVM published a new internal regulation modifying its rule-making process. Among the main changes are the introduction of a phase for assessment of the regulatory impact as a means to consider the cost-effectiveness of a proposed rule and the possibility of introducing a regulatory sandbox phase through issuance of temporary rules for empirical testing of their adequacy to market requirements. In line with the discussions

between the CVM and the market in the past couple of years, the new rule-making process allows for the creation of an experimental regulatory environment where temporary regulatory instruments may be issued to empirically assess the benefits and most suitable procedures to implement a recommended solution. This experimental environment, commonly known as a regulatory sandbox, will enable the regulator to test, individually and for a limited period, regulatory changes that, owing to their features and according to the CVM Board, justify a trial environment, avoiding additional risks to the national financial system or to investors' protection. Security tokens issuances are among the first projects expected to receive this treatment and are aligned with the efforts of the regulators to foster innovation in Brazil's financial and capital markets.

III BANKING AND MONEY TRANSMISSION

i Electronic currencies

The regulation enacted by the CMN and the Central Bank under the regulatory powers attributed to them by the E-payments Law created the concept of electronic currency in the legal and regulatory framework. An electronic currency is an electronic representation of reais transferred by the user of the payment services to the entity responsible for the issuance and management of the electronic currency – the payment institution. Such funds are stored in an electronic account in the name of the user, and might be utilised for payments or transfers among users or with third parties accredited to receive the electronic currency. The user legally owns the electronic currency and may request the withdrawal of the amount at any time.

Payment institutions' issuers of electronic currencies are required to join a payment arrangement (or establish their own) and request the Central Bank approval to operate. The payment arrangement is the set of rules governing the payment scheme (including the fee structure), and its establishment is carried out by a payment arranger who is also a regulated entity and required to request Central Bank approval to operate.

The regulatory concept of electronic currency was created to cover all prepaid cards issued in Brazil and mainly used for the acquisition of goods with merchants. Nevertheless, given the broad concept of electronic currency as established by the E-payments Law and regulation, it encompasses all kinds of electronic currency directly related to the real. In other words, the E-payments Law will apply to all electronic currencies that mimic the real. Virtual currencies do not fall into this definition and, therefore, are not considered electronic currencies for the purposes of the E-payments Law and its related regulation.

In this sense, the Central Bank issued a communication in 2014, following the enactment of the E-payments Law and at a moment when virtual currencies were not so largely adopted, clarifying and confirming that virtual currencies are different from the electronic currencies concept created by the E-payments Law and related CMN and Central Bank rules. This position was further confirmed in 2017 when the Central Bank issued additional communications to the market restating its position owing to relevant increase in the number of transactions and businesses involving virtual currencies.

ii Foreign exchange transactions and remittances

The Brazilian foreign exchange rules are generally strict, and the foreign exchange laws and regulation thereof still reflect the government's historic concern with foreign exchange

controls, which have been relaxed over the past decade but that still impose a significant hurdle to foreign currency flows. The foreign exchange market and transactions are subject to Central Bank oversight and regulation, as established in the Banking Law and Law 4131/64.

Remittances of funds from abroad to Brazil and vice versa can only be made through financial institutions authorised to operate in the foreign exchange market. In other words, Brazilians can purchase and sell foreign currencies or perform international transfers in reais of any nature, without limitation of amount, on the condition that the counterparty in the operation is an agent authorised to operate in the foreign exchange market, subject to the legality of the transaction and based on economic grounds and responsibilities defined in the related documentation. These rules set out the principles to be observed by banks and agents authorised to operate in the foreign exchange market in each and every transaction.

Pursuant to Decree-Law 23258/33 and Law 7492/86, a foreign exchange transaction carried out without the intermediation of an authorised intermediary is considered a financial crime characterised as the execution of an illegal foreign exchange transaction subject to the penalty of imprisonment from two to six years plus a fine.

In this context, the remittance of funds from Brazil to abroad for the acquisition of virtual currencies is not prohibited, provided that the flow of funds occurs through the appropriate channels by means of an foreign exchange transaction entered into with an authorised agent.

Remittances of funds from abroad to Brazil and vice versa can only be made for specific purposes expressly set forth in the regulation. Each purpose has a corresponding nature (or code) that must be indicated in the corresponding foreign exchange agreements. Brazilian exchange regulations do not specify objective criteria for the characterisation of foreign exchange transactions under a specific nature, and a local agent will request from its clients and keep in its files the documents evidencing that the transaction is legal and corresponds to the specific purpose indicated by the client. The remittance of funds from abroad to Brazil and vice versa not in compliance with this rule is also subject to administrative fines.

Despite the above-mentioned requirements, currently the Central Bank regulation does not provide a specific nature for transactions involving virtual currencies, and remittances must be analysed on a case-by-case basis to determine the most appropriate classification.

IV ANTI-MONEY LAUNDERING

The prevention of money laundering, terrorist financing and similar crimes is among the main concerns regarding the adoption of virtual currencies on a global scale, and it has received the dedicated attention of the Brazilian authorities. Currently, there is no law or regulation in force in the Brazilian legal system that sets forth the specific regimen for the prevention of money laundering in businesses and transactions involving virtual currencies.

The criminalisation of money laundering in Brazil was verified upon the enactment of the Anti-Money Laundering Law, which sets forth not only the definitions, requirements and sanctions of the matter, but also creates the basis for a local legal framework bound for the prevention of money laundering crimes in Brazil. It also establishes a preventive control mechanism for all commercial and financial transactions to restrain the practice of using certain sectors of the economy as a conduit for recycling illegal gains. This preventive control mechanism, however, applies only to a limited range of legal entities and individuals based on the involvement of such persons in certain activities (either as a main or ancillary activity).

Nevertheless, depending on the type of business and transaction carried out involving virtual currencies, it is possible to adopt a conservative interpretation of the Anti-Money Laundering Law and establish its application for the specific business or transaction. This is the case for the activities practiced by virtual currency exchanges, which, although not expressly included in the roll provided by the Anti-Money Laundering Law, may be considered as subject to its provisions due to its ancillary activities.

In this sense, over the past few years, several government bodies and representatives under the National Initiative for Fighting Corruption and Money Laundering have discussed the implications of the usage of virtual currencies and electronic payment methods for the prevention of money laundering. In parallel, as part of the discussions regarding Bill of Law 2303/15 in Congress, the benefits of amending the Anti-Money Laundering Law to include entities that operate with virtual currencies in the roll of activities expressly subject to this Law is one of the recurring topics.

In any case, market practice most generally adopted in Brazil has been enacting sound anti-money laundering mechanisms and safeguards, especially by virtual currency exchanges.

i General overview of the Anti-Money Laundering Law and related regulation

As mentioned above, the Anti-Money Laundering Law also establishes a preventive control mechanism for all commercial and financial transactions to curb the practice of using certain sectors of the economy as conduits for recycling illegal gains. This Law also created a special agency, the Financial Activities Surveillance Committee (COAF), which is linked to the Ministry of Finance, and is responsible for regulating, imposing administrative penalties, and receiving, reviewing and identifying the suspected occurrence of illicit activities under the Anti-Money Laundering Law, without prejudice to the spheres of authority of other agencies and authorities.

In this regard, the Anti-Money Laundering Law determines that the entities subject to its regimen are bound by the following obligations:

a client identification and record keeping: to properly identify clients and adopt adequate and updated record-keeping systems for such client information, and to keep records of transactions that meet certain thresholds determined by law or the competent regulatory agencies, or both;[11]

b monitoring of transactions: to afford special attention to transactions that, given the involved parties, the amounts, the nature, the instruments used or the lack of legal or economic reason, may serve as substantial indicia of the crimes set forth in or related to the Anti-Money Laundering Law (suspicious transactions); [12]

c transaction reporting: to report to COAF within 24 hours, without making this fact known to clients, all transactions that exceed thresholds established by local authorities; and any proposals or transactions that are considered by a given institution as suspicious transactions. Reports are made electronically through a system called Siscoaf, which is available on COAF's website; and

11 The Anti-Money Laundering Law transferred to the duly empowered authorities (e.g., the Central Bank) the responsibility for defining such thresholds.

12 The Anti-Money Laundering Law also transferred to the duly empowered authorities (e.g., the Central Bank), the responsibility for listing these suspicious transactions.

d internal controls: to adopt internal policies and procedures consistent with an institution's size and transactions volume, and to adequately comply with the anti-money laundering legal requirements.

If the above-mentioned obligations and requirements are not observed, in addition to any other penalties that may apply, including in the criminal, administrative and civil law spheres, a virtual currency exchange and its managers may be subject to penalties including warnings, monetary fines, or temporary or indefinite suspension or cancellation of the authorisation to operate, depending on the seriousness of the breach.

The Anti-Money Laundering Law also sets forth the ground rules for the criminalisation of money laundering in Brazil, which include not only definitions, requirements and sanctions on the matter, but also create the basis for a local legal framework for the prevention of money laundering crimes in Brazil. Individuals involved in such crimes are subject to the penalty of imprisonment from three to 10 years plus a fine.

V REGULATION OF EXCHANGES

Until 2017, two virtual currency exchanges accounted for more than 50 per cent of the market share in Brazil. However, the boom in the virtual currencies market in 2017 resulted in the creation of multiple new virtual currencies exchanges business and products, and the number of virtual currency exchanges operating in Brazil jumped from 15 to 28 from December 2017 to August 2018, an increase of 86 per cent.[13] In addition, in August 2018 the third-largest virtual currency exchange announced its entrance in the Brazilian market.

The growth in users' adoption of virtual currencies is not the only factor contributing to this increase. The light regulatory requirements to operate a virtual currency exchange in Brazil have also contributed to attract new players to this market.

The activities practised by virtual currency exchanges consist of the development and administration of platforms that enable their clients to buy, sell and trade virtual currencies among themselves.

The regulation that will apply to these platforms depends on the type of virtual currency the exchanges will list for acquisition, sale and trading by users.

As mentioned above, in cases where the virtual currencies listed in a given exchange are classified as securities as provided by the Capital Markets Law, they can only be traded in stock exchanges or over-the-counter markets authorised by the CVM.

On the other hand, virtual currencies that do not fit into the concept of securities are not subject to such rules, as is the case of Bitcoins, the virtual currency with the largest trading volume in Brazil. These assets can be traded in non-regulated environments. Thus, a virtual currency exchange that lists only virtual currencies that do not fit into the concept of securities will not be subject to the capital markets rules.

In addition to the development of a platform for buying, selling and trading of virtual currencies, many virtual currency exchanges end up providing ancillary services to their customers. These ancillary services are intended to enable clients to carry out transactions on a platform in a more efficient way with immediate settlement of the transactions.

13 Radar Fintechlab Brazil, August 2018.

The most common ancillary service is the custody of virtual currencies of clients in virtual portfolios in the name of the clients. The custody of virtual currencies is also not a regulated activity; therefore, it is subject to the general legal regimen established by the Civil Code for the custody of assets.

The second most common ancillary service is the provision of prepaid accounts in reais to clients (as a payment institution). Prepaid accounts allow clients to contribute reais to those accounts that, once converted into electronic currency, can be used to execute transactions on the platform (such as for payments for acquisitions of virtual currencies). This service is provided by a virtual currency exchange by acting as a payment institution issuer of electronic currencies and operating its own payment arrangement with the purpose of enabling transactions in the platform.

A prepaid account, pursuant to the Central Bank regulation, is an account destined for the execution of payment transactions in an electronic currency based on funds contributed to the account in advance.[14] In this sense, the E-payments Law and related regulation establish that an institution responsible for the management of prepaid payment accounts, the availability of payment transactions based on an electronic currency contributed into those accounts, and the conversion of those funds into physical or book entry currency or vice versa, is considered a payment institution, and subject to the Law and regulation.

Payment institutions that participate in payment arrangements that integrate with the SPB depend on Central Bank authorisation to operate once they reach certain volume triggers. This requirement does not apply in cases where a payment institution participates only in limited purpose payment arrangements.[15]

Thus, a virtual currency exchange that operates as a payment institution issuer of electronic currencies may be subject to authorisation from the Central Bank to operate depending on the type of payment arrangement that it participates in. This requirement, however, results from the operation of prepaid accounts in reais and is not related to virtual portfolios of virtual currencies, or to any of the services and operations of a platform that involve exclusively virtual currencies.

VI REGULATION OF MINERS

Mining activity is not regulated in Brazil. Mining activities have mostly been explored in the south of Brazil, where mining farms have been established close to the Itaipú hydroelectric power plant (although it is very common to see Brazilian miners setting up in neighbouring countries such as Paraguay). The main concerns regarding mining activities are related to the receipt of virtual currencies as payment for mining owing to anti-money laundering issues (see Section IV).

14 Circular 3680/13 issued by the Central Bank, as amended, defines pre-paid payment accounts as those 'intended to perform payment transactions with electronic currency based on funds in Brazilian currency transferred onto such account in advance'.

15 Circular 3682/13 issued by the Central Bank, as amended, lists examples of limited purpose payment arrangements, which are those whose instruments are accepted only at the network of establishments of one same business company, even if not issued by it; accepted only at the network of establishments that clearly display the same visual identity among them, such as franchisees and fuel station networks; and intended for payment of specific public utility services, such as public transport and public telephony.

In spite of the fact that mining activities are not regulated, the public offering and sale of quotes of investment in mining farms are considered a public offering of a collective investment agreement that would generate share, partnership or remuneration rights, and that would fit into the definition of securities subject to the Capital Markets Law (see Section II).

VII REGULATION OF ISSUERS AND SPONSORS

The legal and regulatory framework applicable to issuers and sponsors of virtual currencies depends on the legal and regulatory regimen applicable to virtual currencies. Issuers and sponsors of virtual currencies that are subject to the general assets regimen are not also subject to any specific regulation.

However, in the case of virtual currencies that fit within the definition of virtual currencies under the Capital Markets Law referred to in Section II, the issuers or sponsors of the virtual currencies will also be subject to the Capital Markets Law, including the requirement of registration as an issuer of securities with the CVM, pursuant to the terms of CVM Ruling 480/09.

CVM Ruling 480/09 establishes the terms for registration of companies as Class A or Class B issuers of securities, depending on the type of security issued, which includes an authorisation for the issuance of shares in the case of Class A issuers that does not apply to Class B issuers. CVM Ruling 480/09 also sets forth the procedures for the registration of foreign issuers with the CVM.

VIII TAX

The Brazilian tax legislation has no legal provision governing the taxation of virtual currencies, and the lack of proper regulation may lead to uncertainties regarding compliance with certain tax obligations.

Despite that, the tax authorities have included two comments in their annual Income Tax of Individuals Q&A, establishing that:

a although virtual currencies are not considered currencies under the current regulatory framework, they must be declared in income tax statements in assets records, as they can be equated to financial assets. A virtual currency must be declared at its acquisition cost; and

b the capital gains ascertained on the sale of virtual currencies are subject to income tax.

In this sense, transactions with virtual currencies are subject to the same taxation as transactions with different classes of assets. This means that: (1) the revenue generated from the settlement in virtual currency is regularly subject to taxation; (2) an entity that settles an obligation with the use of virtual currencies should proceed with the withholding of the applicable taxes; and (3) capital gains ascertained with the sale of a virtual currency are subject to income tax.

The applicable income tax rate on the capital gains from transactions with virtual currencies for Brazilian individuals is determined as follows:

a capital gains not exceeding 5 million reais are subject to income tax at a rate of 15 per cent;

b capital gains that exceed 5 million reais but do not exceed 10 million reais are subject to income tax at a rate of 17.5 per cent;

c capital gains that exceed 10 million reais but do not exceed 30 million reais are subject to income tax at a rate of 20 per cent; and

d capital gains exceeding 30 million reais are subject to income tax at a rate of 22.5 per cent.

The capital gains earned by individuals on the sale of small value goods (i.e., virtual currency), whose unit price (or the value of all assets sold in the month) is equal to or less than 35,000 reais is exempt from income tax.

Given some particularities of virtual currency technology, there are still debates on the applicable tax treatment in some specific situations, for instance, whether the swap of a virtual currency for another virtual currency is a taxable event; the tax treatment of virtual currencies received by means of a hard fork,[16] the criteria for accounting a virtual currency in the balance sheet of local companies and the taxation on the variations of the price of the virtual currency.

Recently, with the purpose of obtaining information on transactions carried out with virtual currencies, the Brazilian Internal Revenue Services (RFB) published Normative Ruling No. 1.888/2019, which creates a specific tax ancillary obligation related to virtual currencies transactions.

Under the new regulation, information on the transactions with virtual currencies must be reported to the authorities: (1) by Brazilian cryptocurrency exchanges, with respect to the transactions carried out on their platform; or (2) by the individuals or legal entities holding virtual currencies, when the transactions exceed the monthly amount of 30,000 reais and take place off an exchange or through a foreign exchange.

The RFB's definition of virtual currencies is quite broad as it encompasses any digital representation of value. Therefore, the reporting obligation involves transactions with currencies, utility tokens and other assets similar to securities.

The report must contain information on the date, type and parties to the transaction, the virtual currencies used, the quantity of virtual currencies traded, the transaction value in reais, the value of service fees, and the wallet address for sending and receiving virtual currencies.

The information must be reported to the RFB every month – the first set of information will be delivered in September 2019 with respect to transactions held in August 2019. In addition, Brazilian exchanges must also provide information every year about the balance of virtual currencies held by each of the customers, with their position as of December 31.

The RFB's normative ruling also foresees the levy of a 3 per cent fine on the value of the transactions if the information reported is inaccurate, incomplete or incorrect. This percentage is reduced to 1.5 per cent of the transaction value if the declarant is an individual.

IX OTHER ISSUES

i Data protection rules

In mid-August 2018, Brazil enacted the General Data Protection Act (GDPA), and it will be effective within 18 months. The GPDA brings extensive changes to the processing of

16 Bitcoin: 'A permanent divergence in the block chain, commonly occurs when non-upgraded nodes can't validate blocks created by upgraded nodes that follow newer consensus rules.'

personal data in Brazil, including rules for processing, storage, use and transfer of personal data, as well as specific rules for the transferring of data abroad, and will impact activities of both Brazilian and foreign companies with a linkage in Brazil as well as digital platforms that operate in Brazil. Businesses and transactions involving virtual currencies are not excluded from its scope of application, and will therefore be impacted by the GDPA.

ii Consumer protection rules

Unlike other jurisdictions, Brazilian law does provide a definition of consumer, and the existence of a consumer relationship and, therefore, the application of the provisions of the Consumer Protection Code, are identified when there is a supplier supplying a product or providing a service under a contract, and an end user using the product or service. Therefore, the relationship between providers of solutions involving virtual currencies and their clients may be subject to the Brazilian consumer protection legal and regulatory framework, and especially the Consumer Protection Code.[17]

X LOOKING AHEAD

The adoption of virtual currencies in Brazil has increased significantly over the past 12 months, and the entrance of new players is expected to give an additional boost. The increase in the market cap of transactions with virtual currencies and the development of new businesses are also likely to draw the attention of Brazilian legislators and regulatory authorities.

Therefore, it is expected that the public hearings and discussions regarding Bill of Law 2303/15 will intensify, and that the Central Bank and the CVM will look more closely at transactions and new products involving virtual currencies, and especially those that push the limits of the banking and capital markets regulations, such as investment fund structures, derivatives and ICOs of virtual currencies classified as securities.

17 Law 8078/90.

Chapter 7

CANADA

Alix d'Anglejan-Chatillon, Ramandeep K Grewal, Éric Lévesque and Christian Vieira[1]

I SECURITIES AND INVESTMENT LAWS

Securities regulation in Canada is primarily a matter of provincial jurisdiction. While each province and territory has its own rules and securities regulators, the securities regulatory framework is largely streamlined and harmonised across Canada, with certain provincial or regional variances.[2] However, legislative jurisdiction in the area of derivatives is divided between the federal and provincial governments, and the harmonisation of rule-making in this area has been more elusive.

Generally, the two basic purposes of the securities laws are to provide protection from unfair, improper or fraudulent practices, and to foster fair and efficient capital markets, and confidence in those capital markets.[3] Securities regulation in Canada generally governs the distribution and trading of both securities and derivatives. The distribution and trading of securities and derivatives is primarily regulated through the imposition of prospectus requirements, dealer, adviser and investment fund manager registration requirements, and certain requirements imposed upon those operating exchanges, alternative trading facilities or other marketplaces that facilitate their trading.

The Canadian Securities Administrators (CSA) is an umbrella organisation of Canada's provincial and territorial securities regulators whose objective is to improve, coordinate and harmonise regulation of the Canadian capital markets. While Canadian securities regulators have not yet formulated any definitive regulations, the CSA has published two staff notices with respect to virtual currencies with a view to being responsive to the evolving activity related to virtual currencies: Staff Notice 46-307 – Cryptocurrency Offerings[4] and Staff Notice 46-308 – Securities Law Implications for Offerings of Tokens.[5] More recently, the CSA and Investment Industry Regulatory Organization of Canada (IIROC) also published a more comprehensive joint consultation paper[6] (the Consultation Paper) seeking input on various

1 Alix d'Anglejan-Chatillon, Ramandeep K Grewal and Éric Lévesque are partners and Christian Vieira is an associate at Stikeman Elliott LLP.

2 While the province of Quebec has a separate Derivatives Act that regulates over-the-counter and exchange-traded derivatives, derivatives regulation in the remaining provinces is governed by the securities and, in certain provinces, commodities futures legislation.

3 Securities Act, R.S.O. 1990, c. S.5, s. 1.1.

4 Canadian Securities Administrators, Staff Notice 46-307 – Cryptocurrency Offerings (2017), 40 OSCB 7231. (Canadian Securities Administrators, 2017).

5 Canadian Securities Administrators, Staff Notice 46-308 – Securities Law Implications for Offerings of Tokens (Canadian Securities Administrators, 2018).

6 Canadian Securities Administrators and Investment Industry Regulatory Organization of Canada, Consultation Paper 21-402 – Proposed Framework for Crypto-Asset Trading Platforms (Canadian

considerations relating to the potential regulation of virtual currencies. The Staff Notices are intended to provide guidance to industry participants on the applicability of securities laws to virtual currencies and, together with the Consultation Paper, are the primary basis for the discussion that follows.

i Applicability of Canadian securities laws to virtual currencies

Virtual currencies may be subject to Canadian provincial securities laws to the extent that a virtual currency is considered a security or a derivative for the purposes of such laws, such as the Securities Act (Ontario). The Securities Act defines a security to include, among other things, an investment contract. The seminal case in Canada for determining whether an investment contract exists is *Pacific Coast Coin Exchange v. Ontario (Securities Commission)*,[7] where the Supreme Court of Canada identified the four central attributes of an investment contract, namely:

a an investment of money;
b in a common enterprise;
c with the expectation of profit; and
d which profit is to be derived in significant measure from the efforts of others.

If an instrument satisfies the *Pacific Coin* test, it will be considered an investment contract and, therefore, a security under Canadian securities laws.

The application of the *Pacific Coin* test to virtual currencies is not always straightforward, however. Industry participants have taken the position that utility tokens, which have a specific function or utility beyond the mere expectation of profit (such as providing their holders with the ability to acquire products or services) should not be considered securities.[8] This position appears to have been accepted by the CSA and IIROC in the Consultation Paper, in which it was acknowledged that proper utility tokens may not be securities. However, the CSA has also noted that most of the offerings of virtual currencies purporting to be utility tokens that its staff had reviewed involved the distribution of a security, usually in the form of an investment contract.[9]

The CSA and IIROC have also acknowledged that it is widely accepted that some of the well-established virtual currency assets that function as a form of payment or means of exchange on a decentralised network, such as Bitcoin, are not currently in and of themselves, securities or derivatives and have features that are analogous to commodities such as currencies and precious metals.[10] The regulators have cautioned, however, that securities law requirements may still apply to platforms that offer trading of virtual currencies that are neither securities nor derivatives where the arrangement, when viewed as a whole, including the investor's contractual rights and how they relate to the manner in which the virtual currency is transacted, among other things, is sufficient to constitute an investment contract.[11]

Securities Administrators and Investment Industry Regulatory Organization of Canada, 2019) (the Consultation Paper).

7 *Pacific Coast Coin Exchange v. Ontario (Securities Commission)*, [1978] 2 SCR 112.

8 ibid., footnote 5.

9 ibid., footnote 6.

10 ibid., footnote 6.

11 ibid., footnote 6.

In assessing whether a particular virtual currency will be considered a security subject to Canadian securities laws, the CSA will consider the substance of the virtual currency over its form.[12] The CSA has outlined a number of considerations in determining whether an investment contract exists. While no single factor is determinative, the CSA has stated that the existence of some or all of the following circumstances may cause a virtual currency to be considered an investment contract:[13]

a the underlying blockchain technology or platform has not been fully developed;
b the token is immediately delivered to each purchaser;
c the stated purpose of the offering is to raise capital, which will be used to perform key actions that will support the value of the token or the issuer's business;
d the issuer is offering benefits to persons who promote the offering;
e the issuer's management retains a significant number of unsold tokens;
f the token is sold in a quantity far greater than any purchaser is likely to be able to use;
g the issuer suggests that the tokens will be used as a currency or have utility beyond its own platform, but neither of these things is the case at the time the statement is made;
h management represents or makes other statements suggesting that the tokens will increase in value;
i the token does not have a fixed value on the platform;
j the number of tokens issuable is finite or there is a reasonable expectation that access to new tokens will be limited in the future;
k the token is fungible;
l the tokens are distributed for a monetary price; and
m the token may be reasonably expected to trade on a trading platform or otherwise be tradeable in the secondary market.

A particular virtual currency that meets the criteria of the *Pacific Coin* test or has certain of the characteristics described in the CSA guidance discussed above may be properly considered an investment contract and therefore a security, subject to Canadian securities laws.

ii Virtual currency offerings in Canada

Canadian securities laws generally require the filing of a prospectus to qualify any distribution of securities. No person or company may trade in a security where the trade constitutes a distribution unless a prospectus has been filed or the trade is made in reliance upon a prospectus exemption. Securities originally distributed under a prospectus exemption are generally subject to resale restrictions that require the issuer to have been a reporting issuer (i.e., a public company) for a specified period of time and, in some cases, that the securities be held for a specified period of time. To the extent that a virtual currency is considered a security or a derivative, the issuance or distribution to the public is subject to prospectus, qualification or similar requirements, or must be effected pursuant to applicable exemptions from prospectus or derivatives qualification requirements.

There are a number of options available for distributing securities in Canada on a prospectus-exempt basis, generally referred to as exempt distributions or private placements. Most of these are harmonised under National Instrument 45-106 – Prospectus Exemptions.[14]

12 ibid., footnote 5.
13 ibid., footnote 5.
14 Ontario Securities Commission, National Instrument 45-106 – Prospectus Exemptions (2018).

The CSA has indicated that persons wishing to distribute virtual currencies may do so pursuant to these exemptions.[15] Specifically, distributions may be completed pursuant to the accredited investor exemption, which provides a prospectus exemption for trades of securities to entities and individuals that are qualified accredited investors.[16]

Distributions may also be made to investors who do not qualify as accredited investors in reliance on the offering memorandum prospectus exemption.[17] To rely on this exemption, investors must be provided with a written document that contains certain prescribed disclosure, but this exemption does not require the same level of disclosure as a prospectus. Importantly, an investor has certain rights in connection with this type of investment, including a two-business-day withdrawal right and a right of action for rescission or damages if the offering memorandum contains a misrepresentation.[18] Non-reporting issuers (generally, unlisted companies) that rely on the offering memorandum exemption will generally be required to provide to the applicable securities regulatory authority audited annual financial statements and a notice describing how the money raised has been used. The financial statements and notice must be made available to investors within 120 days of each financial year end.

A number of companies have successfully completed virtual currency offerings in compliance with applicable securities law requirements and bespoke exemptions from such requirements. Montreal-based Impak Finance Inc (Impak) was the first Canadian company to complete a virtual currency offering with the approval of Canadian securities regulators. Impak issued Impak Coin (MPK), a new virtual currency based on the Waves blockchain platform, for gross proceeds of over C$1 million by way of private placement, in reliance on the offering memorandum exemption.[19]

A few months later, Token Funder Inc (Token Funder) completed the first virtual currency offering under the oversight of the Ontario Securities Commission (OSC). Token Funder was established for the purpose of creating a smart token asset management platform that is intended to, inter alia, facilitate capital raising by third-party issuers through the offering of blockchain-based securities, including tokens and coins.[20] Token Funder issued its virtual currency, FNDR, in reliance on the offering memorandum exemption. In this case, the OSC granted an exemption from the dealer registration requirement for a period of 12 months from the date of the decision, subject to a number of conditions similar to those imposed on Impak.[21]

More recently, ZED Network Inc (ZED) became the first company to obtain exemptive relief from the prospectus and dealer registration requirements (discussed below) under Canadian securities laws for the distribution and trading of the ZED digital remittance and foreign exchange blockchain tokens to (1) money transfer operators (MTOs) registered as money services businesses in Canada with the Financial Transactions and Reports Analysis

15 ibid., footnote 4.

16 ibid., footnote 4.

17 ibid., footnote 4.

18 ibid., footnote 14 at s. 2.9.

19 Ontario Securities Commission, AMF Impak Finance Decision, 16 August 2017.

20 Ontario Securities Commission, OSC Token Funder Decision, 17 October 2017.

21 ibid.

Centre of Canada (FINTRAC Registered MTOs), and (2) MTOs appropriately registered or authorised to operate as money services businesses, or its equivalent, in accordance with the laws of foreign jurisdictions (Foreign Registered MTOs), as applicable.[22]

Notwithstanding the success stories of Impak, Token Funder and ZED, the prospectus and registration requirements imposed by Canadian securities laws may be an obstacle to the issuance of virtual currencies in Canada on a retail basis, even with negotiated bespoke exemptions.[23]

iii Regulatory considerations for intermediaries

Any person or company engaging in, or holding themselves out as engaging in, the business of trading or advising in securities, and, in certain Canadian jurisdictions, in derivatives, must register as a dealer or as an adviser or, where available, conduct these activities pursuant to an exemption from the dealer or, as the case may be, adviser registration requirement under the applicable securities laws. A person or entity that directs the business, operations and affairs of an 'investment fund' must comply with the investment fund manager registration requirements or obtain an exemption from such requirements. Registration requirements are generally harmonised under National Instrument 31-103 – Registration Requirements, Exemptions and Ongoing Registrant Obligations,[24] which sets out requirements for dealers and advisers dealing with capital, proficiency, insurance, financial reporting, know your client, investor suitability, client disclosure, safekeeping of assets, record-keeping, account activity reporting, complaint handling and other compliance matters.

In Canada, the requirement to register as a dealer or adviser is triggered where a person or company conducts a trading or advising activity with respect to securities or derivatives for a business purpose.[25] The mere holding out, directly or indirectly, as being willing to engage in the business of trading in securities may trigger the requirement to register as a dealer; however, a number of factors must be considered when determining whether registration is required, including whether a business:

a engages in activities similar to a registrant;
b intermediates trades or acts as a market maker;
c carries on an activity with repetition, regularity or continuity;
d expects to be remunerated or compensated; and
e directly or indirectly solicits.[26]

In the context of virtual currency distributions, the CSA has noted the following additional factors in determining whether a company may be considered to be trading in securities for a business purpose:[27]

a soliciting of a broad range of investors, including retail investors;

22 Ontario Securities Commission, OSC ZED Network Decision, 21 May 2019.

23 Kik Interactive opted to exclude Canadian investors from the initial offering of its virtual currency following discussions with the OSC. See Claire Brownell, 'Kik bans Canadians from investing in new crypto-token, cites 'weak guidance' from regulators', *Financial Post* (8 September 2017).

24 Ontario Securities Commission, National Instrument 31-103 – Registration Requirements, Exemptions and Ongoing Registrant Obligations.

25 Ontario Securities Commission, Companion Policy 31-103 CP – Registration Requirements, Exemptions and Ongoing Registrant Obligations.

26 ibid.

27 ibid., footnote 4.

b using the internet to reach a large number of potential investors;
c attending public events to actively advertise the sale of a virtual currency; and
d raising a significant amount of capital from a large number of investors.

The CSA has stated that persons facilitating offerings of virtual currencies that meet the business trigger must collect know your client information and perform suitability assessments to ensure that purchases of virtual currencies are suitable, including with respect to investment needs and objectives, financial circumstances and risk tolerance.[28]

The creation and marketing of products related to virtual currencies are also subject to derivatives-related regulatory requirements, including in relation to qualification, registration and trade data reporting in a number of Canadian jurisdictions, including specifically Quebec, where the rules in relation to over-the-counter (OTC) and exchange-traded derivatives are more fully developed.[29]

The CSA has also issued recent proposals to establish a harmonised framework of registration and business conduct requirements for OTC derivatives market participants.[30] The proposals expressly define a commodity to include a cryptocurrency.

iv Exchanges and other platforms

As marketplaces, exchanges are regulated pursuant to their applicable provincial securities statutes, as well as National Instrument 21-101 – Marketplace Operation (NI 21-101),[31] National Instrument 23-101 – Trading Rules (NI 23-101)[32] and their related companion policies.

NI 21-101 defines a marketplace as a facility that brings together buyers and sellers of securities, brings together the orders for securities of multiple buyers and sellers, and uses established non-discretionary methods under which the orders interact with each other.[33]

An exchange is a marketplace that may:

a list the securities of issuers;
b provide a guarantee of a two-sided market for a security on a continuous or reasonably continuous basis;
c set requirements governing the conduct of marketplace participants; or
d discipline marketplace participants.[34]

28 ibid., footnote 4.
29 Autorité des marchés financiers, Notice relating to the public offering of derivatives on cryptocurrencies and other innovative assets (22 May 2018).
30 Canadian Securities Administrators, Notice and Request for Comment – Proposed National Instrument 93-102 Derivatives: Registration and Proposed Companion Policy 93-102 Derivatives: Registration (published 19 April 2018 for comment until 17 September 2018), and Notice and Second Request for Comment – Proposed National Instrument 93-101 Derivatives: Business Conduct and Proposed Companion Policy 93-101CP Derivatives: Business Conduct (published 14 June 2018 for comment until 17 September 2018).
31 Ontario Securities Commission, National Instrument 21-101 – Marketplace Operation (2018).
32 Ontario Securities Commission, National Instrument 23-101 – Trading Rules.
33 ibid., footnote 31.
34 ibid.

To operate as an exchange in Canada, a person or company must first apply for recognition as an exchange or for an exemption from the recognition requirement.[35] As another type of marketplace, alternative trading systems, which provide automated trading systems that match buyer and seller orders, are also regulated under NI 21-101 and NI 23-101.

It follows that exchanges or other platforms that facilitate the purchase, transfer or exchange of virtual currencies that are considered securities or derivatives may be subject to recognition requirements as securities or derivatives exchanges or marketplaces.[36] In the institutional market, prescribed or negotiated exemptions may be available in respect of platform-related recognition requirements under securities or derivatives laws, subject to the satisfaction of certain conditions and acceptance by the applicable regulators.

On 14 March 2019, the CSA and IIROC published the Consultation Paper, seeking input from the fintech community, market participants, investors and other stakeholders on how securities regulatory requirements may be tailored for platforms that facilitate the buying and selling or transferring of virtual currencies operating in Canada. The feedback is intended to be used to establish a framework to provide regulatory clarity to virtual currency exchange platforms and address risks to investors while fostering market integrity. The content and tone of the Consultation Paper suggest that the CSA and IIROC are looking to develop a regulatory framework for virtual currency exchange platforms that would largely rely on or be inspired by the existing regulatory framework applicable to marketplaces, while addressing more appropriately the specific factors and nuances relevant to the trading of virtual currencies in a largely digital environment. The Consultation Paper proposed a number of factors that may be considered in determining whether the trading of a security or derivative is involved, including:

a whether the platform is structured so that there is intended to be and is delivery of crypto assets to investors;

b if there is delivery, when that occurs, and whether it is to an investor's wallet over which the platform does not have control or custody;

c whether investors' crypto assets are pooled together with those of other investors and with the assets of the platform;

d whether the platform or a related party holds or controls the investors' assets;

e if the platform holds or stores assets for its participants, how the platform makes use of those assets;

f whether the investor can trade or roll over positions held by the platform; and

g having regard to the legal arrangements between the platform and its participants, the actual functions of the platform and the manner in which transactions occur on it:

- who has control or custody of crypto assets;
- who the legal owner of such crypto assets is; and
- what rights investors will have in the event of the platform's insolvency.

In formulating applicable requirements for a future regulatory framework, the CSA and IIROC have suggested that such a framework take into account risks associated with:

a custody;

b price determination;

35 ibid., footnote 4.

36 Canadian Securities Administrators, CSA Investor Alert: Caution Urged for Canadians Investing with Crypto-Asset Trading Platforms, 6 June 2018.

c surveillance of trading activities;
d systems and business continuity;
e conflicts of interest;
f insurance; and
g clearing and settlement.

To date, no virtual currency trading platform has been recognised as an exchange, or otherwise authorised to operate as a marketplace or dealer in Canada.[37] As such, the CSA has urged Canadians to be cautious when buying virtual currencies. The CSA has issued a steady stream of market advisories alerting market participants to risks related to products linked to virtual currencies, including futures contracts, on both regulated and unregulated platforms.[38,39]

v Asset management and investment funds

The demand for economic exposure to virtual currencies is high and investment funds have been a popular vehicle for obtaining this exposure. However, persons operating or administering collective investment structures that hold or invest in virtual currencies may also be subject to investment fund manager registration requirements in addition to dealer, adviser and prospectus or private placements requirements. The structures themselves may also be subject to reporting and conduct requirements that apply to investment funds.

In September 2017, First Block Capital Inc became the first registered investment fund manager (IFM) in Canada for a fund dedicated solely to investments in virtual currencies.[40] The British Columbia Securities Commission (BCSC) granted First Block Capital registration as an IFM and exempt market dealer in order to operate a Bitcoin investment fund, subject to certain bespoke exemptions from the applicable regime.[41] In its decision, the BCSC imposed a number of conditions on First Block Capital, including the requirement to seek the prior approval of the BCSC:

a to establish or manage any virtual currency investment fund;
b to change the investment objective of the virtual currency investment fund;
c to change the entity that maintains custody of the specified virtual currencies held by any investment fund;
d to change the entity responsible for the execution of trades in specified virtual currencies; and
e to change the firm's policies and procedures used to value any virtual currency held by any investment fund managed by the firm.[42]

37 ibid., footnote 6.
38 For example, the CSA reminds investors of the inherent risks associated with virtual currency futures contracts (18 December 2017). OSC Study: Lack of understanding of crypto assets puts Ontarians at risk (28 June 2018).
39 CSA Investor Alert: Caution Urged for Canadians Investing with Crypto-Asset Trading Platforms (6 June 2018).
40 British Columbia Securities Commission, B.C. Securities Commission grants landmark bitcoin investment fund manager registration (6 September 2017).
41 ibid.
42 ibid.

The BCSC also imposed a number of other obligations on First Block Capital with respect to oversight of the third-party custodians and brokers.[43]

Additional investment fund managers have also been approved by the CSA since the *First Block Capital* decision.[44]

The CSA has encouraged fintech businesses interested in establishing a virtual currency investment fund to consider:

a the prospectus requirements when distributing securities to retail investors;
b the legal and operational suitability of virtual currency exchanges;
c the registrations required with respect to the investment fund;
d the valuation methodology for the virtual currencies; and
e the virtual currency expertise of the custodian for the virtual currencies.[45]

Although certain virtual currency investment fund applications have been successful, it has proven difficult for these funds to become accessible to the general public. In October 2018, 3iQ Corp (3iQ) filed a non-offering preliminary prospectus on behalf of the Bitcoin Fund (3iQ Fund), a non-redeemable investment fund established as a trust under the laws of the province of Ontario, in its capacity as investment fund manager of the Fund.[46] As stated in the prospectus, the 3iQ Fund intended to invest in long-term holdings of Bitcoin purchased from various sources, including Bitcoin exchanges, to provide its investors with (1) exposure to Bitcoin and the daily price movements of the US dollar price of Bitcoin; and (2) the opportunity for long-term capital appreciation.[47] Cidel Trust Company (the Custodian), which was expected to be appointed as the custodian of the assets of the 3iQ Fund, had advised 3IQ that it did not have the capacity to hold bitcoin and that it intended to appoint a sub-custodian to hold bitcoin on behalf of the 3iQ Fund.[48]

On 15 February 2019, the Director, Investment Funds and Structured Products (the Director) of the OSC decided that it would be contrary to the public interest to issue a receipt for the 3iQ Fund's preliminary prospectus for multiple reasons, including:

a the difficulty of asset valuation as a result of the fragmented and unregulated environment in which Bitcoin generally trades;
b the difficulty of the sub-custodian to provide customary reports on the design of the 3iQ Fund's controls and their ability to operate as intended over a defined period of time; and
c the lack of clarity as to how the 3iQ Fund's auditor would be able to provide an unqualified opinion on its annual financial statements in accordance with Canadian securities laws.[49]

43 ibid.
44 See, for example, Canadian Securities Administrators, Majestic Asset Management; Canadian Securities Administrators, Rivemont Investments Inc; and Canadian Securities Administrators, 3iQ Corp.
45 ibid., footnote 4.
46 Ontario Securities Commission, OSC 3iQ Corp. Decision, 15 February 2019.
47 ibid.
48 ibid.
49 ibid.

On 15 March 2019, 3IQ and the 3iQ Fund made an application to the OSC seeking an order to et aside the decision of the Director to refuse to issue a receipt for the final non-offering prospectus of the 3iQ Fund and an order directing the Director to issue the receipt.[50] The appeal process is ongoing.

II ANTI-MONEY LAUNDERING

The Financial Transactions and Reports Analysis Centre (FINTRAC) is Canada's financial intelligence unit. FINTRAC administers the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)[51] and its associated regulations, and assists in the detection, prevention and deterrence of money laundering and terrorist financing activities.[52] The PCMLTFA applies to a wide range of regulated entities, including money services businesses (MSBs). It requires that reporting entities develop a risk-based compliance programme to identify clients, monitor business relationships, keep records and report certain types of financial transactions.[53]

In 2017, the PCMLTFA was amended through the Budget Implementation Act, 2017[54] to, among other things, expand the application of the MSB rules to foreign persons and entities that have a place of business outside Canada but that are engaged in providing services to their customers in Canada as a foreign MSB. The application of the PCMLTFA was also extended to regulate businesses dealing in virtual currencies. These amendments are scheduled to come into force on 1 June 2020.

On 9 June 2018, the amendments to the regulations to the PCMLTFA were published for industry comments.[55] Final amendments to the regulations were issued on 22 June 2019 and are currently scheduled to come into force on 1 June 2020 concurrently with the MSB amendments to the PCMLTFA.[56] To mitigate the money laundering and terrorist activity financing vulnerabilities of virtual currencies, while at the same time not excessively obstructing innovation, the final amendments do not target virtual currencies themselves, but the persons or entities engaged in the business of dealing in virtual currencies. These dealing in activities include virtual currency exchange services and value transfer services. Persons and entities that are dealing in virtual currency would be financial entities, or domestic or foreign MSBs. As required of all MSBs, persons and entities dealing in virtual currencies would need to implement a full compliance programme and register with FINTRAC. Foreign MSBs would be subject to the same obligations (e.g., to register with FINTRAC, exercise customer due diligence, report transactions and keep records) for these activities. Furthermore, a

50 3iQ Corp. Press Release: 3iQ Appeals Decision of OSC Director on The Bitcoin Fund. 19 March 2019.

51 Proceeds of Crime (Money Laundering) and Terrorist Financing Act, S.C. 2000, c.17.

52 Financial Transactions and Report Analysis Centre of Canada, FINTRAC Annual Report Maximizing Results Through Collaboration, 2017.

53 ibid., footnote 51.

54 Budget Implementation Act, 2017 No. 1 (S.C. 2017, c. 20). Note: the amendment was originally proposed and made in 2014 although not brought into force.

55 Canada Gazette, Part I, Volume 152, Number 2: Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act 2019.

56 Canada Gazette, Part II, Volume 153, Number 14: Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act 2019 (expected to be officially published on 10 July 2019).

foreign MSB found to be non-compliant with the PCMLTFA and its regulations could face an administrative monetary penalty, and in the case of a failure to pay, revocation of its MSB registration, making it ineligible to do business in Canada.

The final amendments define the term 'virtual currency' as:

a a digital representation of value that can be used for payment or investment purposes that is not a fiat currency and that can be readily exchanged for funds or for another virtual currency that can be readily exchanged for funds; or

b a private key of a cryptographic system that enables a person or entity to have access to a digital representation of value referred to in point (a).

The final amendments do not specifically outline what constitutes dealing in virtual currency, although guidance published in connection with the 9 June 2018 proposed amendments states that dealing in activities would include virtual currency exchange services and value transfer services.[57] A virtual currency exchange transaction is defined to mean an 'exchange, at the request of another person or entity, of virtual currency for funds, funds for virtual currency or one virtual currency for another'.[58]

Quebec has enacted separate MSB legislation, which is administered by the AMF. The Money-Services Businesses Act[59] requires that any person or entity who operates a money-services business for remuneration be registered as an MSB. MSB registration issues in Quebec should be considered in connection with any virtual currency businesses with a Quebec nexus.

Canadian federal legislation also provides for economic and political sanctions, including additional monitoring and reporting obligations and prohibitions. These rules include offences such as knowingly collecting or providing funds to terrorist organisations or associated individuals, or dealing with sanctioned governments, entities or individuals.

III REGULATION OF MINERS

The process of virtual currency mining, which utilises specialised, high-speed computers, is energy-intensive. While virtual currency mining is not specifically regulated in Canada at this time, the use of virtual currency mining hardware may be subject to provincial or municipal requirements, or both, relating to the use of energy.

Canada's cold temperatures and low electricity costs make it particularly attractive for virtual currency miners.[60] This increased demand for electricity has caused some provincial and municipal governments to re-evaluate how to process requests from virtual currency miners going forward.

On 25 April 2019, Quebec's Régie de l'énergie issued a decision[61] regarding the rates and conditions for electricity use by blockchain (including virtual currency) clients. In its decision, the Régie de l'énergie, among other things, approved the creation of a new 'blockchain' consumer category and approved the creation of a reserved block of 300 megawatts (MW)

57 ibid.

58 ibid.

59 Money-Services Businesses Act, CQLR, c. E-12.000001.

60 Hooman B, 'Crypto-miners flood into Canada, boosting the hopes of small towns looking for a break', *Financial Post*, 9 April 2018.

61 *Régie de l'énergie* decision D-2019-052 (29 April 2019).

for this category, of which 50 MW must be allocated to blockchain projects of 5 MW or less. On 5 June 2019, Hydro-Quebec launched a request for proposals with respect to the allocation of the 300 MW block reserved for the blockchain consumer category. Projects will be evaluated based on economic and environmental criteria, including number of direct jobs in Quebec, total payroll of direct jobs in Quebec, capital investment in Quebec and total electricity use.

IV CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

Given the relatively nascent stage of the market, the policing of virtual currencies and virtual currency offerings in Canada presents unique enforcement challenges for both criminal prosecutors and securities regulatory authorities. While most of the litigation in the virtual currency market to date has occurred outside Canadian borders, a few Canadian cases warrant discussion.

In 2017, PlexCorps undertook an initial offering of its own virtual currency, PlexCoin. PlexCorps distributed to prospective investors a white paper stating that investors could expect a 1,354 per cent return on investment in less than 29 days.[62] On 20 July 2017, at the request of the AMF, Quebec's Financial Markets Administrative Tribunal issued various *ex parte* orders against PlexCorps, PlexCoin and related businesses, prohibiting them from engaging in activities for the purpose of directly or indirectly trading in any form of investment described in Section 1 of the Securities Act (Quebec),[63] including the solicitation of investors in Quebec and the solicitation, from Quebec, of investors outside the province.[64] The orders effectively required PlexCorps to abandon the planned token offering. PlexCorps disregarded the order and pursued the offering, and, despite AMF warnings to potential investors that PlexCorps had disregarded its orders, Plexcorps still raised approximately US$15 million from over 1,000 investors.[65]

In December 2018, the sole officer and director of Quadriga Fintech Solutions Corp (Quadriga), the operator of a platform that facilitated the purchase and sale of virtual currencies, died suddenly. It was alleged that this individual was the only Quadriga employee with knowledge of the encrypted passcodes required to gain access to Quadriga's virtual currency cold wallets and, as a result, upon the passing of the individual, the majority of Quadriga's virtual currency assets could not be located. In an email statement, a spokesperson for the BCSC stated that the regulatory body did not have any indication that Quadriga was trading in securities or derivatives or operating as a marketplace or exchange under British Columbia securities laws and, as such, that the BCSC did not regulate it.[66]

62 Jonathan Montpetit, 'Alleged Cryptocurrency fraud by Quebec company highlights need for more regulations, experts say', CBC News, 6 December 2017.

63 Quebec Securities Act, 1982, c.48; 2001, c.38. s.1.

64 Autorité des marchés financiers, Virtual Currency – Orders issued against PlexCorps, PlexCoin, DL Innov inc., Gestio inc. and Dominic Lacroix, 21 July 2017.

65 Autorité des marchés financiers, AMF urges utmost caution regarding solicitations relating to PlexCoin, 3 August 2017.

66 Debroop Roy and John Tilak, 'Canada Securities Watchdog Says Crypto Firm Quadriga Beyond its Purview', Reuters, 9 February 2019.

On 5 February 2019, the Supreme Court of Nova Scotia granted Quadriga protection under the Companies' Creditors Arrangement Act (Canada)[67] and Ernst & Young Inc was appointed as monitor in connection with the proceedings. As at 19 June 2019, approximately 76,000 unsecured creditors of Quadriga are owed approximately C$215 million.[68]

V TAX

i Taxation of virtual currencies

For Canadian tax purposes, the Canada Revenue Agency (CRA) has taken the position that virtual currencies constitute a commodity rather than a currency.[69] As such, gains or losses resulting from the trade of virtual currencies are taxable either as income or capital for the taxpayer.[70] Whether a transaction is on the account of income or capital is a question of fact. As with any transactions in securities, the CRA examines the following criteria to determine the nature of a transaction:

a the primary and secondary intentions of a taxpayer;
b the frequency of transactions;
c the period of ownership;
d the taxpayer's expertise and knowledge of virtual currencies markets;
e the relationship between the virtual currency's transaction and the taxpayer's business;
f the time spent engaged in virtual currencies activities;
g the type of financing required to support the taxpayer's cryptocurrency activities; and
h the taxpayer's advertising of the activities, if any.

Where a transaction is considered on capital account, the taxpayer will be required to include in computing its income for the taxation year of disposition one-half of the amount of any capital gain (a taxable capital gain) realised in such year. Subject to and in accordance with the provisions of the Income Tax Act,[71] the taxpayer will generally be required to deduct one-half of the amount of any capital loss (an allowable capital loss) realised in the taxation year of disposition against taxable capital gains realised in the same taxation year. Allowable capital losses in excess of taxable capital gains for the taxation year of disposition generally may be carried back and deducted in any of the three preceding taxation years or carried forward and deducted in any subsequent taxation year against net taxable capital gains realised in such taxation years, to the extent and under the circumstances specified in the Tax Act. Where a transaction is considered on income account, the resulting gains are taxed as ordinary income and the losses are generally deductible.

67 Companies' Creditors Arrangement Act, RSC 1985, c. C-36.
68 Fifth Report of the Monitor in the matter of Application by Quadriga Fintech Solutions Corp, Whiteside Capital Corporation and 0984750 B.C. Ltd. dba Quadriga CX and Quadriga Coin Exchange for relief under the Companies' Creditors Arrangement Act, 19 June 2019.
69 Canada Revenue Agency, Document No. 2013-0514701I7, 23 December 2013.
70 Canada Revenue Agency, Fact Sheets & Taxpayer Alerts, What You Should Know About Digital Currency, 17 March 2015.
71 Income Tax Act, RSC 1985, c.1.

ii Virtual currency mining

The tax treatment of virtual currency mining will depend on whether the activity is undertaken for profit or as a personal endeavour.[72] A personal endeavour is an activity undertaken for pleasure and does not constitute a source of income for tax purposes, unless it is conducted in a sufficiently commercial and business-like way. However, the mining of virtual currencies is likely to be considered a business activity by the CRA considering the complexity of such activity. The mining of virtual currencies would therefore require the taxpayer to compute and report business income in compliance with the Income Tax Act, including the rules with respect to inventory.

iii Paying with virtual currencies

Where a virtual currency is used as payment for salaries or wages, the amount must generally be included in the employee's income computed in Canadian dollars.[73] As a result of the qualification of virtual currencies as a commodity, the use of virtual currencies to purchase goods or services is subject to the rules applicable to barter transactions.[74] Therefore, where virtual currencies are used to purchase goods or services, the value in Canadian dollars of the goods or services purchased must be included in the seller's income for tax purposes, rather than the value of the virtual currencies.[75] However, the CRA has stated that the fair market value of the virtual currency at the time the supply is made must be used to determine the goods and services tax and harmonised sales tax payable on the purchase of a taxable supply of a good or service.[76]

iv Specified foreign property

The CRA has finally stated that virtual currencies situated, deposited or held outside Canada fall within the definition of specified foreign property, as defined in the Tax Act.[77] As such, Canadian residents must report to the CRA when the total costs of virtual currencies situated, deposited or held outside Canada exceed C$100,000 at any time in the year by filing Form T1135 with their income tax return for the year.

v Collection of goods and services tax and harmonised sales tax with respect to virtual currency transactions

There is currently no legislation indicating how to address the collection of goods and services tax and harmonised sales tax (GST/HST) in virtual currency transactions. The CRA's position on the characterisation of virtual currencies for GST/HST purposes is equally unclear. On 17 May 2019, the Department of Finance sought to clarify this issue by releasing draft legislation[78] amending the Excise Tax Act (ETA)[79] to include explicit reference to virtual currencies. The proposed amendment adds 'virtual payment instruments' to the definition of 'financial instruments' in Section 123(1) of the ETA, thus rendering any sale of the virtual

72 Canada Revenue Agency, Document No. 2014-0525191E5, 28 March 2014.
73 ibid., footnote 72.
74 ibid., footnote 68.
75 ibid., footnote 70.
76 ibid., footnote 69.
77 Canada Revenue Agency, Document No. 2014-0561061E5, 16 April 2015.
78 Department of Finance Canada, Draft Legislation Relating to the Excise Tax Act, 17 May 2019.
79 Excise Tax Act, RSC 1985, c. E-15.

currency or transaction involving virtual currencies as a form of payment exempt from GST/HST collection. If the draft legislation is enacted and adopted as proposed, the changes would be effective as of 18 May 2019.

VI LOOKING AHEAD

To achieve a balance between investor protection and innovation, the CSA has introduced the CSA regulatory sandbox, an initiative to support financial technology businesses seeking to offer innovative products, services and applications in Canada.[80] The initiative, along with province-specific initiatives such as the OSC's Launchpad, allow firms to register or obtain exemptive relief from securities law requirements, or both, under a faster and more flexible process than through a standard application, to test products, services and applications in the Canadian market on a time-limited basis.[81] Regulated offerings of virtual currencies such as Impak Coin, FNDR and ZED and approvals of virtual currency investment funds, represent early success stories of the CSA regulatory sandbox.

Market events such as those described in this chapter have highlighted certain risks that the CSA is seeking to address through rule-making and exemptive relief. However, it is clear that while Canadian securities regulators will attempt to make and enforce rules that foster innovation, and fair and efficient capital markets, they will seek to prioritise investor protection, particularly in the retail space.

80 Canadian Securities Administrators, CSA Regulatory, Sandbox, 2018.

81 ibid.

Chapter 8

CAYMAN ISLANDS

Daniella Skotnicki[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

Owing to its neutral tax treatment, political stability and respected legal regime, the Cayman Islands is the global jurisdiction of choice for the formation of investment funds, which are increasingly investing in cryptocurrencies and taking advantage of the investment opportunities in this space.

The Cayman Islands securities regime is more favourable to initial coin offerings (ICOs) and security token offerings (STOs) than those of many other jurisdictions, and Cayman Islands entities have gained popularity as the token generation vehicles for ICOs, STOs and platform development companies. There have also been a number of cryptocurrency exchanges launched by Cayman Islands entities. The Cayman Islands Special Economic Zone provides a simplified route to establishing a physical presence and employing staff in the Cayman Islands.

The Cayman Islands has no specific existing or proposed legislation or regulation regarding ICOs, STOs, cryptocurrency exchanges or investment vehicles investing in cryptocurrency; nor has any case law considered issues arising in the cryptocurrency space. The application of existing laws needs to be considered in relation to this developing space.

i Structuring of virtual currency businesses

There is no direct taxation imposed on Cayman Islands entities, and structuring will largely be driven by onshore tax considerations and business needs.

Exempted companies

The most common type of entity used to form investment funds investing in digital assets, issuers of ICOs and STOs and cryptocurrency exchanges in the Cayman Islands is the exempted company. Exempted companies conduct business on the basis of a declaration by the incorporating subscriber that the operations of the company are to be carried on mainly outside the Cayman Islands.

An exempted company must have a minimum of one shareholder and one director. The appointment of officers is optional. There is no requirement for Cayman-resident directors or officers.

1 Daniella Skotnicki is a partner at Harneys.

Exempted limited partnerships

Exempted limited partnerships are more commonly used to form closed-ended funds investing in cryptocurrencies, which may be investing in illiquid ICOs and STOs rather than more commonly traded cryptocurrencies. The Exempted Limited Partnership Law (the ELP Law) governs the formation of exempted limited partnerships.

The ELP Law also contains provisions relevant to the affairs of an exempted limited partnership, being the primary legislation governing partnerships generally. An exempted limited partnership is a partnership consisting of at least one general partner (who has responsibility for the business affairs of the partnership) and any number of limited partners that is registered as such under the ELP Law.

An exempted limited partnership is not a separate legal entity. It is instead a set of contractual obligations affecting the partners, between themselves, where a general partner is vested with certain powers and obligations in relation to a business and the assets of the business.

Exempted limited partnerships are often treated differently to companies for onshore tax purposes, typically being treated as fiscally transparent. The general partner holds the partnership's assets in statutory trust for the partners, and is tasked with managing the business and affairs of the exempted limited partnership. In the event that the assets of the partnership are inadequate to satisfy the claims of creditors, the general partner is liable for the debts and obligations left unpaid.

Foundation companies

A foundation company shares many of the features of an exempted company. A foundation company is a body corporate with limited liability and separate legal personality from its members and directors and other officers. It can sue and be sued and hold property in its own name. The key feature of a foundation company that often makes it an attractive vehicle for ICOs and STOs is that it is not required to have members following incorporation. This is a particularly useful structure for those projects that will ultimately be decentralised and governed by the community.

A foundation company must, however, unlike an exempted company, appoint a qualified person as a secretary, being a person who is licensed or permitted by the Companies Management Law (revised) to provide company management services in the Cayman Islands, and that secretary must maintain a full and proper record of its activities and enquiries made for giving notice.

Trusts

If ownership and autonomy are concerns, which may be relevant particularly for an ICO or STO, they can be addressed to a certain degree by having a Cayman Islands charitable trust or STAR trust (introduced by the Special Trusts (Alternative Regime) Law) hold all the shares in issue of the exempted company. A Cayman Islands STAR trust is a non-charitable purpose trust that can hold assets for a specific purpose. The trustee must be a licensed trustee in the Cayman Islands.

ii Summary of Cayman laws to be considered in the virtual currency space

The following Cayman Islands statutory and regulatory regimes must be considered when structuring a virtual currency business through the Cayman Islands:

a the Securities Investment Business Law (SIBL);
b the Mutual Funds Law (MFL);
c the Money Services Law (MSL);
d the Bank and Trust Companies Law;
e the Proceeds of Crime Law (PCL), the Anti-Money Laundering Regulations (the AML Regulations) and existing guidance notes, and the Terrorism Law;
f the Stock Exchange Companies Law;
g the US Foreign Account Tax Compliance Act (FATCA) and the OECD Common Reporting Standard (CRS);
h the beneficial ownership regime; and
i the International Tax Co-operation (Economic Substance) Law (the Economic Substance Law).

II SECURITIES AND INVESTMENT LAWS

i SIBL

SIBL regulates securities investment business in the Cayman Islands. Securities investment business refers to dealing in securities, arranging deals in securities, managing securities and advising on securities.

The definition of a security is set out in SIBL, and contains a list of instruments that are common in today's financial markets (securities, instruments creating or acknowledging indebtedness, instruments giving entitlements to securities, certificates representing certain securities, options, futures and contracts for differences), and does not in and of itself include virtual currencies.

Digital assets that take the form of warrants, options, futures or derivatives for securities or commodities may still be securities. If a Cayman entity was deemed to be issuing securities, it would be exempt from any form of licensing under SIBL if the nature of the security was an equity interest, debt interest, or a warrant or similar for equity or debt interests.

If a Cayman entity was issuing or trading digital assets that were options, futures or derivatives, it would need to consider the implications of SIBL in respect of licensing. A business considered to be conducting securities investment business must be licensed under SIBL unless it is considered to be conducting certain activities listed in Schedule 4 of SIBL, which include those businesses that are only providing services to sophisticated persons, high-net-worth persons or a company, partnership or trust (whether or not regulated as a mutual fund) of which the shareholders, unitholders or limited partners are one or more persons falling within such definitions. Persons carrying out activities listed in Schedule 4 must register with the Cayman Islands Monetary Authority (CIMA), make certain filings and pay an annual fee.

ii MFL

The MFL gives CIMA responsibility for regulating certain categories of funds operating in and from the Cayman Islands.

To be categorised as a mutual fund under the MFL, the fund must:

a be issuing equity, and not debt or contractual interests: in other words, shares, limited partnership interests, LLC interests or trust units (this therefore excludes token issuers);

b be a collective investment vehicle effecting the pooling of investor funds;

c issue equity interests that are redeemable or repurchasable at the option of the investors; and

d be established in the Cayman Islands or be a foreign fund seeking to make an offer or invitation to the public in the Cayman Islands to subscribe for its equity interests.

The following funds are not regulated, therefore they are not required to be registered with or licensed by CIMA:

a single investor funds – these are not master funds and are not mutual funds as there is no pooling of investor funds;

b closed-ended funds – funds of this kind that do not permit the redemption or repurchase of investor equity (e.g., private equity funds) are not mutual funds;

c exempted funds – these are not master funds and fall within the definition of a mutual fund, but the equity interests of these funds cannot be held by more than 15 investors, a majority of whom (in number, and without reference to the number of shares or other equity interests held by each investor) are capable of appointing or removing the operator of the fund; and

d listed or otherwise regulated funds that are not incorporated or established in the Cayman Islands and that make invitations to the public in the Cayman Islands to subscribe for a fund's equity interests through a person licensed under SIBL, provided that the fund in question is either listed on a stock exchange recognised for the purpose by CIMA or regulated in a category and by a regulator recognised for the purpose by CIMA.

III BANKING AND MONEY TRANSMISSION

i MSL

The MSL regulates money services businesses in the Cayman Islands. Such businesses include the business of providing (as a principal business) money transmission and currency exchange. The applicability of this law will depend upon the specifics of any ICO or STO, or cryptocurrency exchange. While any specific ICO or STO may, by its nature, fall within the remit of the MSL, the MSL is unlikely to apply to most ICOs and STOs.

The MSL provides that an entity in the business of providing, inter alia (as a principal business), money transmission or currency exchange requires a licence. The meaning of a currency exchange is not defined by the law; however, the Penal Code defines currency notes as legal tender in the country in which they are issued.

ii Bank and Trust Companies Law

Cayman entities require licences to conduct banking business or trust business. Banking business means the 'business of receiving (other than from a bank or trust company) and holding on current, savings, deposit or other similar account money which is repayable by cheque or order and may be invested by way of advances to customers or otherwise'. Trust business means the 'business of acting as trustee, executor or administrator'. This may be relevant to cryptocurrency exchanges, as discussed in Section V.iii.

IV ANTI-MONEY LAUNDERING

i PCL

The PCL has general application to all Cayman-domiciled entities. It is an offence under the PCL to enter into or become concerned in an arrangement that a person knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person (commonly known as money laundering). In addition, the PCL prescribes ancillary offences to money laundering, including aiding, abetting, counselling or procuring money laundering.

Schedule 6 of the PCL provides that certain businesses that are considered to be conducting a relevant financial business (RFB) must also comply with the AML Regulations.

The following businesses are included in the definition of an RFB, which may be relevant to the virtual currency sector:

a investing, administering or managing funds or money on behalf of other persons;

b issuing and managing means of payment (e.g., credit and debit cards, cheques, travellers' cheques, money orders and bankers' drafts, electronic money);

c safe custody services; and

d money or value transfer services.

ii AML Regulations

If an entity is conducting an RFB and therefore is subject to the AML Regulations, it is required to implement know your client (KYC) and anti-money laundering (AML) policies and procedures that comply with the AML Regulations.

In addition to monitoring the business of an entity and downstream investment activities, the AML Regulations require that the entity obtain customer due diligence information, including regarding the source of funds and information on the beneficial owners of customers.

The AML Regulations require that an entity conducting an RFB (or its delegate, i.e., the service provider):

a appoint an anti-money laundering compliance officer (AMLCO) at a managerial level: the role of the AMLCO is to ensure that the entity adopts measures as set out in the AML Regulations and functions as a point of contact for CIMA;

b appoint a money laundering reporting officer (MLRO), which may be the same person as the AMLCO, and a deputy MLRO: the entity must maintain procedures with respect to internal reporting of suspicious activity to the MLRO or deputy MLRO, and the MLRO and deputy MLRO are responsible for reporting to the Financial Reporting Authority;

c maintain, and comply with, identification and verification procedures in accordance with the AML Regulations: this refers to the maintenance of customer due diligence procedures, which are detailed in subsection iv, below;

d adopt a risk-based approach to monitor financial activities, including identifying high-risk activities, which requires the entity to identify risks and to implement policies, controls and procedures to mitigate those risks;

e ensure that appropriate records of documentation and information obtained to comply with the AML requirements are maintained;

f maintain adequate systems to identify risk in relation to persons, countries and activities, including checks against all applicable sanction lists;

g adopt risk management procedures concerning the conditions under which a customer may utilise the business relationship prior to verification;

h observe a list of countries, published by any competent authority, which are non-compliant or do not sufficiently comply with the recommendations of the Financial Action Task Force;

i implement such other procedures of internal control, including appropriate, effective risk-based independent audit and communication functions, as may be appropriate for the ongoing monitoring of business relationships; and

j provide employee training in respect of money-laundering risks and procedures.

iii Risk assessment

An entity (or its delegate) is required to undertake an assessment of the risks of money laundering and terrorist financing based on its customers, the country in which customers reside or operate, the products and services offered, and the delivery channels by which they are offered, and determine the appropriate level and type of mitigation of such risks.

It is arguable that, as most business involving virtual currency is conducted online, this represents a delivery channel with a higher risk of money laundering, and therefore should be considered in the risk assessment undertaken by a business.

iv Customer due diligence

If simplified due diligence cannot be applied (see below) and a customer is a legal person or arrangement, identification and verification procedures need to be applied not only to the legal person or arrangement itself, but also its beneficial owner.

The due diligence information and documentation required will depend on whether the customer is an entity or an individual. However, original or certified documentation of identity (i.e., a certified copy of a passport), address (i.e., a certified copy of a utility bill) and source of funds or wealth in respect of an individual and corporate documents in respect of entities, are generally required.

Simplified due diligence procedures

In certain instances, the RFB can rely on simplified due diligence procedures.

If simplified due diligence is permitted, and the payment for subscriptions is remitted from an account held in a customer's name at a bank in the Cayman Islands or a bank regulated in an equivalent jurisdiction, detailed verification might not be required at the time of subscription (although evidence identifying the branch or office of the bank from which the moneys have been transferred, verification that the account is in the name of the applicant and the retention of a written record of such details is required). However, verification of the identity of the customer will need to be carried out prior to any payment of proceeds or distributions.

If simplified due diligence cannot be applied, and the customer is a legal person or arrangement, identification and verification procedures need to be applied not only to the legal person or arrangement itself, but also its beneficial owner.

Simplified due diligence cannot be applied to any business relationship or one-off transaction believed to present a higher risk of money laundering or terrorist financing by the entity. However, where a customer has been assessed as lower risk, a entity is permitted

to apply simplified due diligence. Any assessment of lower risk must be consistent with the findings of CIMA or any risk assessment carried out by the Cayman Islands Anti-Money Laundering Steering Group.

Depending on the circumstances, it may be possible to apply simplified due diligence where:

a the customer is an RFB required to comply with the AML Regulations, or is a majority-owned subsidiary of such a business;

b the customer is acting in the course of a business in relation to which a regulatory authority exercises regulatory functions, and that is in an equivalent jurisdiction or is a majority-owned subsidiary of such a customer;

c the customer is a central or local government organisation, statutory body or agency of government in the Cayman Islands or an equivalent jurisdiction;

d the customer is a company that is listed on a recognised stock exchange and subject to disclosure requirements that impose requirements to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company;

e the customer is a pension fund for a professional association or trade union, or is acting on behalf of employees of an entity referred to above; or

f the application is made through an intermediary that falls within one of the above categories and provides written assurance from that intermediary in accordance with the AML Regulations.

Enhanced due diligence

Where a customer relationship has been assessed as higher risk by an entity, persons conducting an RFB must apply enhanced due diligence. Enhanced due diligence must also be applied to politically exposed persons (and their family members and close associates); and when a customer or business is from a country that has been identified by credible sources as having serious deficiencies in its AML and combating of financing of terrorism regime, or a prevalence of corruption.

The RFB is required to develop and implement procedures in circumstances where enhanced due diligence is required, such as obtaining additional information from customers and updating it more frequently, enhanced monitoring or requiring additional information in respect of the source of funds.

v Penalties

Any person who breaches the AML Regulations commits an offence and is liable on summary conviction to a fine of up to CI$500,000, or on indictable conviction to an unlimited fine and imprisonment for two years. Where an offence is committed by an entity with the consent or connivance of, or is attributable to neglect on the part of, a director, member, partner, manager, secretary or other similar officer as applicable, that person is liable as well as the entity.

In addition, under amendments to the Monetary Authority Law (2016 Revision) and the Monetary Authority (Administrative Fines) Regulations 2017, CIMA will have the power to impose administrative fines for non-compliance with the AML Regulations.

The penalties under the PCL for the offences described in Section IV are on summary conviction, a fine of CI$15,000 or imprisonment for a term of two years, or both; or on conviction on indictment, to imprisonment for a term of 14 years or to a fine, or both.

vi Terrorism Law

Section 19 of the Terrorism Law (TL) makes it an offence to solicit, receive or provide property with the intention that it be used, or having reasonable cause to suspect that it may be used, for the purposes of terrorism.

According to Section 20 of the TL, it is an offence for a person to use property for the purposes of terrorism or to possess property intending that it be used, or having reasonable cause to suspect that it may be used, for the purposes of financing acts of terrorism, terrorists or terrorist organisations.

Section 21 of the TL makes it an offence for a person to enter into or become concerned with an arrangement as a result of which property is made available to another knowing, or having reasonable cause to suspect, that it will or may be used for the purposes of terrorism.

Under Section 22 of the TL, a person commits a money laundering offence if he or she 'enters into or become concerned in an arrangement that facilitates the retention or control by or on behalf of another person of terrorist property by concealment, by removal from the jurisdiction or by transfer to nominees'.

V REGULATION OF EXCHANGES

i Stock Exchange Company Law (revised)

The Stock Exchange Company Law was introduced to regulate traditional stock exchanges. However, there is no specific legislation in respect of crypto trading platforms. The application of the Stock Exchange Company Law needs to be considered.

Pursuant to the Stock Exchange Company Law, the Cayman Islands Stock Exchange has the sole and exclusive right to operate one or more securities markets in the Cayman Islands. A securities market is defined broadly, and includes offering a place where, or a facility or arrangement by which (and situated in whole or in part in the Islands), securities are listed, or regularly offered for purchase or sale.

Securities are defined to include securities of all descriptions. As there is no further definition of securities under the Stock Exchange Company Law, without evaluating the characteristics of each cryptocurrency offered, there are likely to be many cryptocurrencies that fall within this definition.

Whether a stock exchange is operating within the Cayman Islands will need to be determined based on the operations of the exchange: for instance, where its employees and servers are located.

ii PCL

The PCL applies to all Cayman-domiciled crypto trading platforms, which will need to ensure that they implement policies and procedures to avoid breaching the PCL.

An exchange conducting business that is considered to be an RFB will be required to comply with the AML Regulations. As stated earlier, RFB includes money or value transfer services, which is likely to be relevant in the context of an exchange.

The requirements applicable to businesses conducting an RFB are detailed in Section IV, and includes obtaining KYC and AML information in respect of both the initial purchasers and subsequent purchasers of tokens.

iii MSL

As cryptocurrencies (subject to very limited potential exceptions) are not legal tender in any country, a cryptocurrency exchange is likely not to be considered a currency exchange, and therefore would not require a licence.

A cryptocurrency exchange that only permits crypto-to-crypto exchange is not likely to be considered as offering, as a principal business, a money transmission service. However, whether a cryptocurrency exchange is considered to be a money services business will need to be determined on a case-by-case basis depending on the service offered on the platform.

iv SIBL

If an exchange is issuing or trading in digital assets that are options, futures or derivatives, it will need to consider the implications of SIBL in respect of licensing.

A business considered to be conducting securities investment business must be licensed under SIBL unless considered to be conducting excluded activities, including those businesses that are only providing services to sophisticated persons, high-net-worth persons or a company, partnership or trust (whether or not regulated as a mutual fund) of which the shareholders, unitholders or limited partners are one or more persons falling within such definitions. Excluded persons must register with CIMA and pay an annual fee.

v Bank and Trust Companies Law

A Cayman entity carrying out the business of acting as a trustee requires a licence pursuant to the Bank and Trust Companies Law. Depending on the operation of the platform, a Cayman entity operating an exchange may be considered to be carrying out trust business under the law.

VI REGULATION OF ISSUERS AND SPONSORS

There is no specific legislation applicable to ICO and STO issuers. However, outlined below are some laws that may be of particular relevance.

i PCL

The PCL applies to all Cayman-domiciled ICO and STO issuers, which will need to ensure that they implement policies and procedures to avoid breaching the PCL.

As mentioned in Section IV.i, an issuer conducting business that is considered to be an RFB will be required to comply with the AML Regulations. An RFB includes the following: investing, administering or managing funds or money on behalf of other persons, issuing and managing means of payment (e.g., credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money), and money or value transfer services.

The requirements applicable to businesses conducting an RFB are detailed in Section IV, and include obtaining KYC and AML information in respect of both the initial purchasers and subsequent purchasers of tokens.

ii SIBL

The definition of a security is set out in SIBL and contains a list of instruments that are common in today's financial markets (securities, instruments creating or acknowledging indebtedness, instruments giving entitlements to securities, certificates representing certain

securities, options, futures and contracts for differences), but does not in and of itself include virtual currencies. An issuer of an ICO or STO is therefore unlikely to require a licence under SIBL in respect of issuing the tokens.

iii MSL

As cryptocurrencies (subject to very limited potential exceptions) are not legal tender in any country, an ICO or STO is likely not to be considered a money transmission business and therefore would not require a licence.

iv MFL

The current definition of equity interests in the MFL (which is a key determining factor as to whether an entity qualifies as a mutual fund) excludes most ICO and STO issuers, as tokens are not considered to be equity interests and therefore ICO and STO issuers (as distinct from any blockchain or cryptocurrency asset class focused fund) should not be impacted by the MFL.

VII TAX

There is no taxation imposed on Cayman entities. However, parties interested in virtual currency businesses in the Cayman Islands will need to obtain tax advice in their own jurisdictions. Cayman entities will need to consider their reporting obligations (if any) under FATCA and the CRS, as detailed below.

FATCA, the US–Cayman intergovernmental agreement and implementing legislation, and the CRS

FATCA requires foreign financial institutions and certain other non-financial foreign entities to report on foreign assets held by US account holders, or to be subject to a 30 per cent withholding tax on payments of United States source income and proceeds from the sale of property that could give rise to United States source interest or dividends. The Cayman Islands has entered into an intergovernmental agreement with the United States in respect of FATCA, and has passed legislation to implement FATCA in the Cayman Islands.

The CRS is a global standard for the automatic exchange of financial account information in respect of holders of financial accounts, and requires participating jurisdictions to obtain and report certain information. The Cayman Islands is a participating jurisdiction of the CRS. It has passed legislation implementing both FATCA and the CRS (Automatic Exchange of Information (AEOI) legislation) that imposes reporting obligations on Cayman entities considered to be reporting financial institutions.

The definition of financial institutions for the purposes of the AEOI legislation includes investment entities, which are entities 'that conduct as a business (or is managed by an entity that conducts as a business)' and are 'investing, administering, or managing financial assets or money on behalf of other persons'. The definition of investment entity would include investment funds investing in virtual currency and tokenised funds. The definition of financial assets is very broad, and includes securities and financial instruments; however, it specifically excludes a non-debt direct interest in real property.

An entity that is considered to be an investment entity will be required to implement a compliance and diligence programme to allow the company to identify and report reportable accounts. A reportable account is an account held by one or more reportable persons, or by a passive non-financial entity with one or more controlling persons that is a reportable person.

The definition of an account of an investment entity is 'any equity or debt interest in the investment entity other than interests which are regularly traded on established securities markets'.

It is arguable that the tokens issued by an investment entity do not constitute either equity or debt interest, which are not further defined in respect of an investment entity. However, there are anti-avoidance provisions in both the Cayman FATCA and CRS legislation that would arguably apply to these interests.

Custodial institutions and depository institutions are also considered to be financial institutions for the purposes of the AEOI legislation.

The term custodial institution means any entity that holds, as a substantial portion of its business, financial assets for the account of others. An entity holds financial assets for the account of others as a substantial portion of its business if the entity's gross income attributable to the holding of financial assets and related financial services equals or exceeds 20 per cent of the entity's gross income during the shorter of the three-year period that ends on 31 December (or the final day of a non-calendar year accounting period) prior to the year in which the determination is being made; or the period during which the entity has been in existence.

The term depository institution means any entity that accepts deposits in the ordinary course of a banking or similar business.

An entity is considered to be engaged in a banking or similar business if, in the ordinary course of its business with customers, it accepts deposits or other similar investments of funds and regularly engages in one or more of the following activities:

a makes personal, mortgage, industrial or other loans, or provides other extensions of credit;

b purchases, sells, discounts or negotiates accounts receivable, instalment obligations, notes, drafts, cheques, bills of exchange, acceptances or other evidences of indebtedness;

c issues letters of credit and negotiates drafts drawn thereunder;

d provides trust or fiduciary services;

e finances foreign exchange transactions; or

f enters into, purchases or disposes of finance leases or leased assets.

A cryptocurrency exchange may fall within the above definitions depending on the operations of the exchange.

Financial institutions are required to register with the US Internal Revenue Service for a global intermediary identification number, appoint a principal point of contact and authorised person, and register with the Cayman Tax Information Authority.

Financial institutions are required to report, by 31 May each year, names, addresses, taxpayer identification numbers, dates of birth (where applicable), account numbers, and account balances or values as at the period's end and in respect of any accounts closed during the period.

Financial institutions issuing tokens will need to obtain self-certification forms in respect of the initial purchasers and subsequent transferees of such tokens.

VIII OTHER ISSUES

i Beneficial ownership legislation of the Cayman Islands

The beneficial ownership legislation requires certain companies to maintain details of their beneficial owners and related legal entities on a beneficial ownership register.

If a virtual currency business is established as a Cayman company, the company will need to provide the full name, residential address and identification document details of any entity or person holding more than 25 per cent of the shares or control of the company. If the company is an issuer in respect of an ICO, whether the company will be required to disclose any details in respect of the holders of tokens pursuant to the beneficial ownership legislation will depend on the rights attaching to such tokens.

ii Economic Substance Law

The International Tax Co-operation (Economic Substance) Law (the Economic Substance Law) came into force on 1 January 2019 and the Cayman Islands Tax Information Authority published detailed Guidance Notes on 30 April 2019.

Under the Economic Substance Law any relevant entity that carries on a relevant activity and receives relevant income in a financial period must satisfy the economic substance test in relation to that activity (the ES Test) and make an annual filing with the Tax Information Authority.

Aside from the basic filing requirements, a relevant entity that does not carry on any relevant activity is not required to satisfy the ES Test.

Under the Economic Substance Law, all Cayman Islands companies incorporated under the Companies Law or the Limited Liability Companies Law, all limited liability partnerships registered under the Limited Liability Partnerships Law and all overseas companies that are registered in the Cayman Islands under the Companies Law are relevant entities except those entities that are:

a an investment fund;
b tax resident outside the Cayman Islands; or
c a domestic company.

Relevant income is 'all of an entity's gross income from its relevant activities and recorded in its books and records under applicable accounting standards'. Any income that is not generated from relevant activities is not to be considered when determining adequate substance in the Cayman Islands.

Relevant activities include the business of holding, exploiting or receiving income from 'intellectual property assets', being any intellectual property right including a copyright, design right, patent or trademark, that may be relevant to an ICO or STO.

As income derived from intellectual property assets are considered to be at higher risk of profit shifting from higher to lower (or zero) tax jurisdictions, a more rigorous requirement applies to certain entities that carry on intellectual property business.

ICOs and STOs issued by entities located the Cayman Islands will need to consider the potential requirement to maintain physical substance in the Cayman Islands, depending on where the intellectual property is held.

IX LOOKING AHEAD

The Cayman Islands has not yet implemented specific laws relating to virtual currency. However, it is possible that specific legislation regulating issuers, cryptocurrency exchanges and other entities involved in the cryptocurrency space may be introduced in the future.

Chapter 9

DENMARK

David Moalem and Kristoffer Probst Larsen[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

The Danish financial sector is regulated under numerous acts. Banks, investment firms, management companies, insurance companies, pension funds and mortgage credit institutions are mainly regulated by the Danish Financial Business Act (FBA). Furthermore, the following, inter alia, all have their own separate regulations: alternative investment fund managers, investment advisers, payment service providers and issuers of electronic money.

Danish financial regulation is influenced by both national and international regulatory trends, and Denmark implements most of the directives and guidelines of the European Union into its financial regulations. Certain regulations drafted and adopted by the European Union are also directly applicable in Denmark.

The Danish Financial Supervisory Authority (FSA) is the main supervisory authority in Denmark, although Nationalbanken, the national bank, also has an oversight role.

The European Banking Authority (EBA) published a warning on virtual currencies on 12 December 2013 (the Warning) that defines virtual currencies as 'a form of unregulated digital money that is not issued or guaranteed by a central bank and that can act as means of payment'.[2] The FSA did not materially change the EBA's definition of virtual currencies when it published the Warning on 17 December 2013 or when it revised it on 27 August 2015. On this basis, it is reasonable to assume that this is the definition that has been applied by the FSA until now. However, from 10 January 2020, the Danish Act on Measures to Prevent Money Laundering and Financing of Terrorism (the AML Act) will define a virtual currency as 'a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically'. The definition of virtual currency is inserted into the AML Act as part of the Danish implementation of the Fifth Anti-Money Laundering Directive (AMLD V; see Section IV).[3] Consequently, the definition of virtual currencies provided by the AMLD V has been used in this chapter. The definition must be read in conjunction with the other financial regulations currently in force in Denmark, as it is supplementary to any assets or activities defined in these regulations.

1 David Moalem is a partner and Kristoffer Probst Larsen is an associate at Bech-Bruun.

2 http://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies.

3 Directive 2018/843/ EU.

II SECURITIES AND INVESTMENT LAWS

As mentioned in Section I, Danish financial regulation is, to a large extent, influenced by EU law. The Danish securities and investment laws are regulated both by the rules for securities and offerings thereof, and by rules for providing investment services related to securities, which in Denmark are defined overall as financial instruments.

Prospectus requirements are relevant when offering securities to the public or having securities admitted to trading on a trading venue. Compliance with the rules on prospectus requirements must be ensured before offering securities to the public.

The Danish rules on offering securities to the public or having securities admitted to trading are mainly regulated in the Danish Capital Markets Act (CMA), which implements the Prospectus Directive[4] and certain aspects of the Markets in Financial Instruments Directive II (MiFID II),[5] the Market Abuse Regulation (MAR)[6] and the Prospectus Regulation.[7]

Overall, the rules in the CMA apply to participants and their conduct on the capital markets.

Although market abuse is regulated in the MAR, we have not reviewed virtual currencies in terms of the MAR, as it is beyond the scope of this chapter. However, this seems to be becoming increasingly relevant, as significant financial institutions have listed instruments that derive their value from virtual currencies.

The FBA is the main regulation regarding investment services in Denmark, and it implements, inter alia, parts of MiFID II and the Capital Requirements Directive IV.[8] Furthermore, the area of investment services is also dependent on EU legislation under the Markets in Financial Instruments Regulation (MiFIR).[9] The FBA applies to financial companies such as credit institutions, investment firms, management companies, pensions funds and insurance companies. It thereby regulates a significant amount of services provided; however, in terms of investment law, the defined services in question are investment services as defined in Annex 4 of the FBA, which is similar to Annex I, Sections A and B, MiFID II. This includes, inter alia, the following investment services:

a the reception and transmission of orders in relation to one or more financial instruments;
b the execution of orders on behalf of clients;
c dealing on own account;
d portfolio management; and
e investment advice.

i Financial instruments

Financial instruments are defined directly in the FBA and cited again in the CMA. Both Acts use the same terminology for financial instruments, which include:

a negotiable securities (except for payment instruments) that can be traded on the capital market, including:
    - shares in companies and other securities equivalent to shares in companies, partnerships and other businesses, and share certificates;

4 Current Directive 2003/71/EC.
5 Directive 2014/65/EU.
6 Regulation (EU) No. 596/2014.
7 Regulation (EU) 2017/1129.
8 Directive 2013/36/EU.
9 Regulation (EU) 600/2014.

- bonds and other debt instruments, including certificates for such securities; and
- any other securities of which securities as mentioned above can be acquired or sold, or give rise to a cash settlement the amount of which is fixed with securities, currencies, interest rates or returns, commodities indexes or other indexes, or targets as reference;

b units in collective investment schemes;

c options;

d futures;

e swaps;

f credit derivatives; and

g financial contracts for difference.

Similar to the definition of investment services, the definition of financial instruments under Danish law is similar to that provided by Annex I, Section C in MiFID II.

A virtual currency, in comparison to the above definition, is not a financial instrument, but rather a negotiable security, and will therefore not per se be subject to the above-described securities regulation, since virtual currencies are not included in the list of financial instruments.

Under Danish law, there is no strict requirement regarding structure or legal identity before an asset may be defined as a financial instrument. It is therefore possible that a virtual currency can be defined as a financial instrument whereby the issuer or the virtual currency itself, or both (depending on the set-up), will be subject to regulatory requirements.

The FSA has not yet published any guidance as to when a virtual currency should fall within the definition of financial instruments. However, other financial supervisory authorities have done so. For example, the Swiss Financial Market Supervisory Authority (FINMA) published guidelines on 16 February 2018 regarding how it intends to apply financial market legislation when handling enquiries from initial coin offering (ICO) organisers. FINMA mainly focuses on the economic function and purpose of virtual currencies. The most essential point in FINMA's analysis is the underlying purpose of tokens, and whether they are tradable or transferable.[10]

In addition, the UK Financial Conduct Authority (FCA) has stated that:

> *Cryptocurrency derivatives are, however, capable of being financial instruments under the Markets in Financial Instruments Directive II (MIFID II), although we do not consider cryptocurrencies to be currencies or commodities for regulatory purposes under MiFID II. Firms conducting regulated activities in cryptocurrency derivatives must, therefore, comply with all applicable rules.*[11]

Accordingly, it seems that, like FINMA, the FCA also focuses on the underlying purpose.

We believe that the financial instrument test to be performed under Danish law must be similar to that of FINMA and the FCA.

ii Prospectus requirements

The CMA applies to capital market participants and their conduct on the markets. As such, it regulates different aspects of the Danish capital markets.

10 FINMA; https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/.

11 https://www.fca.org.uk/news/statements/cryptocurrency-derivatives.

The CMA is drafted so that all requests for the admission of securities for trading on a regulated market and all public offerings of negotiable securities in the European Union or European Economic Area are subject to the prospectus requirement.

A prospectus is basically a document describing the major features and attractions of a particular asset or issuer. A prospectus must be prepared in accordance with the regulations applicable to a particular area.

If a virtual currency falls under the definition of a financial instrument, an offering to the public would be subject to the prospectus requirement. If so, it would have to be assessed, on a case-by-case basis, whether an exemption from the prospectus requirement may be relied upon.

Prospectus requirement exemptions for offerings to the public

To our knowledge, there are no virtual currencies listed on regulated markets, therefore only offerings to the public are discussed here.

The most relevant exemptions from the prospectus requirement when offering negotiable securities to the public are as follows:

a offerings with a value of less than €1 million measured over 12 months;

b offerings with a value of less than €8 million, unless a certificate is needed to provide the offering in other EU or EEA Member States; and

c securities for trading issued by a collective investment scheme, however not closed-ended.

An offer to the public of negotiable securities can also be exempted based on the type of addressees of the offer, the amount of addressees, the denomination of units offered and the minimum considerations per investors.

Provided that a particular ICO is not subject to the prospectus requirements, the relationship between the issuer and the sponsor in the ICO will, under Danish law (if applicable), be regulated by (1) the subscription agreement between the issuer and the sponsor as governed by the Danish laws on obligations and contracts and (2) by the overarching principle of the seller's (the issuer's) duty to disclose material facts to the purchaser (the sponsor) (see Section VII).

Investment services

If a virtual currency falls within the definition of a financial instrument, conducting any of the investments services listed in the FBA will be subject to Danish regulations, the FBA and other EU regulations. While a discussion on the consequences of this is outside the scope of this chapter, it must be noted that this may influence the distribution of the virtual currencies, the pricing model with regards to both the issuance and the administration (if any) of the virtual currency, and the disclosure requirements.

III BANKING AND MONEY TRANSMISSION

The business of banking and money transmission is regulated in the FBA regarding credit institutions, and in the Danish Act on Payments (PA) regarding payment service providers and issuing e-money.

i Banking

According to the FBA, an entity carrying out activities comprising receiving from the public deposits or other funds to be repaid, as well as activities comprising granting loans on their own account but not on the basis of issuing mortgage-credit bonds, must be licensed as a credit institution.

The FSA issued guidelines on 4 July 2012 according to which the following four requirements discussed must be satisfied for an activity to trigger the licence requirement under Section 7 of the FBA:

a the entity must receive deposits or other funds to be repaid;
b the entity must receive such funds from the public;
c the entity must grant loans for its own account; and
d if the entity only receives other funds to be repaid, this must be a significant part of that entity's business operation.[12]

We have not yet seen any issuers of virtual currencies that would qualify as a credit institution in accordance with the above conditions, which is an assessment must be made at the level of the issuer. For the issuer to fulfil the above conditions, its financing must be based partly on deposits or other funds to be repaid.

An issuer of virtual currencies will likely be using virtual currencies for financing. We have not seen virtual currencies being used in a way whereby there was an immediate request for repayment. It is therefore our assessment that the purchase of virtual currencies is unlikely to be deemed as deposits or other funds to be repaid, owing to the way virtual currencies are traded. A purchaser's possibility of redeeming the purchase amount relies in most cases on the liquidity of the virtual currency (i.e., supply and demand). In contrast, the blockchain technology seems highly relevant for the market of credit institutions. However, as the technology continues developing, we may see advances in the market of virtual currencies that change aspects or the use of virtual currencies whereby they may be seen as deposits.

If provided to non-consumers, lending not based on deposits is considered a non-regulated service under Danish law, although the issuer will have to be registered in accordance with the AML Act. Lending not based on deposits will, in some cases, require a licence, if loans are provided to consumers. Again, the focus must be on the issuer.

ii Payment services

As mentioned above, payment services are regulated in the PA, which implements the Second Payment Services Directive[13] and the Second Electronic Money Directive.[14]

Under the PA, the definition of money remittance is as a 'payment service where funds are received from a payer for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, without any payment accounts being created in the name of the payer or the payee'.

As virtual currencies are not defined as currencies as such, transferring them cannot be defined as a money remittance service. It may be possible to create a money remittance service based on blockchain technology and virtual currencies, which means a person using virtual

12 https://www.finanstilsynet.dk/~/media/Lovgivning/Regler-og-praksis/2012/Vejledende-udtalelse-040712.pdf?la=da.

13 Directive 2015/2366/EU.

14 Directive 2009/110/EC.

currencies or blockchain technology, or both, to transfer money on behalf of other persons must be aware of whether the service will fulfil the definition of at least money remittance. The focus must therefore be on the issuer and which services it provides.

Furthermore, under the PA e-money is defined as an electronically or magnetically stored monetary value representing a claim on the issuer that is issued on receipt of funds for the purpose of making payment transactions, and that is accepted by people other than the issuer of the e-money.

Before virtual currencies can become e-money, it is required that the value was electronically or magnetically stored, and represented a claim against the issuer. It is rare for both of these requirements to be fulfilled by virtual currencies. Blockchain technology, however, seems rather purposeful for the issuance and use of e-money.

Furthermore, Denmark has chosen to specifically regulate instruments that were formerly known as payments surrogates. These instruments are paid-for electronic services that can be used to (1) acquire goods and services or (2) make payment transactions with the payer's consent to carry out the transaction by telecommunication where the payment goes to the operator who manages the communication network, and who only operates as an intermediary between the user of the payment service and the supplier of goods and services, unless the service constitutes a payment service.

We believe virtual currencies will not fall under the definition of the instruments formerly known as payment surrogates. However, as the technology progresses there may be certain virtual currencies or uses thereof that would fall under this part of the regulations.

IV ANTI-MONEY LAUNDERING

The Danish Parliament has adopted a bill that amends the AML Act and implements the AMLD V, which is designed to bring virtual currencies within the scope of the AMLD IV.[15] The amendments to the AML Act include, inter alia, regulation of providers primarily and professionally engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet providers. These providers will become subject to the AML Act. The definitions of 'virtual currencies' and 'custodian wallet providers' in the AMLD V have been implemented into the AML Act and closely resemble the legal text of AMLD V. The regulation regarding virtual currencies in the AML Act will enter into force on 10 January 2020. The AML Act does not provide direct regulation of exchanges for trading, issuers, sponsors or miners of virtual currencies.

V REGULATION OF EXCHANGES

There is no direct regulation of exchanges for trading of virtual currencies alone. The connection between the purchaser of a virtual currency and the exchange where the purchase has been made will, if Danish law is applicable, be regulated under the Danish laws on, inter alia, contracts and good business practices.

If a virtual currency falls within the definition of a financial instrument as mentioned in Section II.ii, the exchange will be subject to Danish financial regulation, which is under the

15 Directive 2015/849/EU.

FBA, and to MiFID II and MiFIR. If so, buying or trading virtual currencies on the exchange will be an investment service. This will impact exchanges' business models in numerous ways (see Section II).

VI REGULATION OF MINERS

There is no regulation of mining for virtual currencies. Even if a virtual currency would be defined as a financial instrument, the miner would most likely not be deemed to provide any regulated services, as the miner itself will only provide IT resources to the particular trade with a virtual currency.

VII REGULATION OF ISSUERS AND SPONSORS

There is no direct financial regulation of either issuers or sponsors of ICOs. The same applies for investors in virtual currencies. In 2018, the FSA considered, for the first time, whether a specific ICO was within the scope of Danish financial regulation. In the decision, it considered whether the ICO was subject to the prospectus rules and whether the token offered was covered by the e-money rules.

The token in question was issued through the ICO with the specific purpose of being a payment instrument on the issuing company's trading platform when – and if – it was established. Users of the platform were able to acquire the tokens by investing in the ICO.

The FSA found that the token offered was not a transferable security and thus not within the scope of the prospectus rules. The reason for this conclusion was that the token concerned did not impose any economic or decision-making rights over the issuing company or the issuing company's earnings on the purchaser.

The FSA furthermore found that the token could not be equated to e-money, as the prerequisite for being governed by the rules on e-money is that the holder of the e-money has a claim against the issuer which is used as a means of payment. That was not the case with the token in question, as payment with the token on the platform neither initiated an underlying payment to the payee nor could be redeemed with the issuer.[16]

If Danish law is applicable, the relationship between the issuer and the sponsor or initial investor in an ICO as well as the relationship between the sponsor and subsequent purchasers will be regulated under, inter alia, the Danish laws on contracts and obligations. The marketing of virtual currencies will be regulated under the Danish Act on Marketing.

A key aspect of Danish contract law is the duty to loyally inform the other contracting party (i.e., a duty of loyal disclosure). Under this duty, the seller (the issuer of the ICO) must ensure that the purchaser (the sponsor) has received all the information that would be vital in influencing the sponsor's decision and that the seller knows or should know. If the sponsor has not received the vital information, this fact must have been a deciding condition for the sponsor. It is, however, not a condition that the sponsor would have refused to purchase the virtual currency if the sponsor knew of the particular matter, but only that the sponsor's lack of knowledge has had an influence on the terms of the ICO.[17]

16 See https://www.finanstilsynet.dk/Nyheder-og-Presse/Sektornyt/2018/FT-tagerstilling-ICO.

17 See U.2004B.133, David Moalem, PhD, 'Fortielser ved kontraktindgåelse – Om obligationsrettens loyale oplysningspligt'.

The level of information required to be provided to a sponsor will depend on the particular virtual currency. The duty to loyally disclose information to the sponsor does not include a requirement to disclose all the information provided in a regulated prospectus, as the duty is seen as a general obligation up to and in contracts.

As the requirements for a prospectus in general are considered best practice, an issuer should review which parts of the requirements for a prospectus may be vital for a potential sponsor. Unfortunately, the prospectus requirements cannot be used as a checklist for the necessary information, as the issuer may be required to provide information on other matters as well to potential sponsors.

VIII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

As there is no financial regulation applicable to virtual currencies, the risk of enforcement against an issuer in non-compliance with the Danish financial regulations must be considered low.

If a virtual currency qualifies as a financial instrument, as described above, the offering thereof or trade with the virtual currency in non-compliance with the Danish financial regulations can be enforced accordingly. A breach thereof can be enforced with a fine or imprisonment of up to four months, or both, unless a stronger punishment is deserved under other legislation.

Fraud is illegal under the Danish Criminal Code regardless of whether virtual currencies are not directly regulated elsewhere in the Danish regulations. If a person obtains an unjustified gain for himself or herself or others it is fraud, and it will be punished in accordance with Section 279 of the Criminal Code. Those convicted of fraud can be subject to prison sentences of up to one year and six months according to Section 285.

Depending on the circumstances of the virtual currency and the issuance hereof, sanctions may be enforced in accordance with other aspects of the Criminal Code, which may have a higher maximum penalty.

In terms of breaches of the financial regulations, it is usually the FSA that introduces cases and passes them on to the State Prosecutor for Serious Economic and International Crime. The State Prosecutor can also pursue matters on its own account.

IX TAX

i Introduction

No Danish tax acts deal specifically with virtual currencies, and virtual currency income is taxed under the Danish National Tax Act dating from 1922.

Following decisions of the Danish Tax Council[18] in 2016, 2017, 2018 and 2019 greater clarity regarding Danish taxation of virtual currencies is now available.

For Danish tax purposes, any disposal is a tax event, regardless of whether a virtual currency is sold, or is exchanged for another virtual currency or for an entirely different type of asset. Danish exit taxation may furthermore be triggered upon cessation of Danish tax residency.

18 The supreme administrative appellate board within the Danish tax authorities comprising legal experts, experts from the Danish tax authorities and political appointees.

ii Taxation of gains and deductibility of losses on the buying and selling of virtual currencies

Income realised on a disposal of assets is generally not subject to tax unless deemed income from speculation or from active trade with the assets. Technically, the individual intent is decisive for whether a transaction may be deemed speculation.

Technically, the possibility to argue that exchanges of virtual currencies is not speculation exist. Following two decisions of the Danish Tax Council of 9 March 2018 and of 18 June 2018,[19] all acquisitions and disposals of virtual currencies should, from a practical point of view, be deemed by the Danish tax authorities to be speculation, meaning that income realised is taxable in Denmark.

An individual realising gains on virtual currencies must accordingly include the gains as personal income being subject to tax at a marginal rate of approximately 53 per cent. Conversely, losses incurred may be deducted. The tax value of a loss will, however, be significantly lower (approximately 27 per cent) than the marginal tax rate applied to a gain.

If a Danish company buys and sells virtual currencies, the net income generated will be subject to Danish tax at the standard corporate income tax rate of 22 per cent.

iii Taxation of gains and deductibility of losses on the mining and disposal of virtual currencies

According to a decision of the Danish Tax Council of 8 January 2019,[20] income derived from the mining of virtual currencies as a hobby (in the case at hand the virtual currencies were mined through 'pool-mining' utilising personal computers) is subject to tax on each virtual currency granted through mining. Gains realised on a subsequent sale of the virtual currencies will be taxable as well. Only the difference between costs incurred and the value of the virtual currency granted or the gain realised on the subsequent sale will be taxable. Losses incurred as part of hobby businesses may not be deducted in other income sources and cannot be carried forward. Losses realised can only set off gains realised in the same income year.

In principle, an individual may be deemed to act as a professional in relation to the mining of virtual currencies. If that is the case, the individual will be allowed to deduct and carry forward losses similar to a Danish company.

Similarly, a company mining virtual currencies is subject to Danish corporate income tax at a rate of 22 per cent on the net income realised. The restrictions on the applicability of losses and the right to carry forward losses should not apply to companies.

iv Summary

Following decisions of the Danish Tax Council, the Danish practical position is that income derived from buying and selling Bitcoins is subject to Danish tax. If an investor is an individual, income is almost certainly income from speculation, and as such is subject to a marginal tax rate of approximately 53 per cent. Losses may be deducted, but will only carry a tax value of approximately 27 per cent. A corporate investor will be subject tax at the Danish corporate tax rate of 22 per cent.

19 See SKM2018.104.SR and SKM2018.288.SR.

20 See SKM2019.7.SR.

An individual mining virtual currencies will almost certainly be deemed to be carrying out a hobby, and as such be made subject to tax on the net income realised in the income year, but not be allowed to deduct losses in other income or carry forward losses.

X OTHER ISSUES

It is still unclear how virtual currencies will be treated in terms of auditing. According to the Danish Financial Statements Act, virtual currencies are not themselves described. They should most likely be treated either as intangible fixed assets or inventory. The relevant category for each virtual currency depends on an entity's usage of that virtual currency.

XI LOOKING AHEAD

With the exception of the transposition of the AMLD V into Danish law, the Danish legislature has not announced or proposed any changes to the legal framework to regulate virtual currencies. Accordingly, the only relevant legislative changes are the amendments to the AML Act, which will enter into force on 10 January 2020.

However, we expect that the Danish FSA will maintain its increased supervisory focus on the relationship between virtual currencies and the current financial regulatory legal framework. In addition, in October 2019 the government will publish its legislative plans for 2019–2020. As virtual currencies are the subject of ever-increasing focus in the public sphere, the government's legislative plans may well contain initiatives on them.

Chapter 10

FRANCE

Hubert de Vauplane and Victor Charpiat[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

As in many countries, the first contact between cryptocurrencies and French law was through the lens of financial crime. In its 2011 annual report, Tracfin (the French financial intelligence unit tasked with fighting financial fraud, money laundering and terrorism financing) was the first French authority to mention Bitcoin.[2]

Cryptocurrencies then came under scrutiny from other regulators during the Bitcoin bubble of November and December 2013. The French Central Bank published a short report on 'the dangers linked to the development of virtual currencies'.[3] In January 2014, the Prudential Supervision and Resolution Authority (ACPR), the French banking and insurance regulatory authority, stated that entities receiving legal currency on behalf of clients in relation to the purchase or sale of cryptocurrencies were required to obtain a licence to provide payment services.[4]

In December 2016, cryptocurrency trading platforms and brokers were included in the list of entities subject to the anti-money laundering legislation.[5]

In 2016, a distinction arose between the concept of blockchain and the universe of cryptocurrencies. Experimentations using blockchain technology to simplify various technological processes were initiated. Several French banks joined the R3 consortium (which developed a private blockchain platform named Corda). The Deposits and Consignments Fund (a state-owned financial institution) launched LaBChain, a blockchain innovation lab that started working in July 2016 on a business case dedicated to the use of blockchain to manage digital identity and know-your-customer procedures.[6]

Simultaneously, the French government started working on a legal framework allowing the use of blockchain for the registration of securities. Registration on a blockchain was

1 Hubert de Vauplane is a partner and Victor Charpiat is an associate at Kramer Levin Naftalis & Frankel, LLP.

2 Tracfin, Rapport d'activité 2011.

3 Banque de France, Les dangers liés au développement des monnaies virtuelles: l'exemple du bitcoin, 5 December 2013.

4 ACPR, Position 2014-P-01, https://acpr.banque-france.fr/sites/default/files/20140101_acpr_position_bitcoin.pdf.

5 Article 2 of Ordinance No. 2016-1635 of 1 December 2016, modifying Article L. 561-2 of the Monetary and Financial Code (MFC).

6 Caisse des dépôts, LaBChain, launched by Caisse des Dépôts, reveals its first business case, 18 July 2016: https://www.caissedesdepots.fr/en/labchain-launched-caisse-des-depots-reveals-its-1rst-business-case.

first limited to short-term bonds dedicated to small and medium-sized enterprises (SMEs),[7] but was soon extended to all unlisted securities pursuant to Ordinance No. 2017-1674 of 8 December 2017.

In 2017, the renewed cryptocurrencies and initial coin offerings (ICOs) bubble led the French regulators and the government to start working on the creation of a dedicated legal framework. The French government tasked Jean-Pierre Landau, a former top executive of the Central Bank, with preparing a report on cryptocurrencies, which was published in July 2018. Three working groups were created among the French Parliament to prepare reports on ICOs, blockchains and cryptocurrencies. In addition, both the French Financial Markets Authority (AMF) and the ACPR created internal fintech teams acting as 'innovation hubs' in 2016.

In October 2017, the AMF published a discussion paper on ICOs.[8] Following an extended consultation of experts and actors of the French cryptocurrency and ICO economy, it was finally decided to create a dedicated framework for ICOs, rather than try to include them in the scope of the existing regulation of securities offerings. This legal framework was included in Act No. 2019-486 of 22 May 2019 on the growth and transformation of enterprises (the PACTE Act), which contains many measures aimed at facilitating the growth of SMEs and giving employees and stakeholders more control over corporations. Before its adoption, the PACTE Act was amended by the National Assembly and the Senate, and an ad hoc legal framework for intermediaries dealing with cryptocurrencies was added.

In the meantime, widespread lobbying was conducted by the French cryptocurrency community (with the notable help of several legislators interested in cryptocurrencies) to adapt the French tax regime. The capital gains related to cryptocurrencies were taxed at very high rates, and this became a significant problem during the 2017 bull market, as many individual investors threatened to leave France and cash out in tax-friendly jurisdictions. Consequently, Act No. 2018-1317 of 28 December 2018 (the 2019 Budget Act) created a specific tax regime that taxes capital gains at a flat rate of 30 per cent.

With the PACTE Act and the new tax regime now fully in force, the legal environment for companies dealing with cryptocurrencies, ICO issuers and individual investors has been clarified.

II SECURITIES AND INVESTMENT LAWS

i Tokenisation of securities and issuance of security tokens

More than a year before the bubble of late 2017, the French government started studying the emerging concept of blockchain technology (or distributed ledger technology).

The first appearance of the concept of blockchain in French law was in Ordinance No. 2016-520 of 28 April 2016, which created a dedicated framework for the financing of SMEs through crowd-lending platforms. The Ordinance allows for the issuance of promissory notes (known as *minibons*) through a crowd-lending platform. The registration and transfer

7 Ordinance No. 2016-520 of 28 April 2016.

8 AMF, 'The AMF publishes a discussion paper on Initial Coin Offerings and initiates its UNICORN programme', 26 October 2017: https://www.amf-france.org/en_US/Actualites/Communiques-de-presse/AMF/annee-2017?docId=workspace%3A%2F%2FSpacesStore%2F5097c770-e3f7-40bb-81ce-db2c95e7bdae&langSwitch=true.

of *minibons* can either be done in the traditional way (i.e., the issuer maintains and updates a register of all *minibons* holders) or by a shared electronic recording system (i.e., a distributed ledger).[9]

Ordinance No. 2017-1674 of 8 December 2017 took a much bigger step by extending to unlisted securities[10] the possibility to use a distributed ledger for their issuance, registration and transfer. These securities tend to be presented as security tokens, although it would be more accurate to call them 'tokenised securities'; in any case, the PACTE Act makes it clear that tokens issued pursuant to ICOs cannot be securities.[11]

Both Ordinances provided that the technical requirements (i.e., the level of security and authentication) of the shared electronic recording system would have to be specified by a decree to be passed by the government. Instead of rushing this, the government chose to consult the European Commission, which then validated the government's definition of the distributed ledger.[12] The much-awaited decree was published on 24 December 2018 (the Decree).[13]

The Decree provides that the distributed ledgers used for the registration of securities should comply with four technical conditions:[14]

a they must be 'conceived and implemented' in a manner that preserves the integrity of the information recorded;

b they must 'directly or indirectly' allow the identification of the owners of securities, and the nature and number of securities held;

c they must include a business continuity plan, which includes an external data recording system; and

d the owners of the securities registered on them must be able to access their statements of transactions.

The Decree does not specify which of the issuer or its technology provider will be responsible for complying with these technical requirements. In addition, it does not address the distinction between private and public blockchains. Although the Decree does not exclude the possibility to issue and register securities through a public blockchain (such as Ethereum), complying with some of these technical conditions could be more complicated if a public blockchain is used.

The Decree also modifies the rules applicable to the pledging of securities to allow securities registered on a distributed ledger to be effectively pledged.[15]

9 Article L. 223-12 and L. 223-13 of the MFC.

10 More precisely all securities that are not recorded in a central depositary system (Article L. 211-7 of the MFC). Units in collective investment undertakings and negotiable debt securities may also be registered on a distributed ledger (Article R. 211-5 of the MFC).

11 Article L. 552-1 of the MFC.

12 European Commission, Notification Detail, 'Decree on the use of shared electronic recording devices for the representation and transmission of financial securities', 17 July 2018: http://ec.europa.eu/growth/tools-databases/tris/en/index.cfm/search/?trisaction=search.detail&year=2018&num=367&mLang=EN.

13 Decree No. 2018-1226 of 24 December 2018.

14 Article R. 211-9-7 of the MFC.

15 Article R. 211-14-1 of the MFC.

French start-ups and large corporations have already started using the Decree to tokenise their securities. Carthagea[16] and DomRaider[17] announced that they planned to raise funds through the issuance of shares registered on a distributed ledger. In April 2019, Societe Generale issued €100 million worth of covered bonds registered on the Ethereum blockchain, as part of a pilot project in which it was also the sole subscriber of the bonds.[18] In June 2019, the share capital of a company owning a €6.5 million building located near Paris was tokenised by start-up Equisafe.[19]

However, registering securities on a blockchain is only useful insofar as various burdensome or costly processes, such as the vote at general meetings or the secondary market of unlisted securities, are made easier. While the registration of unlisted securities was greatly modernised pursuant to the Ordinance of 8 December 2017 and the Decree, the other obligations to which an issuer is subject with respect to its shareholders have remained the same, thus creating many practical problems. Various regulations (both French and European) will need to be amended to make the registration of securities on a blockchain an attractive option (see Section XI).

ii Asset managers and investment funds

In the past two years, alternative fund managers have started to create cryptocurrency investment funds. Tobam Bitcoin Fund, launched in November 2017 by French alternative asset manager Tobam, claimed to be the very first European cryptocurrency fund.[20] However, Tobam's fund was not licensed by the AMF, as cryptocurrencies, as an asset class, did not fit in any category of the regulatory framework applicable to asset managers.

Napoléon X, which raised around €10 million following an ICO in 2018, became the first French crypto start-up to obtain an asset manager licence from the AMF. The first regulated funds are expected to be launched in 2019.[21]

In addition, the PACTE Act now allows professional specialised investment funds (FPSs), which are dedicated to professional investors, to purchase assets registered in a shared electronic recording system (i.e., a blockchain).[22] The PACTE Act also allows professional private equity funds (FPCIs) to invest up to 20 per cent of their assets in digital assets.[23] FPSs and FPCIs are alternative investment funds and, therefore, may only be managed by a

16 Chaineum, 'Chaineum Acts as STO Advisor for Carthagea', 14 March 2019: https://medium.com/@Chaineum/chaineumacts-as-sto-advisor-for-carthagea-da428bdfa8e8.

17 DomRaider, 'DomRaider to launch an Equity Token Offering and sell shares registered on blockchain', 27 May 2019: https://www.domraider.com/en/equity-token-offering-shares-blockchain/.

18 Societe Generale, 'Societe Generale issued the first covered bond as a security token on a public blockchain', 23 April 2019: https://www.societegenerale.com/en/newsroom/first-covered-bond-as-a-security-token-on-a-public-blockchain.

19 Equisafe, 'Equisafe réalise la première vente d'immeuble via la technologie blockchain en Europe pour un montant de 6,5 millions d'euros', 25 June 2019: http://web.lexisnexis.fr/LexisActu/CommuniquedepresseEquisafe.pdf.

20 Tobam, 'TOBAM launches first Bitcoin mutual fund in Europe', 22 November 2017: https://www.tobam.fr/tobam-launches-first-bitcoin-mutual-fund-in-europe/.

21 Napoleon Group, 'France authorizes Napoleon AM as first regulated Asset Manager expert on crypto solutions', 8 December 2018: https://medium.com/napoleonx-ai/france-authorizes-napoleon-am-as-first-regulated-asset-manager-expert-on-crypto-solutions-1212dbd01a59.

22 Article L. 214-154 of the MFC.

23 Article L. 214-160, II of the MFC.

licensed asset manager; however, they are required to appoint a depositary (which is notably in charge of the custody of the assets owned by the fund). Licensed cryptocurrency asset managers will still need to find depositaries willing to take custody of cryptocurrencies.

Regarding cryptocurrency derivatives, the AMF took actions to increase the protection of retail investors against websites offering to bet on cryptocurrencies through derivatives (such as contracts for difference or binary options). In February 2018, the AMF issued an analysis stating that cash-settled contracts on cryptocurrencies qualified as derivatives under French law.[24] Consequently, platforms that offer cryptocurrency derivatives trading must now obtain an administrative authorisation and may not target French residents in their online marketing.

Finally, the management of individual cryptocurrency portfolios on behalf of clients is now included in the list of the digital assets services.[25] Obtaining a licence will be optional for entities providing this service and, as a general rule, they will not be subject to any regulation.

III BANKING AND MONEY TRANSMISSION

Over the past few years, French banking regulators have frequently reminded the general public that cryptocurrencies are not real money. The Central Bank and the ACPR, for example, consider that the term 'cryptocurrency' is misleading, and prefer to use the term 'cryptoassets'.[26]

Their position clearly matters because the French regulation of payment services revolves around the use of legal currency (i.e., a legal tender issued by a sovereign country). All the payment services defined by Article L. 314-1 of the MFC involve the use of funds. Pursuant to Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market (PSD 2), funds mean 'banknotes and coins, scriptural money or electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC'.[27] Therefore, as a general rule, receiving and sending cryptocurrencies on behalf of third parties does not qualify as a regulated service under the payment services regulation.

However, the recent development of stablecoins (and in particular fiat-backed stablecoins) blurs the line between legal currencies and cryptocurrencies. As the European Banking Authority (EBA) stated in its advice on cryptoassets of 9 January 2019, redeemable fiat-backed stablecoins may qualify as electronic money when the token (1) is electronically stored, (2) has monetary value, (3) represents a claim on the issuer, (4) is issued on receipt of funds, (5) is issued for the purpose of making payment transactions and (6) is accepted by persons other than the issuer.[28] Consequently, some fiat-backed stablecoin issuers may be required to obtain electronic money licences to be allowed to operate in France.

Finally, the announcement of Facebook's plan to launch a cryptocurrency called Libra has been met with scepticism by the French government and the Central Bank. Bruno Le Maire, the Minister of Economy and Finance, stated that Facebook may create its own payment

24 AMF, Analysis of the legal qualification of cryptocurrency derivatives, 23 March 2018: https://www.amf-france.org/en_US/Reglementation/Dossiers-thematiques/Marches/Produits-derives/Analyse-sur-la-qualification-juridique-des-produits-d-riv-s-sur-crypto-monnaies?langSwitch=true.

25 Article L. 54-10-2, 5°, b) of the MFC.

26 Banque de France, L'émergence du bitcoin et autres crypto-actifs: enjeux, risques et perspectives, 5 March 2018.

27 Article 4(25) of the PSD 2.

28 EBA, Report with advice for the European Commission on crypto-assets, 9 January 2019, pp. 12–13.

system, but under no circumstance should it be allowed to create a sovereign currency.[29] François Villeroy de Galhau, the governor of the Central Bank, stated that Libra would in any case need the relevant licences if payment or banking services are to be provided.[30] France also announced that a taskforce dedicated to stablecoins would be created within the G7.[31]

IV ANTI-MONEY LAUNDERING

French authorities started monitoring the use of cryptocurrencies in illegal transactions as early as 2011. The 2011 annual report of Tracfin briefly described how Bitcoin could be used in money laundering schemes.[32] In June 2014, a working group led by Tracfin published a report on cryptocurrencies and issued various recommendations aimed at limiting the use of cryptocurrencies in money laundering or terrorism financing schemes.[33]

Tracfin closely monitors cryptocurrencies. Its last annual report describes how untraceable and privacy-oriented cryptocurrencies (such as Monero or Zcash) and anonymous prepaid payment cards linked to cryptocurrency wallets are increasingly used by fraudsters and money launderers.[34]

Cryptocurrencies were left out of the scope of French anti-money laundering and terrorism financing (AML/CFT) regulation until Order No. 2016-1635 of 1 December 2016, which added cryptocurrency trading platforms and brokers to the list of persons subject to AML/CFT requirements.

The European Union addressed cryptocurrency-related AML/CFT issues through Directive (EU) 2018/843 of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (the Fifth Anti-Money Laundering Directive), which states that the 'Member States shall ensure that providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers, are registered.' The Fifth Anti-Money Laundering Directive defines virtual currencies as 'a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically'.

To implement the Fifth Anti-Money Laundering Directive, the PACTE Act extends the list of entities subject to AML/CFT requirements to include the following categories: (1) ICO issuers that obtained the optional approval of the AMF; (2) digital assets custodians and entities allowing the purchase or sale of digital assets against legal currency; and (3) licensed

29 Bloomberg, 'Facebook Token Runs Into Instant Political Opposition in Europe', 18 June 2019: https://www.bloomberg.com/news/articles/2019-06-18/france-calls-for-central-bank-review-of-facebook-cryptocurrency.

30 Cointelegraph, 'French Central Bank: Facebook's Libra May Need Banking License', 25 June 2019: https://cointelegraph.com/news/french-central-bank-facebooks-libra-may-need-banking-license.

31 The Block, 'France to create G7 stablecoin taskforce following Libra's announcement', 21 June 2019: https://www.theblockcrypto.com/tiny/france-to-create-g7-taskforce-on-cryptocurrency-stablecoin/.

32 Tracfin, Rapport d'activité 2011, pp. 21–23.

33 Ministry of Economy and Finance, Regulating virtual currencies – Recommendations to prevent virtual currencies from being used for fraudulent purposes and money laundering, June 2014: https://www.economie.gouv.fr/files/regulatingvirtualcurrencies.pdf.

34 Tracfin, 2017–2018 – Money Laundering and Terrorist Financing Risk – Trends and Analysis, June 2019.

digital assets services providers.[35] The PACTE Act includes the definition of virtual currencies under the Fifth Anti-Money Laundering Directive in the definition of digital assets.[36] (The definition of digital assets also includes tokens issued pursuant to ICOs.) As French banks are reluctant to open accounts for cryptocurrency-related companies because the AML/CFT regulation applicable to them is still unclear, the above-mentioned categories of entities will also benefit from preferential access to banking services (see Section X).

However, surprisingly, the PACTE Act does not extend the scope of AML/CFT requirements to cryptocurrency trading platforms, although the Fifth Anti-Money Laundering Directive requires Member States to register 'providers of exchange services between virtual currencies and fiat currencies'. In fact, crypto-to-fiat trading platforms would be subject, in any case, to Position 2014-P-01 of the ACPR, which requires them to obtain a licence to provide payment services. Licensed payment services providers are themselves subject to AML/CFT requirements.

Finally, in March 2018, the G20 finance ministers asked the Financial Action Task Force (FATF) to clarify how its standards apply to cryptoassets. In October 2018, the FATF stated that 'jurisdictions should ensure that virtual asset service providers are subject to AML/CFT regulations, for example conducting customer due diligence including ongoing monitoring, record-keeping, and reporting of suspicious transactions. They should be licensed or registered and subject to monitoring to ensure compliance.'[37] In 2019, the FATF also updated its guidance for a risk-based approach on virtual assets and virtual asset service providers. The Fifth Anti-Money Laundering Directive will probably need to be further amended to comply with these recommendations.

Cryptocurrency-related companies that are not currently included in the list of persons subject to AML/CFT requirements must still report any suspicious transaction to the public prosecutor, which will then notify Tracfin.

V REGULATION OF EXCHANGES AND OTHER DIGITAL ASSET SERVICES PROVIDERS

Before the creation by the PACTE Act of a comprehensive legal framework for digital assets services providers (DASPs), certain actors of the cryptocurrency industry were already subject to a specific regulatory status. Since January 2014, the ACPR requires that any intermediary receiving funds in relation to a purchase or sale of cryptocurrencies (e.g., a trading platform or a broker) must obtain a licence to provide payment services.[38] To our knowledge, the ACPR has not clarified what effect the adoption of the PACTE Act will have on this requirement.

DASPs are entities that provide services related to digital assets. Digital assets, as defined by the PACTE Act, include: (1) tokens, as this term is defined in the ICO legal framework (i.e., intangible digital assets incorporating rights that can be issued, registered, held and transferred on a shared electronic recording system), as long as they do not qualify as financial instruments; and (2) any digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal

35 Article L. 561-2, 7° *bis* to 7° *quater* of the MFC.

36 Article L. 54-10-1 of the MFC.

37 FATF, Regulation of virtual assets, 19 October 2018.

38 ACPR, Position 2014-P-01, 29 January 2014.

persons as a means of exchange and that can be transferred, stored and traded electronically.[39] This definition of digital assets is slightly more precise than the definition of virtual assets in the FATF Recommendations.[40] In any case, all cryptoassets and cryptocurrencies would be covered by the definition of digital assets, but certain tokens that may not be based on cryptography may also qualify as digital assets.

To establish the list of the services related to digital assets, the promoters of the PACTE Act looked to traditional investment services for inspiration. Therefore, digital assets services include the following services, as soon as they are performed in relation to digital assets:

a custody of digital assets or cryptographic private keys;
b purchase or sale of digital assets against legal currency;
c purchase or sale of digital assets against other digital assets;
d operation of a digital assets trading platform; and
e various other services related to digital assets, including receipt and transmission of orders on behalf of third parties, portfolio management, investment advice, underwriting, and placing with or without a firm commitment.[41]

These digital assets services will be further described in an implementing regulation, to be adopted during summer 2019.

Licensed entities will be subject to obligations equivalent to those of regulated investment services providers: they will have to subscribe to professional liability insurance (or comply with capital requirements), possess secure and resilient IT systems, and establish adequate policies to manage conflicts of interests. In addition, depending on the regulated services they intend to provide, licensed DASPs will have to comply with additional requirements. For example, licensed custodians will be required to establish a custody policy, ensure that they are always able to return the cryptoassets or the keys to their clients (or both) and implement segregated accounts.[42]

The AMF presents this regulatory approach based on optional licences as an incentive-based system. It emphasises non-mandatory provisions to foster professionalism and promote sound market practices while avoiding constraining frameworks that might deter innovation and diminish France's attractiveness. Licensed actors will regarded as 'white-listed' and may use their licence as a marketing tool. However, owing to anti-money laundering concerns (arising notably from the Fifth Anti-Money Laundering Directive), obtaining a registration with the AMF will be mandatory for both custodians of digital assets and providers of the service of purchase or sale of digital assets against legal currency. The requirements to obtain this registration will not be overly burdensome: registered providers must give the AMF information regarding the reputation and professional qualifications of their managers and beneficial owners, as well as implement the internal procedures required to comply with the anti-money laundering legislation. The registration will be granted by the AMF, although the prior approval of the ACPR will also be required.

39 Article L. 54-10-1 of the MFC.

40 The FATF Recommendations, p. 124: 'A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.'

41 Article L. 54-10-2 of the MFC.

42 Article L. 54-10-5 of the MFC.

Anti-money laundering requirements will also apply to digital assets service providers that obtained the optional licence. Although obtaining a DASP licence will mostly serve as a marketing tool, licensed entities will also be granted the following benefits:

a they will not be arbitrarily forbidden from opening a bank account and accessing basic banking services (see Section X); and

b they will be allowed to contact potential individual clients on a massive scale (through emails or cold calls) to market their services, in accordance with the 'financial or banking solicitation' regime.[43] Licensed DASPs will also be able to broadly advertise their services to the general public and use sponsorship as a marketing tool. On the other hand, the use of these marketing methods will be forbidden for unlicensed DASPs.

The licence granted by the AMF has no extraterritorial effect. As this regulatory framework is unique to France, there is no passporting regime applicable to DASPs.

The PACTE Act also requires the French government to prepare a report discussing the possibility of making the licence mandatory for all DASPs, taking into consideration the upcoming recommendations of the FATF.[44]

VI REGULATION OF MINERS

Miners of cryptocurrencies are not subject to any specific regulatory regime. The French mining industry is almost non-existent, as electricity prices have been too high to make mining profitable in the past few years.[45] However, many individuals mine cryptocurrencies as a hobby or a side job.

A parliamentary report of 30 January 2019 on virtual currencies[46] suggested that French miners be legally included in the list of 'electro-intensive industries', and thus exempted from the domestic tax on final electricity consumption (TICFE). This exemption could lower electricity costs by a third, thus making France more attractive for miners. However, the environmental impact of cryptocurrency mining has been widely criticised recently, and it seems unlikely that the government will take the risk of granting these benefits to cryptocurrency miners.

VII REGULATION OF ISSUERS

While France has struggled to attract prominent ICOs in the past few years,[47] the government and the AMF have taken multiple steps to turn France into an ICO-friendly jurisdiction.

43 Articles L. 341-1 et seq. of the MFC.

44 Article 86, X of the PACTE Act.

45 *Les Echos*, 'Blockchain : le français Bigblock Datacenter délocalise ses fermes de minage au Kazakhstan', 11 March 2019: https://www.lesechos.fr/tech-medias/hightech/blockchain-le-francais-bigblock-datacenter-delocalise-ses-fermes-de-minage-au-kazakhstan-999360.

46 National Assembly, Rapport d'information en conclusion des travaux d'une mission d'information relative aux monnaies virtuelles, 30 January 2019.

47 According to the AMF, French ICOs only raised €89 million, while the global amount raised by ICOs reached $22 billion. (AMF, French ICOs – A New Method of Financing, 14 November 2018: https://www.amf-france.org/en_US/Publications/Lettres-et-cahiers/Risques-et-tendances/Archives?docId=workspace%3A%2F%2FSpacesStore%2F27604d2f-6f2b-4877-98d4-6b1cf0a1914b&langSwitch=true).

Following a public consultation conducted by the AMF,[48] the government and the AMF chose to create an ad hoc framework for ICOs rather than promote a best practices guide or include ICOs in the scope of the existing regulation of securities offerings.

The AMF will grant its approval (or 'visa') to public offerings of tokens that comply with the requirements set out by the PACTE Act. Obtaining the AMF's approval will be optional for all ICO issuers: no ICO will be forbidden in France for lack of approval, although unapproved ICOs will be subject to marketing restrictions. The AMF expects that ICO promoters will apply for the approval, as the global reputation of the AMF would serve as proof of their trustworthiness and help them market their ICO in foreign jurisdictions, as well as allow them to freely sell their token to French investors.

Under the PACTE Act, ICOs are explicitly separated from securities offerings. No security offering will be allowed to be carried out under the form of an ICO. Issuing a token whose characteristics would make it similar to a security (i.e., a security token) would trigger the application of corporate law.

To obtain the AMF's approval, ICO issuers will have to file an information document containing various details of the offer and the issuer.[49] This document will contain financial and legal information, but also certain technical information about the tokens and the method used to secure the cryptoassets raised during the offering (e.g., multi-signature wallets, smart contracts). The information document must be accurate, not misleading and written in plain language, and it must describe the risks associated with the offer. In a way, the information document will be similar to a white paper. In addition, the issuer will be required to be located in France – if necessary through a subsidiary or a branch.[50]

The marketing materials used by the issuer will also be reviewed by the AMF.[51] This requirement was criticised by the French community as, in theory, it would prevent the issuer from communicating its contemplated offering before the end of the approval process (which may take a few months).

In June 2019, a section dedicated to ICOs was added to the General Regulation of the AMF (i.e., the code containing detailed provisions on securities offerings, capital markets, investment funds, licensed service providers, etc.).[52] The AMF also published on 6 June 2019 an instruction that further details the approval process and the content of the information document.[53]

The legal consequences of obtaining the AMF's approval will be very similar to those of obtaining the DASP licence (see Section V). The approved ICO issuers will:

a not be arbitrarily forbidden from opening a bank account and accessing basic banking services (see Section X); and

48 AMF, 'The AMF publishes a discussion paper on Initial Coin Offerings and initiates its UNICORN programme', 26 October 2017: https://www.amf-france.org/en_US/Actualites/Communiques-de-presse/AMF/annee-2017?docId=workspace%3A%2F%2FSpacesStore%2F5097c770-e3f7-40bb-81ce-db2c95e7bdae&langSwitch=true.

49 Article L. 552-4 of the MFC.

50 Article L. 552-5 of the MFC.

51 Article L. 552-5 of the MFC.

52 Article 711-1 et seq. of the Règlement général de l'AMF.

53 AMF, Instruction DOC-2019-06, Procedure for examination of the application and establishment of an information document for approval by the AMF on an initial coin offering, 6 June 2019.

b will be allowed to broadly advertise their services to the general public, through financial or banking solicitation, online advertising or sponsorship (or all three). Similarly, the use of these marketing methods will be forbidden for unapproved ICO issuers.

In addition, as explained in Section V, approved ICO issuers will be subject to AML/CFT requirements, but only in relation to transactions received from investors during the token offering.

Finally, as for the DASP licence, the approval granted by the AMF has no extraterritorial effect and cannot be passported within the European Union.

VIII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

To our knowledge, there have been no major criminal or civil enforcement decisions related to cryptocurrencies.

Cryptocurrency-related criminal activities may be mentioned in the annual reports of Tracfin. These reports contain various descriptions of financial crime schemes involving cryptocurrencies, but do not, as a general rule, contain any information on the litigation of the case before criminal courts.[54]

IX TAX

The tax regime of cryptocurrencies and utility tokens was largely clarified following the adoption in 2018 of an ad hoc rule applicable to individual investors and the publication by the French Accounting Standards Authority (ANC) of a regulation on the accounting rules applicable to ICO issuers and investors (the ANC Regulation).[55] However, some uncertainties remain.

i Income tax treatment of individual investors

Until the adoption of the 2019 Budget Act, France was arguably one of the worst European jurisdictions for individual investors in cryptocurrencies, with a tax rate of up to 60 per cent. Cryptocurrency capital gains of individual investors are now taxed at a flat rate of 30 per cent,[56] which is still higher than in some neighbouring countries. Crypto-to-crypto transactions fall outside of the scope of the capital gains tax.[57] In practice, the taxation will be deferred until the cryptocurrencies are either sold against legal currency or used to purchase a good or service. This measure greatly simplifies tax accounting and reporting, although individual investors will still need to accurately track their transactions to be able to justify their gains.

In addition, individual taxpayers are not subject to income tax if the gains do not exceed €305 per year.

54 See, for example, Tracfin, 2017–2018 – Money Laundering and Terrorist Financing Risk – Trends and Analysis, June 2019, p. 62.

55 ANC Regulation No. 2018-07 of 10 December 2018 modifying ANC Regulation No. 2014-03 of 5 June 2014 on the national accounting code.

56 Article 150, VH *bis* of the Tax Code.

57 Article 150, VH *bis*, II, A of the Tax Code.

The 30 per cent tax rate will only apply to occasional sales of digital assets. Professional traders and miners will still be subject to the general income tax regime (i.e., a variable rate depending on their taxable income).

ii Corporate income tax – entities purchasing cryptocurrencies and ICO subscribers

Pursuant to the ANC Regulation, the accounting rules applicable to tokens issued following an ICO are also applicable to cryptocurrencies. In accordance with the Regulation, if the cryptocurrencies or tokens are held for an investment purpose, they will be recorded in a newly created account under the short-term financial instruments category, and their market value will be reassessed each year. Whether these unrealised profits or losses will be neutralised from a tax perspective is yet to be determined.

Utility tokens (tokens that are meant to be held until the services associated with them are provided or until the goods are delivered) purchased by a company will be recorded as intangible assets, and amortised or depreciated as such.

iii Corporate income tax – ICO issuers

On the issuer's side, the accounting treatment of the tokens will depend on the rights and obligations associated with the token, as follows:

a if the tokens can be assimilated (even temporarily) to a reimbursable debt, they will be recorded as 'loans and similar debts';

b if the tokens represent services to be provided or goods to be delivered in the future, they will be recorded as prepaid income; or

c otherwise, if the issuer has no implicit or explicit obligation towards the token holders, the funds collected by the issuer will be recorded as income.

In most cases, the funds collected by the issuer will eventually be recorded as income. Then, although there has been no specific regulation on this matter yet, value added tax (VAT) and income tax will have to be paid by the issuer.

iv VAT regime

In 2015, a decision of the Court of Justice of the European Union confirmed that the purchase or sale of cryptocurrencies against legal currency is exempted from VAT.[58]

With regard to utility tokens, in theory, VAT rules should be applicable, as soon as services are provided or goods are delivered in exchange for tokens. However, various technical issues have yet to be clarified (e.g., the actual value of the service provided by the token issuer is generally unknown at the time of the ICO).

X OTHER ISSUES

i Access to banking services

Access to banking services has long been one of the major struggles of French crypto-related companies. During many years, regulatory authorities only mentioned cryptocurrencies in relation to financial crime, money laundering or terrorism financing, and thus bank employees

58 Court of Justice of the European Union, 22 October 2015, C-264/14, *Skatteverket/David Hedqvist*.

are understandably wary. In addition, the ability of bank employees to open bank accounts to these companies is often limited by the bank's internal anti-money laundering policy. Many French banks prefer avoiding any exposure to activities related to cryptocurrencies to simplify their own AML/CFT reporting with their supervisory authorities.

Many start-ups report that they had their bank account frozen or closed when their bank learned that it might be used to receive funds related to cryptocurrencies. Various individuals suffered the same problem, with many retail investors reporting that their bank blocked wire transfers to bank accounts associated with cryptocurrency trading platforms such as Kraken or Coinbase.[59] As a result, many French crypto-related companies had to open bank accounts with banks located in other European countries, where the scrutiny of crypto-related activity was less strict.

In 2011, a French company that received wire transfers from European clients of MtGox (the cryptocurrency trading platform that went bankrupt in 2014) successfully argued before the Central Bank that it should benefit from the right to a bank account set forth in Article L. 312-1 of the MFC, a provision initially meant for the benefit of individuals.[60] However, the bank later managed to close the bank account by claiming that the company was operating as an unlicensed payment services provider.[61]

One of the most important provisions of the PACTE Act is the preferential access to banking services granted to three categories of entities: (1) ICO issuers that obtained the optional approval of the AMF; (2) digital asset custodians and entities allowing the purchase or sale of digital assets against legal currency; and (3) licensed digital asset services providers. Banks will have to set up objective, non-discriminatory and proportionate rules to determine whether these entities should be able to open an account in their books. Once the account is open, the entities' access to basic banking services shall not be hindered by the bank. These provisions create a strong incentive for ICO issuers and crypto-related companies to obtain an optional visa or an optional licence instead of remaining unregulated, as the right to access bank accounts will be tied to this approval or licence.

In addition, if a bank denies one of these entities the right to open an account, it shall communicate the reason for its decision to the AMF or the ACPR. Entities denied a bank account may also appeal the bank's decision.

ii General Data Protection Regulation compliance

Public blockchains seem to be at odds with certain rights guaranteed by the General Data Protection Regulation (GDPR),[62] such as the right to erasure, the right to rectification and the right to object to processing.

In September 2018, the National Commission on Informatics and Liberty (CNIL), France's data protection authority, issued an analysis on the compatibility of public and

59 *Les Echos*, 'Quand une banque interdit à son client d'investir en crypto-monnaies', 24 May 2019: https://www.lesechos.fr/finance-marches/banque-assurances/quand-une-banque-refuse-a-son-client-dinvestir-en-crypto-monnaies-1023752.

60 Court of Appeal of Paris, 26 August 2011, No. 11/15269.

61 Court of Appeal of Paris, 26 September 2013, No. 12/00161.

62 Regulation (EU) 2016/679.

permissioned blockchains with the GDPR.[63] (With regard to private blockchains, the CNIL noted that they do not raise specific issues with respect to the GDPR, as their immutability is usually not guaranteed by design.)

The CNIL stated that whenever a blockchain contains personal data, the GDPR applies. The CNIL focuses on personal data that may be uploaded to a blockchain as a way to ensure traceability of real-world documents (e.g., a diploma), but seems to acknowledge the conflict between some GDPR requirements, such as the right to erasure, and the very nature of public blockchains. In any case, the CNIL recommends not storing unencrypted personal data in a blockchain. The CNIL also announced that the challenges raised by blockchains regarding data protection would have to be addressed at EU level.

XI LOOKING AHEAD

The PACTE Act gave France a complete legal framework for ICO issuers and cryptoasset intermediaries. It is expected that the optional ICO approval and the optional DASP licence will be quite successful and encourage the development of a regulated and compliant French crypto economy.

However, many reforms still need to be made, including the following:

a With regard to tax, the tax reporting applicable to individual investors could be simplified, and shareholders should be allowed to benefit from a tax deferral when financing a company with cryptocurrencies.

b The mining industry should be supported by allowing miners to be exempted from the TICFE.

c The emerging security tokens industry urgently requires certain EU regulations and directives to be amended. The existing regulation effectively prevents the secondary market of security tokens, as securities may only be traded on a regulated trading venue, and trading on a regulated venue requires the registration of the securities with a central depositary system. In addition, the settlement of transactions on security tokens is made complicated by the current absence of a 'blockchainised' cash equivalent (i.e., the cash settlement of the transactions still needs to be conducted 'off-chain', within the legacy banking system). Various working groups have already been formed on these issues in France and at EU level.

Finally, after the European Securities and Markets Authority (ESMA) noted that the multiplication of national regimes within the European Union may create an uneven playing field and encourage regulatory arbitrage,[64] the Minister of Economy and Finance announced in April 2019 that France would support the adoption by the European Union of a legislative framework similar to the one created by the PACTE Act.[65]

63 CNIL, Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, 6 November 2018.

64 ESMA, Advice on Initial Coin Offerings and Crypto-Assets, 9 January 2019.

65 Reuters, 'France to ask EU partners to adopt its cryptocurrency regulation', 15 April 2019: https://www.reuters.com/article/us-france-cryptocurrencies/france-to-ask-eu-partners-to-adopt-its-cryptocurrency-regulation-idUSKCN1RR1Y0.

Chapter 11

GERMANY

Matthias Berberich and Tobias Wohlfarth[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

As early as 2013 – shortly after virtual currencies gained public attention and the first investor risk warnings could be heard[2] – the German financial regulatory authority (BaFin) was quick to bring virtual currencies like Bitcoin within the general financial services licensing scheme (see Section III.i). Distributed ledger technology (DLT) has developed since, and brought with it various business models based on a multitude of tradable token types as digital representations of value.

While Germany has no specific regulatory framework for virtual currencies and other virtual assets in place yet, the general financial regulatory regime applies instead, and brings various types of DLT tokens within the ambit of capital markets, banking, financial services, anti-money laundering (AML) and other laws. In some aspects, the application of these legal regimes for virtual currencies will be clarified in the near future (e.g., qualification of certain tokens and AML obligations) or is envisaged to be clarified by the legislature (e.g., use of digital registers for dematerialised securities). BaFin itself, in line with the European Union, emphasises a reasonable approach, aiming to eliminate risks to financial stability and consumers through virtual currencies, while not stifling innovation. However, the complexity of this regulatory regime with numerous and partially overlapping German and EU sources of law, as well as the initial lack of clarity in regulatory guidance by BaFin and the European Securities and Markets Authority (ESMA),[3] have led to some legal uncertainty. Regulators meanwhile acknowledge the wide variety of cryptoassets and seem to keep pace with new guidance,[4] emphasising the need for a case-by-case analysis, a technology-neutral approach, and a level playing field for similar activities and assets regardless of their form.[5] However, a clear overall picture for the vast number of applications and business models is only emerging slowly. This may be exacerbated by the lack of EU-wide regulation or, where such regulation exists, some leeway for and differences in national implementation by EU Member States.

---

1 Matthias Berberich is counsel and Tobias Wohlfarth is an associate at Hengeler Mueller Partnerschaft von Rechtsanwälten mbB.

2 EBA Opinion on virtual currencies of 4 July 2014 (EBA/op/2014/08), p. 21 et seq.

3 See ESMA statement of 13 November 2017 on ICO regulatory requirements (ESMA50-157-828); BaFin notice of 20 February 2018 (WA 11-QB 4100-2017/0010); for investor risks, see ESMA statement of 13 November 2017 (ESMA50-157-829); BaFin article in BaFin Journal November 2017, p. 15 et seq.

4 See ESMA Advice on Initial Coin Offerings and Crypto-Assets of 9 January 2019 (ESMA50-157-1391).

5 ESMA Advice on Initial Coin Offerings and Crypto-Assets of 9 January 2019 (ESMA50-157-1391); BaFin notice of 20 February 2018 (WA 11-QB 4100-2017/0010).

As a basis for this chapter, we make a distinction between three types of tokens that has proven useful in practice, namely:

a cryptocurrency tokens, which are mainly designed as a means of payment or store of value, and thus shall serve as decentralised virtual currencies for transactions with third parties or marketplaces (with Bitcoin as the prominent example);

b security tokens, which confer upon their holders access to future profits, interest or possibly some control rights over the issuer (e.g., voting rights on certain business decisions, projects, investments), and are therefore in their function similar to rights typically conferred by securities; and

c utility tokens, which do not entitle the holder to payment, but confer access to certain products or services (e.g., specific functions of the respective DLT network) that may already exist or will be developed in the future. Provided that the tokens can be traded on secondary markets, however, holders also may generate profits from the sale of utility tokens.

This classification provides a mere rule of thumb, as hybrid token forms can be easily designed and exist in various business models. Utility tokens especially may take such hybrid forms if their value proposition is not mainly access to services, but also depends on future developments and thus may have a speculative investment component driven by profit expectations through subsequent sales on secondary markets. For such tokens, the regulatory regime is briefly as follows:

a cryptocurrency tokens are regulated under banking laws (but are not considered securities), and related services may require a licence in Germany;

b security tokens will often be considered as securities so that various capital market and investment laws (with prospectus requirements) may apply;

c the regulatory treatment of utility tokens is rather unclear, with good arguments that their service-related (rather investment-related) characteristics justify not applying capital market laws, since typical investor information asymmetries are not concerned; and

d AML rules may apply to all of them.

In any case, the German regulator will engage in an individual case-by-case assessment based on the specific functional token design (form follows function).[6]

II SECURITIES AND INVESTMENT LAWS

This section provides an overview of the qualification of tokens under securities laws, prospectus requirements and liability, asset management regulation and market integrity laws.

i General qualification of tokens under securities laws

The qualification of tokens as financial instruments and, in particular, securities under the securities laws constitutes the linchpin for the application of any financial and capital market

6 BaFin Notice of 20 February 2018 (WA 11-QB 4100-2017/0010), emphasising that terminology is not decisive.

regulation. Under German and European law, a commonly accepted or uniform definition of the notion of a security – such as the *Howey* test under US securities laws[7] – does not exist. Any legal assessment of cryptocurrency tokens, security tokens or utility tokens therefore applies only with respect to the corresponding legal act.

Within an increasingly interlinked framework of EU financial regulation, the revised EU Markets in Financial Instruments Directive 2014/65/EU (MiFID II) constitutes the central reference point, as most EU regulatory acts – including prospectus laws and market abuse laws – refer to the MiFID definition of financial instruments. Under Germany's securities and banking laws, however, a different definition applies (see Section III).

Article 4 Paragraph 1 No. 15 and Section C of Annex I of MiFID II define the term financial instrument under an exhaustive enumeration of different types of instruments of which transferable securities are the most relevant in the context of token sales. Under Article 4 Paragraph 1 No. 44 MiFID II, the notion of transferable securities is defined as 'those classes of securities which are negotiable on the capital market, with the exception of payment instruments, such as: (a) shares in companies and other securities equivalent to shares in companies […] (b) bonds or other forms of securitised debt […] (c) any other securities giving the right to acquire or sell any such transferable securities […]'.

The decisive characteristic for classification as a security is therefore tradability on the capital market. This requires, more specifically, that a security – under a case-by-case-assessment – meets the formal criteria of transferability, standardisation and tradability, and is comparable to the examples of the definition from a functional perspective.

First, as regards transferability, it may generally be assumed that tokens can be transferred freely among holders by way of assignment, and that crypto exchanges allow for liquid secondary markets in those tokens (i.e., that the first criterion will regularly be met).

Secondly, a token will require a sufficient degree of standardisation. Currently, virtual currencies are standardised in the sense of a uniform structure within one issuance of tokens only, but there is no uniform token standard among different categories and types in the sense of a common protocol or platform. Taking into account that standardisation serves the purpose of tradability to allow for efficient trading, however, it becomes clear that a standardisation on the level of the individual issuance should be deemed sufficient.

Thirdly, the actual trading of tokens on crypto exchanges indicates their tradability on a capital market. The fact that tokens – immaterial by nature – cannot be acquired in good faith does not lead to a different result: distributed ledger or blockchain technology serves as a functional equivalent of a bona fide acquisition, as transactions may not be reversed for technical reasons.[8]

Fourthly, and most importantly, according to the prevailing interpretation of securities requirements, a token must be functionally comparable to one of the examples listed in the definition. This criterion substantially limits the scope of tokens qualifying as securities as it requires the token to be similar to shares, bonds or other securities traded on capital markets. Where a token promises access to future revenue streams (e.g., profit-based or interest-like) and possibly control rights, such a securities token will likely be comparable to traditional

7 Cf. Hacker/Thomale, Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law, Working Paper November 2017 (SSRN ID 3075820), p. 18.

8 BaFin Notice of 20 February 2018 (WA 11-QB 4100-2017/0010).

securities. Where, in contrast, the characteristics of tokens are rather comparable to traditional money, they should not constitute securities, as the definition explicitly excludes payment instruments.

Utility tokens that promise future access to goods or services, however, prove difficult to qualify and should be carefully assessed in light of their individual characteristics: if a token, from an objective point of view, may be regarded as an investment promising an increase in value and serves as a corporate financing instrument rather than a means of direct or immediate access to goods or services, it could potentially qualify as a security.[9] Simply put, if a token embeds 'hope and expectations' rather than access to use, its qualification as a security for the purposes of MiFID II appears likely. Whether and to what extent utility tokens should be further included in investor protection legislation is currently being discussed on an EU and German level.[10]

ii Prospectus requirements and liability

In order to provide investors with sufficient information to make an informed investment decision, thereby reducing informational asymmetries and allowing for an efficient allocation of capital, securities laws set out formal prospectus requirements.

Under the existing law, the German Securities Prospectus Act (WpPG), which implements the Prospectus Directive,[11] requires a prospectus for any public offering of securities. From 21 July 2019 onwards, the Prospectus Regulation[12] will provide a common legal basis for securities offerings in the European Union. Both legal acts require, first and foremost, securities within the meaning of MiFID II to be offered to the public. With respect to the definition under the WpPG, this understanding follows from the fact that the definition transposes the notion under the Prospectus Directive, which contains a dynamic reference to MiFID II. With respect to investments that do not qualify as securities, prospectus requirements under asset management laws may apply (see below).

Securities must be offered to the public or admitted to trading on a regulated market. With respect to (securities) token issuances, an admission to trading on a regulated market appears unlikely, as these are authorised and regulated public law institutions under the German Stock Exchange Act that require participants to be formally admitted to trading. An offer may, however, constitute an offer of securities to the public, given that the definition includes communication in any form and by any means that presents sufficient information on the terms of the offer and the securities to be offered.[13]

The WpPG and the Prospectus Regulation contain certain exemptions. In particular, thresholds with respect to institutional offerings or small offerings to retail investors apply. Both legal acts set out detailed criteria on the content of the prospectus that the issuer is obliged to draw up, submit to the national regulator for approval and publish thereafter. Under

9 Cf. Klöhn/Parhofer/Resas, 'Initial Coin Offerings (ICOs) – Markt, Ökonomik und Regulierung', *ZBB* 2018, 89, 102 et seq.; Zickgraf, 'Initial Coin Offerings – Ein Fall für das Kapitalmarktrecht?', *AG* 2018, 293, 303 et seq.

10 ESMA Advice on Initial Coin Offerings and Crypto-Assets of 9 January 2019 (ESMA50-157-1391); Federal Ministry of Finance and Federal Ministry of Justice and Consumer Protection joint discussion paper on the basic framework for the regulatory treatment of electronic securities and crypto tokens of 7 March 2019.

11 Directive 2003/71/EC.

12 Regulation (EU) 2017/1129.

13 Section 2 No. 4 WpPG, Article 2(d) Prospectus Regulation.

the Prospectus Regulation, however, EU companies that qualify as small or medium-sized enterprises (SMEs)[14] that do not fall under the exemption thresholds may also offer securities tokens to the public by taking advantage of a new simplified prospectus regime (the EU Growth prospectus).[15]

Where the prospectus (e.g., in the case of token sales often labelled as a white paper) does not provide sufficient information – that is, all necessary information material to an investor for making an informed decision – or no prospectus exists at all, the issuer or other persons responsible may be held liable towards investors.[16] Such liability may apply to the initiator or sponsor of a token sale (as the issuer) or any third party offering tokens to investors (as the offeror).

Aside from liability provisions under the prospectus laws, issuers or offerors may be subject to prospectus liability under general civil law, which is not limited to the notion of securities under MiFID II. In this case, liability does not result from a responsibility regarding information in a prospectus, but rather the violation of an independent pre-contractual duty of disclosure.

iii Asset management regulation

Collective investment undertakings

The German Capital Investment Code (KAGB) provides a comprehensive regulatory framework for the distribution, management and safekeeping of investment funds, and sets out organisational and transparency requirements for their managers and depositaries. It implements undertakings for collective investment in transferable securities (UCITS)[17] and the Alternative Investment Fund Managers Directive (AIFMD).[18] Prospective investors must be provided with detailed information in the form of a prospectus or offering memorandum. Failure to comply with the pertinent requirements will expose managers to liability claims.

The KAGB defines the central notion of investment undertaking broadly as a 'collective investment undertaking, which raises capital from a number of investors, with a view to investing it in accordance with a defined investment policy for the benefit of those investors and which is not an operative undertaking outside the financial sector'.[19] This definition, which is rooted in the AIFMD, may apply in particular to investment funds investing into cryptocurrency tokens, security tokens or utility tokens (crypto funds) or to crypto-mining ventures (mining pools) – that is, the pooling of resources to share processing power over a network and split the rewards according to the individual contribution to the pool.

14 According to Article 2(f) Prospectus Regulation, this includes companies that meet at least two of the following criteria: (i) fewer than 250 employees on average during the year, (ii) total balance sheet not exceeding €43 million and (iii) annual net turnover not exceeding €50 million.

15 Article 15 Prospectus Regulation.

16 Sections 21 to 25 WpPG, Article 11 Prospectus Regulation.

17 Directive 2009/65/EC on Undertakings for Collective Investment in Transferable Securities.

18 Directive 2011/61/EU on Alternative Investment Fund Managers.

19 Section 1 Paragraph 1 KAGB.

The scope of requirements under the KAGB further depends on the type of fund. In this respect, the KAGB distinguishes between alternative investment funds (AIFs) that are available to professional and semi-professional investors only (special AIFs),[20] and public investment funds,[21] such as public AIF and UCITS funds, that are available to retail investors.

With respect to crypto funds, the eligibility of token investments and the safekeeping of assets remain unresolved key issues, as German and European regulators have not issued any guidance on these questions yet. Public AIFs and UCITS may only invest in certain types of assets, including securities as defined under UCITS.[22] In addition, detailed rules apply to the safekeeping of assets by depositaries.[23] Currently, it appears unclear whether tokens may be held in accounts with a depositary, and how its control function should be performed in this respect.

Mining pools are likely to qualify as investment funds in the form of an AIF if the manager – irrespective of the legal structure – offers to external investors a pooled investment that diversifies risk and does not undertake any further operative business. This may be the case where cloud or hardware-based mining pools collect revenues to allow for a probabilistic distribution of mining rewards. A contribution in the form of tokens such as cryptocurrency tokens will likely qualify as the raising of capital for the purposes of the definition of an investment fund, but would constitute a contribution in kind. Under the KAGB, this form of contribution is permitted with respect to special AIFs, but not with respect to public AIFs and UCITS.[24]

Asset investments

Complementary to the KAGB, the German Asset Investment Act (VermAnlG) sets out further requirements for investments offered publicly to retail investors. It only applies to asset investments that do not qualify as investment funds under the KAGB or as securities under the WpPG, and that are distributed in a public offering. These rules may apply to tokens of any type (i.e., cryptocurrency tokens, security tokens or utility tokens), in particular where a securities token embeds certain characteristics of an investment (e.g., the promise of future revenues) but does not meet all criteria required for the qualification of a transferable security under MiFID II (e.g., where it lacks tradability owing to insufficient standardisation or barriers to transferability).

Under the VermAnlG, a token could qualify as an asset investment as defined under an exhaustive list. These include investments that grant a participation in the profits of a company, trust assets, participatory or subordinated loans, profit participation rights, registered bonds or other investments that promise interest and repayment.[25]

In the context of a typical initial coin offering (ICO), the private placement exemption under the VermAnlG is unlikely to apply as it requires that (either) no more than 20 instruments are offered, the volume of all investments offered within 12 months does not exceed €100,000 or the minimum investment exceeds €200,000 per investor.[26] Issuers

20 Section 1 Paragraph 6 s. 1 KAGB.
21 Section 1 Paragraph 6 s. 2 KAGB.
22 Sections 192 et seq. and Section 219 KAGB.
23 Sections 68 et seq. KAGB.
24 Section 71 Paragraph 1 s. 3 KAGB.
25 Section 1 Paragraph 1 VermAnlG.
26 Section 2 Paragraph 1 VermAnlG.

of certain types of asset investments may, however, benefit from privileges applicable to crowdfunding and social or charitable projects if the total volume of the issuance does not exceed €2.5 million and certain other conditions are met.[27]

Unless an exemption from the prospectus requirements applies, issuers of such asset investments are required to prepare and publish a sales prospectus and an investment information sheet that are both subject to prior BaFin approval. Anyone who assumes responsibility for a prospectus and those who are assumed to have issued a prospectus may be held liable for incorrect or incomplete information in that prospectus or in the information sheet, or for the lack thereof.

iv Market abuse rules

The efficient allocation of capital and the orderly functioning of the capital markets require rules that ensure the integrity of the financial markets and investor confidence. To that effect, market abuse laws prohibit unfair market practices. Effective as of 2016, the Market Abuse Regulation (MAR)[28] provides a common framework that prohibits the unlawful disclosure of inside information and market manipulation (market abuse). Both insider trading and market manipulation constitute criminal offences and may entail severe administrative fines.

MAR applies to any type of financial instrument that is traded or admitted to trading on a regulated market or a multilateral trading facility, as defined under MiFID II, as well as to financial instruments the price of which depends on, or has an effect on, such traded financial instruments (e.g., over-the-counter derivatives).[29] As set out above, tokens that qualify as financial instruments under EU law (i.e., security tokens and certain utility tokens) will generally be within the scope of MAR. Nothing else follows from national provisions[30] that expand the scope of MAR to goods and foreign currencies that are being traded on a domestic exchange because such an exchange – irrespective of the potential qualification of tokens as goods – includes regulated public exchanges only.

Crypto exchange operators that provide a venue to buy or sell financial instruments will typically not qualify as a regulated market, but may qualify as an alternative trading venue in the form of a multilateral trading facility provided that they match buying and selling interests in a non-discretionary manner (see also Section III.i). The consent of the issuer, an approval or listing are not required: that is, the trading of tokens on a venue that qualifies as a multilateral trading facility as such may bring it into the scope of market abuse rules.

For the purposes of MAR, inside information comprises any precise information relating to a token or its issuer that 'would be likely to have a significant effect on the prices': that is, that reasonable investors would be likely to use such information as part of the basis of their investment decisions.[31] Anyone who possesses inside information is prohibited from trading the respective instrument for its own account or that of a third party, and from recommending another person to do so, or inducing another person to do so, as such activity would constitute insider dealing.[32]

27 Sections 2a, 2b and 2c VermAnlG.
28 Regulation (EU) No. 596/2014.
29 Article 2 Paragraph 1 MAR.
30 Section 25 WpHG.
31 Article 7 Paragraph 1 MAR.
32 Article 14 MAR.

In addition, MAR also prohibits engaging in or attempting to engage in market manipulation. This concept includes any transaction, order or behaviour that could or is likely to give false or misleading price signals, or to secure prices at an abnormal or artificial level, or that employs a form of deception or contrivance as well as the dissemination of false or misleading signals or rumours in relation to a financial instrument and the transmission of such information in relation to a benchmark.[33]

Certain aspects of MAR apply to benchmarks, such as indices that financial instruments as defined under MiFID II make reference to.[34] As benchmarks may be based on any type of input data, they can relate to security tokens, cryptocurrency tokens or utility tokens. In addition, Regulation (EU) 2016/1011 on indices used as benchmarks sets out detailed requirements for the provision and use of benchmarks. Crypto market data providers may, therefore, without issuing financial instruments themselves, be subject to registration or authorisation requirements.

III BANKING AND MONEY TRANSMISSION

The core issues in the realm of banking and money transmission regimes are the statutory licence requirements that may arise under various laws and bring with them, inter alia, specific supervisory, process and compliance as well as AML obligations (see Section IV).

i German Banking Act

Banking Act licence requirements

The Banking Act (KWG) entails, in line with various EU laws, the general regulatory regime for banking and financial services in Germany. It sets out strict licence requirements not only for classical banking but also for various financial services, together with, inter alia, minimum capital requirements; management requirements (e.g., fit-and-proper tests) and risk management rules; AML and know your customer (KYC) principles; supervision requirements; and a detailed framework on various other issues.

The licence requirements depend, inter alia, on the types of assets and regulated business activity in question (see below).

Failure to obtain the necessary licences may have harsh consequences: not only can administrative proceedings be brought by BaFin (Section 37 KWG), but this may trigger criminal proceedings against responsible persons such as founders or CEOs (Section 54 KWG), who may also face personal civil liability.

For cross-border operations, which are typical for DLT networks, the BaFin takes the stance that German regulation applies not only for domestic businesses with a seat or branch in Germany,[35] but also where cross-border services (e.g., crypto exchanges located abroad) actively target the domestic market (taking into account, for example, means of advertising, language, share of transactions in Germany; however, the mere accessibility of websites in Germany is unlikely to suffice as such). A licensed financial service business can passport a

33 Article 12 Paragraph 1 MAR.

34 Article 2 Paragraph 2 c) MAR.

35 Section 53 Paragraph 1 KWG.

German licence throughout the European Union (and vice versa). In practice, cooperations with licensed banks or financial services providers are also conceivable, with the caveat that control over the business will vest with the licensed business.[36]

Regulatory trigger: tokens as financial instruments

What constitutes financial services is exhaustively defined in the KWG and entails several activities related to financial instruments. One core question is therefore whether tokens qualify as financial instruments within the meaning of the KWG.[37] This term does not fully correspond with the same term under the WpHG and MiFID II,[38] but is broader and encompasses, inter alia, units of account, which BaFin has applied under the current law since 2013 in standing practice to virtual currencies (cryptocurrency tokens). This approach was confirmed in its 2018 ICO notice,[39] where it reiterated its position that several cryptoasset-related activities may require a licence under the KWG (see below). Differentiated by token, the regulatory approach is therefore as follows: cryptocurrency tokens qualify as financial instruments under the KWG (but not MiFID II) in the specific form of units of account.[40] This category, which has so far covered units of value such as the International Monetary Fund's special drawing rights or privately issued complementary currencies, has evolved to be the new main regulatory anchor for cryptocurrencies. Although this standing administrative practice finds support in the legal literature, it should be noted that a German appellate court rejected such approach in criminal proceedings involving the operation of a Bitcoin exchange.[41] The court had doubts that such a broad reading of regulatory licensing requirements that are subject to criminal penalties is compatible with legal certainty. So far, this is a single decision and it remains to be seen how practice and other courts follow.

However, this discussion could soon become moot in the course of the implementation of Directive (EU) 2018/843 that extends anti-financial crime rules to virtual currencies. A recent legislative draft provides for a KWG amendment that will expressly define 'cryptoassets' widely as digital representations of a value that is neither issued nor guaranteed by a central bank or public entity and does not enjoy the status of a currency or money, but is accepted by natural or legal persons, as agreed or customarily, as a means of exchange, payment, or for investment purposes, and which can be transferred, stored or traded electronically (excluding e-money).[42] It should be noted, in particular, that the draft German notion of cryptoassets goes beyond the definition of the Directive as it also makes explicit reference to 'investment purposes'. Security tokens falling under MiFID II already usually qualify as financial instruments within the meaning of the KWG.[43] The same should apply with respect to cryptocurrency tokens under the expected legislation if these can be considered as a means of exchange of payment. In light of the vague wording of the draft law with respect to

36 Gebundener Vermittler, Section 25e KWG.

37 Section 1 Paragraph 11 KWG with an extensive list.

38 BaFin Notice of 20 February 2018 (WA 11-QB 4100-2017/0010).

39 BaFin Notice of 20 February 2018 (WA 11-QB 4100-2017/0010).

40 Section 1 Paragraph 11 s. 1 No. 7 KWG.

41 Higher Regional Court of Berlin, decision of 25 September 2018, Ref. No. (4) 161 Ss 28/18 (35/18).

42 Federal Ministry of Finance, Legislative draft of 20 May 2019, Draft law transposing the amending directive on the fourth EU Anti-Money Laundering Directive (Directive (EU) 2018/843).

43 Section 1 Paragraph 11 s. 1 No. 1 through 4 KWG. According to the draft law, financial instruments that already meet one of the existing categories should not (additionally) fall under the definition of cryptoassets.

'investment purposes', however, some uncertainty remains that other categories of tokens will also qualify as financial instruments within the meaning of the KWG in the future.[44] Hybrid forms of utility tokens especially will be more likely to qualify as financial instruments the more their characteristics resemble security tokens or cryptocurrency tokens. If utility token transactions also involve cryptocurrency tokens or security tokens, licence requirements may already be triggered by the latter and apply to the whole transaction.[45]

Regulation of token-related business models

Provided that tokens qualify as financial instruments, KWG licences are required for a broad range of business activities if they are performed as commerce or on a scale requiring a commercial business organisation.[46]

A KWG licence is particularly relevant and usually necessary for crypto exchange platforms and similar token trading models. Under the current law, licensing requirements here are commonly discussed on the basis that such activities may constitute investment broking[47] (where broking transactions involve the purchase and sale of financial instruments, which may also be done through an electronic platform[48]) or the operation of a multilateral trading facility[49] (which brings together multiple third-party buying and selling interests in financial instruments in the system, in accordance with non-discretionary rules and in a way that results in a contract).[50] Business models should also be assessed as to whether they might be considered as financial broking services[51] (with the purchase and sale of financial instruments in a service provider's own name but on a third party's account[52]) or contract broking[53] (where the aforementioned purchase and sale occur in a third party's name on its account[54]). The further case of proprietary trading[55] is quite broad, and involves the purchase and sales of financial instruments as a market maker, systemic internaliser or participant in markets with high-frequency trading systems, and also cases where purchases and sales on a person's own account are offered as a specific service for others.[56] This may be relevant, for example, for solicited regular buying and selling activities in virtual currencies if such activities involve a further services element (e.g., if the entity has better access to the market or creates a market by regular trading activities that would otherwise not be

44 Public BaFin statements remain vague (see only BaFin, Journal 11/2017, p. 18); dissenting Bundesverband Blockchain, Statement on Token Regulation, p. 39.

45 The provision of financial services for utility tokens that will not be acquired or disposed of in exchange for security tokens and cryptocurrency tokens will be less likely to qualify as a regulated activity under the KWG, Bundesverband Blockchain, Statement on Token Regulation, p. 27.

46 Section 1 Paragraph 1 s. 2 and Section 1a s. 2 KWG.

47 BaFin notice of 20 February 2018, WA 11-QB 4100-2017/0010.

48 Section 1 Paragraph 1a No. 1 KWG.

49 BaFin Notice of 20 February 2018 (WA 11-QB 4100-2017/0010).

50 Section 1 Paragraph 1a No. 1b KWG, similar to Article 4 Paragraph 1 No. 22 MiFID II.

51 BaFin Notice of 20 February 2018 (WA 11-QB 4100-2017/0010).

52 Section 1 Paragraph 1 s. 2 No. 4 KWG. It is reported that in 2017 BaFin closed down four exchanges of Bitcoins into euros without having a licence for financial broking.

53 BaFin Notice of 20 February 2018 (WA 11-QB 4100-2017/0010).

54 Section 1 Paragraph 1a No. 2 KWG.

55 BaFin Notice of 20 February 2018 (WA 11-QB 4100-2017/0010).

56 Section 1 Paragraph 1a s. 2 No. 4 KWG.

available for others).[57] In any case, this will require a case-by-case assessment of the technical and functional details. In addition to this, the upcoming KWG amendment will expressly bring 'crypto custody business' within the ambit of financial services, which is defined as the safekeeping, administration and safeguarding of cryptoassets or private cryptographic keys used to hold, store or transfer cryptoassets for others.[58] This will also bring wallet providers within the scope of financial services, but is not limited to such services. In this respect, too, the draft law goes beyond the definition of Directive (EU) 2018/843 as the new regulated activity also extends to the safekeeping and administration services as well as to the concept of cryptoassets.

Operating a wallet or safekeeping tokens is not seen as portfolio management or deposit business[59] for securities, given that under current German law, a security deposit business with the provision of custody and administration for others still requires securities with a tangible certificate, which DLT tokens lack[60] (but see Section XI for possible changes).

BaFin further states that in the context of ICOs, depending on the individual circumstances, underwriting business[61] (with the taking over of financial instruments at one's own risk for placement[62]) or placement business[63] (with the placement of financial instruments without a firm commitment basis[64]) require a licence.

Other typical regulated financial intermediary activities may also require a prior KWG licence if such activities are offered in connection with virtual currency business models. This may be the case for rendering investment advice[65] (in the form of personal recommendations for transactions in specified financial instruments, based on an examination of an investor's personal circumstances and not exclusively announced through information distribution channels or to the public[66]) or financial portfolio management[67] (with discretionary management of individual investments in tokens as financial instruments for others[68]).

Within that framework, other actors in a DLT ecosystem normally do not need a KWG licence. The mere use of virtual currencies as a means of payment does not require any licence; neither does operating a DLT network for token transactions as such, given that such network is a mere technical facility for effecting transactions, and not an entity for trading

57 Every transaction that is not trading on own account will qualify as dealing on own account, which normally requires no licence, unless done by undertakings within a Capital Requirements Regulation (CRR) group, engaging in other licensed banking and financial services or as participant in a multilateral trading facility or organised trading facility, or with electronic marketplace access. The question has been raised whether users of a crypto exchange, which qualifies as multilateral trading facility, who purchase or sell tokens may require a licence based on that wording. With the legislative history of the KWG and MiFID II in mind, it appears unlikely that authorities would follow such an approach.

58 Legislative draft of the Federal Ministry of Finance of 20 May 2019, Draft law transposing the amending directive on the fourth EU Anti-Money Laundering Directive (Directive (EU) 2018/843).

59 Section 1 Paragraph 1 s. 2 No. 5 KWG.

60 Section 1 Paragraph 1 DepotG. Such tangible embodiments of German securities are usually stored with Clearstream AG.

61 BaFin Notice of 20 February 2018 (WA 11-QB 4100-2017/0010).

62 Section 1 Paragraph 1 s. 2 No. 10 KWG.

63 BaFin Notice of 20 February 2018 (WA 11-QB 4100-2017/0010).

64 Section 1 Paragraph 1a s. 2 No. 1c KWG.

65 BaFin Notice of 20 February 2018 (WA 11-QB 4100-2017/0010).

66 Section 1 Paragraph 1a s. 2 No. 1a KWG.

67 BaFin Notice of 20 February 2018 (WA 11-QB 4100-2017/0010).

68 Section 1 Paragraph 1a s. 2 No. 3 KWG.

and, in particular, not a multilateral trading facility.[69] Finally, whether operations of miners will in the future fall under the activities regulated by the KWG, remains to be seen. For now, this could be the case for specific services, such as organising mining pools. Where a central pool operator would sell mined virtual currency to third parties and disburse collected money or virtual currency to individual miners, the operator could be considered as acting for a third person and engaging in proprietary trading services.

ii German Payment Services Supervision Act

Further licence requirements, which may potentially be relevant for virtual currencies, exist under the Payment Services Supervision Act (ZAG). This law, which implements the Payment Services Directive[70] and the E-money Directive,[71] regulates in essence two types of business activities, namely rendering certain (enumerated) payment services and issuing e-money. For such business activities, the ZAG sets out certain requirements, inter alia, as to management qualifications, capital requirements and risk management.[72] Structurally similar to the KWG, foreign entities require a licence if their business activities target the German market, and a ZAG licence can be passported throughout the European Union. For some KWG-licensed entities (Capital Requirements Regulation credit institutions), no additional ZAG licence is necessary.[73]

E-money

A licence is required for engaging in the business of issuing e-money.[74] E-money is defined as electronically (including magnetically) stored monetary value represented by a claim against the issuer, which is issued against the receipt of funds for the purpose of making payment transactions, and which is accepted by a natural or legal person other than the electronic money issuer.[75] Thus, where a company provides an electronic monetary value in exchange for an equal amount of (fiat) money, it will serve as an electronic means of payment for the substitution of cash. The ZAG licence covers not only issuing e-money, but also ancillary activities such as related payment services and the operation of payment systems.

While tokens can take various forms, the currently prevailing opinion is that virtual currency tokens – unlike electronic cash cards – are in the majority of cases not e-money. First, these tokens would have to be issued in exchange for (fiat) money (which is conceivable for example, in the case of pre-mined tokens, but is not the general case).[76] Secondly, this would require a monetary claim against a specific issuer, which virtual currency tokens

69 Section 1 Paragraph 1a s. 2 No. 1b KWG.

70 Directive EU 2015/2366.

71 Directive 2009/110/EC.

72 Details in Section 12 ZAG.

73 Section 1 Paragraph 1 No. 1 and 3 ZAG; Section 1 Paragraph 3d KWG.

74 Section 11 Paragraph 1 ZAG.

75 Section 1 Paragraph 2 s. 3 ZAG.

76 BaFin Notice of 22 December 2011 (as amended on 29 November 2017) on the interpretation of the Payment Services Supervision Act.

(especially cryptocurrency tokens) normally do not confer.[77] Thirdly, even if a token was seen as e-money, the ZAG licence would be the responsibility of the issuer, not the miner, for example.

Payment services

The ZAG further sets out an exhaustive list of regulated payment services.[78] Given that all such services are related to money in cash, bank accounts or e-money, but not (yet) to virtual currencies,[79] a ZAG licence becomes relevant where virtual currency transactions involve some element of processing fiat money (rather than being wholly virtual currency transactions). It is mainly for the issuing of virtual currency tokens and exchanges that the question arises of whether they are involved in rendering payment services. As such, the most relevant issues in a virtual currency context include payment initiation services[80] (which allow access to payment accounts, but without acquiring possession of the transferred money); issuing of payment instruments or acquiring of payment transactions, or both;[81] or, as a broad catch-all clause,[82] money remittance services,[83] where a payer (without any payment accounts created) pays funds to a payment service provider with the aim of transferring a corresponding amount to a payee (or another payment service provider acting on the payee's behalf), or where such funds are received on behalf of and made available to the payee, or both.

Thus, if an issuer or trader of virtual currency tokens collects fiat money to broker it on a platform with token purchasers, this may, depending on technical and functional details, constitute a regulated payment services business. The transferor and transferee of tokens are normally not subject to a ZAG licence; neither would a DLT network operator (if any) be regulated. The operation of miners does normally not fall under ZAG-regulated activities, and it is also doubtful whether operating virtual currency wallets (unlike e-money wallets) as such would require a ZAG licence.[84]

Even if activities are related to payment services, some exceptions may apply, for example, for mere technical support service providers who do not obtain possession of funds (including, for example, data processing and storage, trust and privacy protection services, authentication and communication, unless they are payment initiation and account

77 BaFin Notice of 22 December 2011 (as amended on 29 November 2017) on the interpretation of the Payment Services Supervision Act. This interpretation was confirmed by the Higher Regional Court of Berlin, decision of 25 September 2018, Ref. No. (4) 161 Ss 28/18 (35/18).

78 See Section 1 Paragraph 1 s. 2 No. 1 through 8 ZAG for a list of payment services regulated by the ZAG.

79 BaFin Notice of 22 December 2011 (as amended on 29 November 2017) on the interpretation of the Payment Services Supervision Act, No. 2.

80 Section 1 Paragraph 1 s. 2 No. 7 ZAG.

81 Section 1 Paragraph 1 s. 2 No. 5 ZAG.

82 See legislative materials, BT-Drucks. 18/11495, p. 104. The former case of digital payment business has been abandoned in the course of implementation of the Second Payment Services Directive in the ZAG, and legislative materials state that such cases will normally be within the scope of the aforementioned cases: see BT-Drucks. 18/11495, p. 104.

83 Section 1 Paragraph 1 s. 2 No. 6 ZAG.

84 It may be argued that wallets are in particular not payment authentification services (Section 1 Paragraph 1 s. 2 No. 5, Section 1 Paragraph 20 ZAG), as wallets are not personalised means or procedures agreed between a user and a payment services provider for effecting payments.

information services),[85] or commercial agent models[86] (who are authorised via agreement to negotiate or conclude the sale or purchase of goods or services on behalf of only the payer or only the payee).

IV ANTI-MONEY LAUNDERING

i General framework

Several actors in a DLT ecosystem may be subject to AML laws, namely the German Anti-Money Laundering Act (GwG), which provides, together with some AML-related provisions in the KWG,[87] the main legal basis for AML requirements under German law. The GwG transposes the Fourth Anti-Money Laundering Directive (AMLD)[88] into German law, and will soon be amended by a current legislative draft (see Section III) to implement the Fifth AMLD (AMLD 5),[89] which was adopted on 19 April 2018 by the European Parliament and must be transposed by EU Member States within 18 months. AMLD 5 will further tighten AML rules as part of the European Commission's 2016 AML action plan, which also responds to the Panama Papers revelations.

Currently, AML rules are based on a wide understanding of property that may be involved in money laundering, including assets of any kind (corporeal or incorporeal, movable or immovable, tangible or intangible),[90] so that any kind of tokens involved in criminal acts can be the object of money laundering activities. This concerns not only transactions with tokens (as the main subject matter of the transaction), but also payments with tokens (a typical virtual currency case), as long as the transacting entity is subject to the AML rules.[91]

AMLD 5 defines virtual currencies,[92] and will bring entities that provide services such as holding, storing and transferring virtual currencies into the scope of the AML obligations, which most notably apply to crypto exchanges as well as to wallet providers. The draft amendment to the KWG (see Section III.i), which defines cryptoassets as a new category of financial instruments and goes beyond the scope of the AMLD 5, could substantially expand the scope of AML requirements.

85 Section 2 Paragraph 1 No. 9 ZAG.

86 Section 2 Paragraph 1 No. 2 ZAG.

87 In addition to the GwG, financial services institutions are also subject to AML requirements under Section 25h KWG, which partially overlap with the GwG provisions.

88 Directive (EU) 2015/849.

89 Directive (EU) 2018/843.

90 Section 1 Paragraph 7 GwG.

91 In this vein (although very generic), the ESMA statement of 13 November 2017 on ICO regulatory requirements (ESMA50-157-828).

92 Under AMLD 5, virtual currencies means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and that can be transferred, stored and traded electronically.

ii AML subjects

Generally, German AML rules are based on certain listed types of obliged entities that engage in specific activities susceptible to money laundering activities.[93]

As far as is relevant in the context of virtual currencies, banking and financial service institutions that require a KWG licence (first and foremost token exchanges: see Section III.i) must generally comply with AML rules.[94] Thus, the implementation of AMLD 5 into German law will broaden the scope of AML subjects to the extent that they require a KWG licence. In particular, the operation of wallets will trigger AML obligations if a wallet provider provides the financial service of 'crypto custody business', namely the safekeeping, administration and safeguarding of cryptoassets or private cryptographic keys used to hold, store or transfer cryptoassets for others.

Similarly, AML obligations apply to undertakings if they render certain payment or e-money services and require a ZAG licence as payment institutions and e-money institutions (see Section III.ii).[95] In the (currently infrequent) event that tokens should qualify as e-money, the issuer as well as the merchant accepting such payments are also subject to AML rules.[96]

Whether and to what extent transactions with tokens trigger AML obligations of the transacting participants has not yet been entirely clarified. In general, a person trading in goods may also be subject to the AML rules under certain circumstances (e.g., handling cash payments exceeding €10,000 or in the case of specific suspicions).[97] Whether transactions with tokens (be they within an ICO by the issuer in the primary market or later on the secondary markets) qualify as trades in goods is being discussed. The Federal Ministry of Finance refers in that regard to classical civil law sales contracts,[98] which would cover only token-against-fiat transactions,[99] but arguably not the use of tokens as means of payment for, for example, other tokens or goods. In addition, the government has stated that the mere use of cryptographic currencies (without specific token qualification) should not fall under the AML rules.[100] These current ambiguities with regard to the classification under anti-money laundering laws are, however, likely to disappear in the course of the implementation of AMLD 5 owing to the explicit classification of a large number of tokens as cryptoassets (i.e., as financial instruments) and the related fact that a large number of intermediaries will qualify as obliged entities.

Finally, neither the network operation (if any such entity exists at all in a decentralised system) nor mining as such are currently regarded as AML-relevant activities.

93 Section 2 Paragraph 1 GwG.

94 Section 2 Paragraph 1 No. 1 and 2 GwG; Section 1 Paragraph 1 and 1a KWG.

95 Section 2 Paragraph 1 No. 3 GwG; Section 1 Paragraph 3 ZAG.

96 Section 2 Paragraph 1 No. 3 and 16 GwG.

97 Section 2 Paragraph 1 No. 16 GwG. Risk management requirements will only be triggered in the case of handling cash payments exceeding €10,000, Section 4 Paragraph 4 GwG. Normally, no AML representative has to be appointed. Customer due diligence requirements also apply only where the said thresholds for cash handling are reached, or there are indicators of suspicious transactions, Section 10 Paragraph 6 GwG.

98 Statement, German Federal Ministry of Finance, VII A 3–WK 5023/11/10021.

99 Bundesverband Blockchain, Statement on Token Regulation, p. 29.

100 BT-Drucks. 18/12521, S. 8. This is far from being undisputed.

iii AML duties and responsibilities

Entities subject to German AML rules must comply with various duties and responsibilities, most notably:

a establishing an adequate and effective risk management system with ongoing analysis of activity-related risks, and with customer and business-related internal security measures, which may include, for example, procedures and controls, codes of conduct or reliable compliance processes;[101]

b the appointment of a sufficiently equipped AML officer at management level in Germany (and a deputy) who is responsible for ensuring AML compliance;[102]

c customer due diligence (customer due diligence (CDD), as a KYC principle), which aims at identifying and verifying customers and beneficial owners, for example, when entering into a business relationship, where transaction values exceed certain thresholds, where indicators of suspicious transactions exist or when information provided by customers seems to be inaccurate.[103] The scope of CDD is subject to proportionality and depends on certain risk-based criteria, which may limit[104] or broaden[105] the CDD scope. In addition, CDD requires the identification of politically exposed persons; and

d reporting of suspicious transactions to the Central Financial Transaction Investigation Unit where circumstances indicate that assets originate from criminal offences relevant to AML, are related to terrorist financing or where necessary identification documents have not been provided.[106]

For some AML subjects such as persons trading in goods, the aforementioned obligations may be limited and only apply where certain thresholds are reached (e.g., transactions with cash payments exceeding €10,000) or under specific suspicious circumstances.

V REGULATION OF EXCHANGES

German law provides no specific regulation of virtual currency exchanges; however, the general rules as set out above apply (and will soon explicitly include the operation of crypto exchanges and wallet providers for cryptoassets as financial services, which require a licence). Depending on the specific activity and type of token traded, laws on securities (see Section II), banking laws (see Section III) and AML rules (see Section IV) may be applicable.

101 Section 4 through 6 GwG. In 2017, the Joint Committee of European Regulators issued guidance on risk factors for specific sectors (JC 2017 37).

102 Section 7 GwG.

103 Sections 10 through 13 GwG.

104 Simplified due diligence under Section 14 GwG, for example when transactions are conducted by a customer who is a public enterprise or agency or who has its registered office in an EU Member State or a country with similar AML and counter-terrorist financing requirements.

105 Enhanced due diligence under Section 15 GwG. For example, for transactions by politically exposed persons, transactions without any obvious economic purpose or transactions by enterprises or agencies residing in high-risk jurisdictions.

106 See Section 43 GwG.

VI REGULATION OF MINERS

German law provides no specific regulation of miners; however, the general rules set out in this chapter apply. Normally, mining as such will require no licence, but only in special cases (e.g., commercial operation of mining pools; see Section III.i).

VII REGULATION OF ISSUERS AND SPONSORS

German law provides no specific regulation of issuers; however, the general rules set out in this chapter apply. Depending on the specific activity and type of token traded, laws on securities (see Section II), banking laws (see Section III) and AML rules (see Section IV) may be applicable.

VIII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

In addition to specific criminal regulations – as set out above for insider trading and market manipulation,[107] failure to meet prospectus requirements,[108] lack of required financial licences under the KWG,[109] KAGB[110] or ZAG,[111] or money laundering[112] – virtual currency-related fraudulent activities will normally fall within the scope of general criminal law (most notably computer fraud,[113] unauthorised access to data[114] or interference with data[115]). In 2017, the German Federal Supreme Court[116] convicted operators of a botnet for mining cryptocurrency tokens that used the power of infiltrated computers for several offences of data criminality.[117] While German law does not acknowledge a theft of virtual currency in the absence of a physical embodiment, hacking and the misuse of private keys may be sanctioned as computer fraud within the context of data processing. Cases of market manipulation or transactions or ICOs with fraudulent information might also be pursued as general fraud[118] or criminal breach of trust.[119] Any proceeds from such activity may be the object of money laundering. Virtual currencies as proceeds from criminal offences – regardless of their legal character[120] – may be subject to forfeiture.[121]

107 Sections 119 Paragraph 1, 120 Paragraph 2 No. 3 WpHG in conjunction with Article 15 MAR (market manipulation); Section 119 Paragraph 3 No. 1, 2, 3 WpHG in conjunction with Article 14 MAR (insider trading).

108 Actions within the meaning of Section 35 WpPG.

109 Section 54 Paragraph 1 No. 2 in conjunction with Section 32 Paragraph 1 s. 1 KWG.

110 Section 339 Paragraph 1 KAGB.

111 Section 63 Paragraph 1 No. 4, 5 in conjunction with Section 10 Paragraph 1 s. 1, Section 34 Paragraph 1 s. 1 or Section 11 Paragraph 1 s. 1 ZAG.

112 Actions within the meaning of Section 56 Paragraph 1 GwG.

113 Section 263a StGB (Computerbetrug).

114 Section 202a StGB (Ausspähen von Daten).

115 Section 303a StGB (Datenveränderung).

116 BGH, NStZ 2018, 401.

117 Sections 202a, 303a StGB; see BGH, NStZ 2018, 401, 402 et seq.

118 Section 263 StGB (Betrug).

119 Section 266 StGB (Untreue).

120 BGH, NStZ 2018, 401, 404 et seq.

121 Section 73 StGB (Einziehung, formerly Verfall), cf. BGH, NStZ 2018, 401, 404 et seq.

Criminal liability will usually coincide with civil law damages and restitution claims,[122] but procedural details for virtual currencies have apparently not yet been litigated.[123] A transfer of virtual currencies in such cases can be enforced, for example, by handing over a private key to avoid – as generally under German civil procedure law – a penalty payment or imprisonment.[124] For virtual currencies stored in wallets, claims against the wallet provider could also be seized.[125]

Apart from criminal sanctions and private civil law enforcement, administrative enforcement is the most used measure to ensure regulatory compliance in the authorities' toolbox. In 2017, BaFin initiated 36 proceedings to verify regulatory compliance and, in four cases, closed down such operations and involved criminal prosecutors.[126] In 2018, BaFin continued to warn investors of the risks posed by ICOs and by fraudulent online trading platforms and prohibited a number of unlicensed market participants from operating.

IX TAX

While virtual currency tax issues are extensively discussed, authoritative guidance is limited. In the absence of specific virtual currency-related regulation, general German tax laws apply.

Value added Tax (VAT), following the European Court of Justice *Hedqvist* judgment[127] and guidance of the German Federal Ministry of Finance,[128] will not be triggered by a conversion of cryptocurrency tokens to fiat money (and vice versa).[129] Despite some uncertainties at the EU level,[130] the Ministry of Finance further states the same for transaction fees (or cryptocurrency tokens) received by miners.[131] In contrast, fees for services providing a wallet[132] or a cryptocurrency token exchange[133] (unless trading cryptocurrency token as intermediary on its own behalf[134]) may trigger VAT. The mere use of cryptocurrency tokens as a means of payment (instead of fiat money) has normally no influence on the qualification of transactions under tax laws,[135] but may require documenting exchange rates.[136] For utility

122 Section 823 Paragraph 2 German Civil Code (BGB); Section 812 et seq. BGB.

123 See, for example, Bundesverband Blockchain, Statement on Token Regulation, p. 38.

124 Section 888 ZPO. Issue was not answered by Cf. BGH, NStZ 2018, 401, 405.

125 Section 857 ZPO.

126 See statement of the government of 21 February 2018, BT-Drucks. 19/851, p. 2.

127 European Court of Justice, judgment of 22 October, C-264/14 – *Hedqvist*, Paragraph 53; Article 135 Paragraph 1 lit. e Directive 2006/112/EC.

128 German Federal Ministry of Finance, letter of 27 February 2018, III C 3 – S 7160-b/13/10001; Parliamentary State Secretary at the German Federal Ministry of Finance, 5 January 2018, BT-Drucks. 19/370, p. 21 et seq.

129 Section 4 No. 8 lit. b UStG.

130 Parliamentary State Secretary at the German Federal Ministry of Finance, 5 January 2018, BT-Drucks. 19/370, p. 22.

131 German Federal Ministry of Finance, letter of 27 February 2018, III C 3 – S 7160-b/13/10001, p. 2.

132 German Federal Ministry of Finance, letter of 27 February 2018, III C 3 – S 7160-b/13/10001, p. 3.

133 German Federal Ministry of Finance, letter of 27 February 2018, III C 3 – S 7160-b/13/10001, p. 3.

134 German Federal Ministry of Finance, letter of 27 February 2018, III C 3 – S 7160-b/13/10001, p. 3; Section 4 No. 8 b) UStG.

135 Statement of Parliamentary State Secretary of the Federal Ministry of Finance, BT-Drucks. 17/14062, p. 25.

136 German Federal Ministry of Finance, letter of 27 February 2018, III C 3 - S 7160-b/13/10001, p. 2.

tokens and security tokens, the absence of authoritative statements leads to some uncertainties. Some authors argue that the issue of security tokens will not trigger VAT, but that the issue and sale of utility tokens may be subject to VAT.

As it regards taxes on profits, virtual currencies are taxed in accordance with general principles: virtual currencies are immaterial assets, and profits (e.g., as the difference between the acquisition price and disposal price, or for ICOs between the book value and issue price, after the deduction of losses and expenses like platform operating costs) can, in principle, be taxed as personal income. In particular, the issuer of utility tokens in an ICO may have accounting profits taxed if a utility token is issued in exchange for cryptocurrency tokens. According to statements of the Federal Ministry of Finance, profits from occasional mining of virtual currency may also be taxed as income.[137]

Details of the tax regime vary depending on whether transactions are carried out in a private or commercial context, and by whom. In a private context, tax on personal income will accrue for individuals who realise profits such as gains in virtual currency value,[138] but only if in this context virtual currencies are held less than a year.[139] If virtual currencies are created or bought as a commercial activity, earnings from a sale or exchange may be subject to taxation as business income.[140] If done by commercially acting individuals or partnership companies, taxes will accrue as private income tax at the shareholder level; and if done by (both public and private) limited liability companies, taxes will accrue at the corporate level.

X OTHER ISSUES

Anyone commercially involved in a virtual currency business must refrain from false advertising and supplying misleading information. Thus, even in the absence of specific prospectus obligations (see Section II.ii), ICO white papers must be correct and not omit relevant information, and information on the prospects of success and economic development must not be misleading. This follows from German unfair competition law,[141] which is quite effectively enforced by competitors, business associations and consumer organisations. Furthermore, potential contractual parties are required to act truthfully, and may under special circumstances have to disclose information that is important but unknown to the other party proactively under general civil law. If they withhold such information or provide false information, they may be held liable.[142] It is argued that this may apply also for issuers of tokens.

137 Section 22 No. 3 EStG; Parliamentary State Secretary at the German Federal Ministry of Finance, 5 January 2018, BT-Drucks. 19/370, p. 21 et seq.

138 Parliamentary State Secretary at the German Federal Ministry of Finance, 5 January 2018, BT-Drucks. 19/370, p. 21 et seq.; Statement of Parliamentary State Secretary of the Federal Ministry of Finance, 21 June 2013, BT-Drucks. 17/14062, p. 25.

139 Section 23 Paragraph 1 No. 2 EStG.

140 Section 15 EStG; Parliamentary State Secretary at the German Federal Ministry of Finance, 05 January 2018, BT-Drucks. 19/370, p. 21 et seq.

141 Section 5 UWG, implementing the EU Unfair Commercial Practices Directive 2005/29/EC and the EU Misleading and Comparative Advertising Directive 2006/114/EG.

142 Sections 280 Paragraph 1, 311 Paragraph 2, 241 Paragraph 2 BGB.

Operators of internet platforms where virtual currency tokens are commercially offered may also have to comply with general e-commerce and consumer protection laws.[143] Since the legal nature of tokens may vary, some uncertainties exist as to the applicability of such regulations. While the European Central Bank (ECB) has stated that neither consumer rights nor e-commerce regulations are applicable to cryptocurrency token transactions,[144] it is conceivable that at least utility tokens could be subject to such regulation. If applicable, this would include extensive information duties (e.g., on entrepreneur's identity, modalities of online contract formation, characteristics of goods and services, costs)[145] and – rather theoretically – customer withdrawal rights in some cases.[146]

XI LOOKING AHEAD

While the current virtual currency regulation and regulatory practice are still shaped by legal uncertainty and the various national approaches of EU Member States (which means that business models have to be discussed with individual regulators), it can be assumed that, in future, regulators will cooperate more closely and provide more detailed regulatory guidance. Owing to the cross-border nature of virtual currencies and related services, it is also conceivable that further regulation will take place on an EU level, as recently recommended by ESMA,[147] or even on an international level, to create a level playing field. While the substantive virtual currency framework is widely harmonised throughout the European Union, practical differences in enforcement may remain. However, regulatory arbitrage is nonetheless limited because of looming civil law liability.

In addition to the regulatory (i.e., public law) aspects discussed in this chapter, the legal discussion about the issuance, administration and servicing of tokens increasingly takes civil and corporate law aspects into consideration. More fundamentally, use cases and activities related to securities tokens raise the question of potential efficiency gains in post-trade activities, that is, the holding, clearing and settling of securities through custody chains governed by DLT protocols. In this context, two technical concepts appear to emerge: the issuance of tokens linked to securities held by the German central securities depository (CSD) (mirror DLT securities) and the genuine issuance of tokens on a DLT platform in book-entry form (genuine DLT securities). With respect to this strand of the discussion, numerous impediments to the structuring of genuine DLT securities remain, largely owing to provisions that still require some physical form or representation of the securitised right (*in rem* concept of securities ownership). Unlike in other countries, securities issuances under German law must generally be securitised in physically stored paper certificates, which nowadays are normally issued in the form of a global note that is held by the CSD. Therefore, the safekeeping and transfer of securities issued as genuine DLT tokens will require amendments to the German safe custody law.

143 For example, with the E-Commerce Directive 2000/31/EC, Consumer Rights Directive 2011/83/EU and Financial Services Distance Marketing Directive 2002/65/EC, which are implemented in the BGB.

144 ECB, Virtual Currency Schemes, 2012, p. 44 et seq.

145 Details in Section 312d Paragraph 2 and Article 246b Introductory Act to the Civil Code (EGBGB) for B2C financial services; Section 312d BGB and Article 246a EGBGB for B2C distance selling contracts; Section 312j BGB and Article 246a EGBGB for B2C e-commerce contracts; Section 312i BGB and Article 246c EGBGB for all e-commerce contracts (including B2B).

146 Section 312g BGB.

147 ESMA Advice on Initial Coin Offerings and Crypto-Assets of 9 January 2019 (ESMA50-157-1391).

Recently, the Federal Ministry of Finance and the Federal Ministry of Justice and Consumer protection published a joint discussion paper to open German securities law for (optional) electronic issuances of securities in a technology-neutral way (including DLT) to strengthen Germany as a leading fintech centre.[148] This approach is inspired by the German Federal Debt Management Act that already provides for genuine book-entry form with regard to public sector debt (e.g., government bonds). In a first step, this concept is currently discussed for electronic bonds (and not yet for shares or investment fund units), but it could potentially serve as a blueprint for future legislation, possibly setting out a framework for a qualified digital register that might be operated by public or at least regulated entities and thus can ensure reliability of and trust in the correctness of such registers. This transition would, however, require a larger number of legislative changes in regulatory law, company law and general civil law, both at EU and national level, and could mark a true paradigm shift for German banking and capital markets regulation.

148 Federal Ministry of Finance and Federal Ministry of Justice and Consumer Protection joint discussion paper on the basic framework for the regulatory treatment of electronic securities and crypto tokens of 7 March 2019.

Chapter 12

HONG KONG

Graham Lim and Sharon Yiu[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

Increasingly, start-ups and established companies alike have sought to raise funds in Hong Kong by offering digital tokens. These are often styled as plain vanilla or utility digital tokens. However, if such tokens have the attributes of a virtual currency, or if they can be used as a store of value or a medium of exchange, various legal and regulatory issues arise.

While it is part of China, Hong Kong maintains its own domestic legal system by virtue of its status as a special administrative region. Chinese laws do not apply in Hong Kong, save as expressly listed in Annex III of the Basic Law. Accordingly, while China has moved towards an outright ban on offerings of digital tokens and virtual currencies, the position in Hong Kong is a little more nuanced.

At the time of writing, no new legislation has been introduced in Hong Kong to specifically target digital tokens or virtual currencies. Rather, reliance has been placed on existing laws, notably the Securities and Futures Ordinance (SFO),[2] to police this nascent area. At the same time, the Hong Kong authorities are keeping a watchful eye on developments. While digital tokens and virtual currencies are not legal tender in Hong Kong, an increase in their adoption as a de facto medium of exchange could well force the hand of the regulators in the near future.[3]

II SECURITIES AND INVESTMENT LAWS

The primary legislation used to regulate digital tokens in Hong Kong is the SFO. The provisions of the SFO are enforced by the Hong Kong Securities and Futures Commission (SFC), an independent statutory body that has led policing in this area.

On 5 September 2017,[4] against a background of media coverage of the stratospheric rise of Bitcoin prices and a surge in general interest in digital tokens, the SFC issued an

1 Graham Lim is a partner and Sharon Yiu is a trainee solicitor at Jones Day.

2 Chapter 571 of the Laws of Hong Kong.

3 Hong Kong (China) Legislative Council Official Record of Proceedings dated 18 December 2013. Available at http://library.legco.gov.hk:1080/record=b1162178.

4 Statement on initial coin offerings issued by the SFC dated 5 September 2017. Available at https://www.sfc.hk/web/EN/news-and-announcements/policy-statements-and-announcements/statement-on-initial-coin-offerings.html.

official statement urging the public to exercise caution in their dealings with digital tokens. The SFC also indicated that these products could constitute securities subject to regulation under the SFO.[5]

As a rule, if a digital token represents an ownership stake in its issuer's assets, or provides rights to dividends or similar payments, it could be regarded as a security in the form of a share. Similarly, if a digital token creates or evidences a debt payable to its holder, it could constitute a security in the form of a debenture. Most importantly, as a number of initial coin offerings (ICOs) in Hong Kong have previously purported to do, if a person is entitled to a share of economic returns from investments funded by the proceeds of a digital token, then that token could well represent an investment in a collective investment scheme, yet another type of security.[6] The SFC has emphasised that digital tokens that utilise blockchain technology (security tokens) are likely to be considered 'complex products' possessing a higher investment risk profile, and in turn, activities that involve advising, dealing or managing them are likely to be subject to licensing requirements.[7] To the extent a digital token constitutes a security, the conduct of various activities relating to it (including dealing in, advising on or managing them as assets) could constitute regulated activities under Schedule 5 to the SFO, for which a licence would generally be required.[8] Under the SFO, regulated activities that must be carried out with a licence are:

a Type 1: dealing in securities;
b Type 2: dealing in futures contracts;
c Type 3: leveraged foreign exchange trading;
d Type 4: advising on securities;
e Type 5: advising on futures contracts;
f Type 6: advising on corporate finance;
g Type 7: providing automated trading services;
h Type 8: securities margin financing;
i Type 9: asset management;
j Type 10: providing credit rating services;
k Type 11: dealing in over-the-counter (OTC) derivative products or advising on OTC derivative products; and
l Type 12: providing client clearing services for OTC derivative transactions.

5 Securities (as defined in Schedule 1 to the SFO) include shares, stocks, debentures, loan stocks, funds, bonds or notes of, or issued by, a body, whether incorporated or unincorporated, or a government or municipal government authority, rights, options or interests, or interests in any collective investment scheme.

6 Collective investment schemes (as defined in Schedule 1 to the SFO) are composed of four elements: they involve arrangements in respect of any property; participants do not have day-to-day control over the management of the property; the property is managed as a whole by or on behalf of the person operating the arrangements, the contributions of the participants and the profits or income from which payments are made to them are pooled, or both; and the purpose or effect of acquiring the right and interest in the property is to enable participants to participate in or receive profits, income or other returns arising or likely to arise from the acquisition of the property.

7 Statement on Security Token Offerings issued by the SFC dated 28 March 2019. Available at https://www.sfc.hk/web/EN/news-and-announcements/policy-statements-and-announcements/statement-on-security-token-offerings.html.

8 Section 114(1), SFO.

A person who carries on business in a regulated activity (or who holds himself or herself out as doing so) without an appropriate licence is liable to a fine of up to HK$5 million and to imprisonment for up to seven years.[9] As a practical matter, it is relatively easy to establish whether or not a person is appropriately licensed as the SFC maintains a public register of licensed persons on its website.[10]

While many variables are involved, if a digital token has the attributes of a security, it is generally thought that any person engaging in activities relating to that digital token could be required to obtain a Type 1 (dealing in securities), Type 4 (advising on securities) or Type 9 (asset management) licence (or more than one). Depending on the facts of each case, other types of licences could also be required. For instance, investment products tied to virtual currencies could constitute futures contracts, and activities in relation to them could be prohibited without the requisite Type 2 (dealing in futures contracts) or Type 5 (advising on futures contracts) licence.[11]

If a person, without prior authorisation from the SFC, issues an advertisement, invitation or document that is or contains an invitation to the Hong Kong public to acquire digital tokens that are, in fact, securities, he or she could be committing an offence under the SFO. This offence would be punishable by a fine of up to HK$500,000 and to imprisonment for up to three years.[12] In this regard, there are certain exemptions if the target audience is made up of professional investors pursuant to the Securities and Futures (Professional Investor) Rules[13] who satisfy certain criteria, as briefly outlined in the following table.[14]

Individuals	This includes any individual: • either alone or jointly with any of his or her spouse and children; and • who has a portfolio of not less than HK$8 million or its equivalent in any foreign currency on the date the advertisement, invitation or document in respect of the offering is issued (relevant date).
Financial institutions	As defined in Section 1 of Part 1 of Schedule 1 to the SFO, this includes: • any authorised financial institution regulated under the Banking Ordinance; • any bank that is regulated under the law of any place outside Hong Kong but is not an authorised financial institution under the Banking Ordinance;* • any authorised insurer regulated under the Insurance Ordinance;† or • any intermediary, or any other person carrying on the business of the provision of investment services and regulated under the law of any place outside Hong Kong.
Corporations	This includes: • any trust corporation that acts as a trustee in respect of trust assets of not less than HK$40 million or its equivalent in any foreign currency at the relevant date; • any corporation or partnership having a portfolio of not less than HK$8 million or its equivalent in any foreign currency, or with total assets of not less than HK$40 million or its equivalent in any foreign currency at the relevant date; or • any corporation the principal business of which is to hold investments and that at the relevant date is wholly owned by the aforesaid trust corporation, corporation or partnership.
* Chapter 155 of the Laws of Hong Kong. † Chapter 41 of the Laws of Hong Kong.	

9 Section 114(8), SFO.

10 The public register of licensed persons and registered institutions is available at https://www.sfc.hk/web/EN/regulatory-functions/intermediaries/licensing/register-of-licensees-and-registered-institutions.html.

11 Circular to Licensed Corporations and Registered Institutions on Bitcoin futures contracts and virtual currency-related investment products issued by the SFC dated 11 December 2017. Available at https://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=17EC79.

12 Section 103(4), SFO.

13 Securities and Futures (Professional Investor) Rules (Chapter 571D of the Laws and Hong Kong).

14 Section 103(3)(k), SFO.

Reliance on the professional investor exemption requires the exercise of due diligence into the background of the relevant investor. In addition, while not an absolute defence in itself, it would be prudent for a person intending to rely on this exemption to incorporate into the relevant legal documents appropriate representations, acknowledgements and disclaimers from subscribers purporting to be professional investors under the SFO.

Even if a person is licensed under the SFO, there remains an obligation to comply with specific directives and notification requirements given by the SFC from time to time. For example, the SFC has recently indicated that when providing order execution, distribution or advisory services in respect of security tokens[15] via an online platform, a licensed person must ensure that the platform provides sufficient information on the key nature, features and risks of the tokens to clients.[16] The licensed person should also comply with the notification requirements under the Securities and Futures (Licensing and Registration) (Information) Rules, and have discussions with the SFC before engaging in the regulated activities.[17] The SFC also provides guidance on the expected standards and practices in relation to virtual asset funds, regardless of whether the underlying virtual asset constitutes a security or a security token.[18]

III BANKING AND MONEY TRANSMISSION

In Hong Kong, the issuance of legal tender currency is regulated by the Legal Tender Notes Issue Ordinance.[19] Digital tokens and virtual currencies are not legal tender in Hong Kong, and form no part of the traditional banking system. Moreover, they are not transmitted via the traditional banking system. The Hong Kong Monetary Authority has consistently emphasised that digital tokens and virtual currencies such as Bitcoin are merely a type of virtual commodity[20] rather than fiat currencies backed by government authorities, echoing the position of the Basel Committee on Banking Supervision.[21]

In Hong Kong, a vendor is not obliged to accept a digital token as payment for goods and services rendered by him or her, as digital tokens are not legal tender. However, if he or she voluntarily accepts a digital taken as payment, it could be enforceable based on principles of Hong Kong contract law, absent any public policy issues.[22] In this regard, if

15 Non-complex and complex products issued by the SFC dated 12 June 2019. Available at https://www.sfc.hk/web/EN/rules-and-standards/suitability-requirement/non-complex-and-complex-products/.

16 Guidelines on Online Distribution and Advisory Platforms issued by the SFC in July 2019. Available at https://www.sfc.hk/web/EN/assets/components/codes/files-current/web/guidelines/guidelines-on-online-distribution-and-advisory-platforms/guidelines-on-online-distribution-and-advisory-platforms.pdf.

17 Circular to intermediaries on compliance with notification requirements issued by the SFC dated 1 June 2018. Available at https://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=18EC38.

18 Circular to intermediaries on distribution of virtual asset funds issued by the SFC dated 1 November 2018. Available at https://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=18EC77.

19 Chapter 65 of the Laws of Hong Kong.

20 See, for example, 'The Hong Kong Monetary Authority reminds the public to be aware of the risks associated with Bitcoin', released by the Hong Kong Monetary Authority dated 11 February 2015, available at https://www.hkma.gov.hk/eng/key-information/press-releases/2015/20150211-3.shtml.

21 BCBS Statement on Crypto-Assets issued by the Hong Kong Monetary Authority dated 18 March 2019. Available at https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190318e1.pdf.

22 Consideration for a contract need only be sufficient, but not adequate in terms of economic value. See *Chappell v. Nestle* [1960] AC 87.

the use of a digital token in this manner becomes sufficiently widespread, the Hong Kong Monetary Authority could designate it as a medium of exchange,[23] thereby requiring its issuer or operator to obtain a licence under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance.[24]

IV ANTI-MONEY LAUNDERING

Like other global financial centres, Hong Kong has a keen interest in combating money laundering and terrorist financing. Its formidable arsenal of anti-money laundering laws include:

a the Anti-Money Laundering and Counter-Terrorist Financing Ordinance;
b the Organised and Serious Crimes Ordinance;[25]
c the Drug Trafficking (Recovery of Proceeds) Ordinance;[26] and
d the United Nations (Anti-Terrorism Measures) Ordinance.[27]

At the time of writing, no new legislation has been introduced in Hong Kong to specifically target the use of digital tokens as a means of laundering money. However, given the anonymous and decentralised nature of virtual currencies such as Bitcoin, the Hong Kong authorities are acutely aware of recourse to virtual currencies by criminal elements, particularly if a virtual currency can be used as a store of value or can be readily exchanged into actual legal tender currency without a paper trail.[28]

For the moment, the existing framework of anti-money laundering laws would appear to be broad enough to capture the use of digital tokens. For instance, it is an offence under the Organised and Serious Crimes Ordinance if a person knows, or has reasonable grounds to believe, that any property[29] represents the direct or indirect proceeds of an indictable offence and deals with that property. Such an offence is punishable by a fine of up to HK$5 million and imprisonment for up to 14 years.[30]

V REGULATION OF EXCHANGES

Any platform through which digital tokens as virtual currencies can be traded in a way similar to stocks or futures is likely to be regulated under the SFO as an automated trading service. As noted in Section II, the operation of an automated trading service (ATS) is a regulated activity under the SFO that requires a Type 7 licence. An ATS is defined to cover trading

23 Section 2C of the Payment Systems and Stored Value Facilities Ordinance (Chapter 584 of the Laws of Hong Kong) provides that the Monetary Authority may, by notice published in the Gazette, declare a thing to be a medium of exchange.

24 Chapter 615 of the Laws of Hong Kong.

25 Chapter 455 of the Laws of Hong Kong.

26 Chapter 405 of the Laws of Hong Kong.

27 Chapter 575 of the Laws of Hong Kong.

28 See the Hong Kong Money Laundering and Terrorist Financing Risk Assessment Report, available at https://www.fstb.gov.hk/fsb/aml/en/doc/hk-risk-assessment-report_e.pdf.

29 Property, as defined in the Interpretation and General Clauses Ordinance (Chapter 1 of the Laws of Hong Kong), is a broadly defined term that encompasses choses in action. Contractual rights relating to digital tokens or virtual currencies are likely to have the character of a chose in action.

30 Section 25, Organised and Serious Crimes Ordinance.

services provided by electronic means where offers to sell or buy securities are regularly made or accepted in a way that results in a binding transaction.[31] An ATS provider with a Type 7 licence has to comply with rigorous requirements relating to:

a the maintenance of financial capital;
b the keeping of books and records;
c the conducting of audits;
d the safeguarding of client assets; and
e compliance with relevant codes of business conduct.

If these requirements are not met, the SFC has the right to revoke the licence of an ATS provider. A public register of licensed ATS providers is available on the SFC website.[32]

In recent times, virtual currency exchanges operating in Hong Kong have usually done so without obtaining proper authorisation. On 9 February 2018, the SFC announced that following a crackdown, at least seven virtual currency exchanges had been placed under investigation for potentially providing trading services in securities without a licence.[33] These exchanges, while not publicly identified, are understood to have subsequently confirmed to the SFC that they had ceased trading in securities, or that they had taken immediate rectification measures such as blocking access to Hong Kong residents.

VI REGULATION OF MINERS

Decentralised virtual currencies such as Bitcoin rely on mining to ensure the validity of transactions and the integrity of the underlying blockchain. Mining is known to be a difficult and laborious undertaking that would be unprofitable without powerful and specialised mining computers and access to cheap electricity. In themselves, mining activities are generally not thought of as unlawful in Hong Kong as long as they do not involve unlawful access to computer systems or sources of electricity with which to power them.

VII REGULATION OF ISSUERS AND SPONSORS

For a fuller discussion of the rules applicable to issuers or sponsors of digital tokens that constitute securities under the SFO, see Section II.

In addition, it is worth noting the specific regulatory actions taken by the SFC in Hong Kong against Black Cell Technology Limited (Black Cell).[34] Black Cell had previously advertised the uses of its digital token (known as KROPS) on its website with the pitch that the proceeds would be used to fund the development of a mobile app. The website was generally accessible by members of the Hong Kong public. On 19 March 2018, the SFC disclosed that it had taken regulatory action against Black Cell over concerns it had

31 Part 2 of Schedule 5 to the SFO.

32 The public register of authorised ATS providers is available at https://www.sfc.hk/web/EN/regulatory-functions/market-infrastructure-and-trading/approved-or-authorized-entities/register-of-automated-trading-services-authorized-under-part-iii-of-the-sfo/.

33 SFC warns of virtual currency risks issued by the SFC dated 9 February 2018. Available at https://www.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=18PR13.

34 SFC's regulatory action halts ICO to Hong Kong public issued by the SFC dated 19 March 2018. Available at https://www.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=18PR29.

engaged in unauthorised promotional activities and unlicensed regulated activities relating to securities. Following such regulatory action, Black Cell agreed to halt the sale of KROPS and to unwind all of its transactions with Hong Kong customers, even going so far as to place the following pop-up message on its website: 'The following token sale is not open for American citizens (and/or U.S. residents), Hong Kong citizens and any citizen or resident of a country that does not allow participation.'

VIII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

For a fuller discussion of the penalties applicable to violations of laws relating to digital tokens that constitute securities under the SFO, see Section II.

If elements of deception, dishonesty or fraud are involved in the offering, sale or purchase of digital tokens, offences could also arise under the Crimes Ordinance[35] and the Theft Ordinance.[36] The relevant authorities with enforcement jurisdiction would include the Hong Kong Police Force, the Commercial Crime Bureau of the Hong Kong Police Force and the Joint Financial Intelligence Unit (a joint operation of the Hong Kong Police Force and the Hong Kong Customs and Excise Department).

IX TAX

While it is beyond the scope of this chapter to provide a detailed discussion of the subject, if a digital token constitutes a security, any investment income or capital gain arising from the holding of that token would generally be subject to the same taxation principles that would otherwise apply to investments in securities.

X LOOKING AHEAD

The Hong Kong authorities continue to monitor developments in the cryptocurrency space. To raise public awareness, the SFC issues periodic statements on the legality of various ICOs and virtual currencies, and has launched various campaigns to provide the public with a better understanding of the associated investment risks.[37] The SFC also fosters communication with licensed persons to monitor potential products and services that would involve virtual currencies.[38] While it is uncertain if specific laws on virtual currencies will be enacted in the near future, the Hong Kong authorities are likely to remain vigilant in monitoring and protecting the interests of local investors and ensuring Hong Kong's continued growth as a global financial hub.

35 Chapter 200 of the Laws of Hong Kong.

36 Chapter 210 of the Laws of Hong Kong.

37 Regulation for Quality Markets – Annual Report 2017-18 published by the SFC. Available at https://www.sfc.hk/web/files/ER/Annual%20Report/2017-18/Eng/SFC_Annual_Report_2017-18_Eng_Full.pdf.

38 Vigilant | Protective | Impartial – Annual Report 2018-19 published by the SFC. Available at https://www.sfc.hk/web/files/ER/Annual%20Report/2018-19/Annual%20Report%202018-19_EN.pdf.

Chapter 13

INDIA

Vaibhav Parikh, Jaideep Reddy and Arvind Ravindranath[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

The Indian population has shown significant interest in virtual currencies. Prior to a major regulatory restriction that was introduced in April 2018, there were estimated to be around 5 million traders in India in 24 exchanges, with trading volumes in the range of 1,500 bitcoins a day.[2]

As the law currently stands, there is no clear definition of virtual currencies, crypto assets or cryptocurrencies in India. The single regulation directly on the subject of virtual currencies is a circular (the VC Circular) issued by India's central bank, the Reserve Bank of India (RBI), which restricts the use of regulated banking and payment channels for the sale and purchase of virtual currencies. The VC Circular is currently under challenge before the Supreme Court of India on constitutional grounds.[3]

Prior to the VC Circular, the RBI and the Ministry of Finance had issued warning statements about the risks associated with virtual currencies, including money laundering, consumer protection, market integrity, cybersecurity and volatility.

This shows that so far, the key government bodies, namely the government and the RBI, have significant reservations with respect to the usage of and trade in virtual currencies in India.

In July 2019, an Inter-Ministerial Committee established by the Ministry of Finance released a report on a proposed regulatory approach towards distributed ledger technology and virtual currencies. The committee has recommended an outright prohibition, along with criminal penalties, on dealing with virtual currencies.[4] It has also recommended the promotion of distributed ledger technology without the use of virtual currencies, and the exploration of a sovereign digital currency. The committee's recommendation is non-binding and is currently under consideration by the government.

---

1 Vaibhav Parikh, Jaideep Reddy and Arvind Ravindranath are lawyers at Nishith Desai Associates. The authors would like to thank Rahul Ramesh of Monash University for his research assistance.

2 https://dea.gov.in/sites/default/files/Approved%20and%20Signed%20Report%20and%20Bill%20of%20IMC%20on%20VCs%2028%20Feb%202019.pdf (13 August 2019).

3 Disclosure: the authors are advising the Internet and Mobile Association of India in the proceedings against the RBI.

4 https://dea.gov.in/sites/default/files/Approved%20and%20Signed%20Report%20and%20Bill%20of%20IMC%20on%20VCs%2028%20Feb%202019.pdf (13 August 2018).

Currently, there is no express law that classifies a virtual currency as a good, service, security, commodity, derivative or currency. The categorisation of virtual currencies into one or more of these stated classes is important, as the existing law would apply differently based on the categorisation.

At the time of writing, there are over 2,000 virtual currencies in existence,[5] all with differing properties, and their categorisation depends on their nature.[6] For instance, some are intended to be electronic cash (e.g., Bitcoin) and some are intended to be 'gas' for computer processing operations (e.g., Ether).

In our view, for the reasons described in Section X, it is likely that virtual currencies in the nature of Bitcoin and Ether will be in the nature of goods or digital products, akin to software.

As there is no specific legislation regulating virtual currency, the laws referred to in this chapter are all of general application and we have interpreted them in the context of virtual currency.

II SECURITIES AND INVESTMENT LAWS

i Virtual currencies as securities

As the law currently stands, virtual currencies in the nature of Bitcoin and Ether are unlikely to attract regulations relating to securities. The Securities Contracts (Regulation) Act 1956 (SCRA) provides a non-exhaustive definition of securities, and there is currently no regulatory guidance on its application in the virtual currency context. Virtual currencies do not fall within the enumerated items of the definition. Further, the items under the definition derive their value from an underlying asset. However, virtual currencies like Bitcoin and Ether do not have underlying assets. Rather, the value is determined purely based on demand and supply. Further, virtual currencies such as Bitcoin often do not have an identifiable issuer, unlike the items in the definition of security under Indian law.

Securities are defined in *Black's Law Dictionary*[7] to include instruments evidencing a holder's ownership rights in a firm or a holder's creditor relationship with a firm (or government). It also states that securities indicate an interest based on investment in a common enterprise. Virtual currencies, including Bitcoin and Ether, do not have such ownership rights, credit relationships or investment in a common enterprise. Therefore, such virtual currencies are unlikely to fall within the definition of securities.

However, some tokens (although not all) issued through initial coin offerings (ICOs) may fall within the ambit of the SCRA if they are issued from an Indian entity and meet the above tests. This is likely to be the case if they are issued by an identifiable issuer and are backed by the underlying assets of the issuer. Such tokens should be subject to regulation

5 https://coinmarketcap.com/all/views/all/ (13 August 2019).

6 A useful definition provided by the Financial Action Task Force is as follows: 'Virtual Currency means a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency.'

7 *Black's Law Dictionary* (10th edition 2014).

under the Companies Act 2013 (the Companies Act) (in respect of requirements surrounding the issuance and transfer of securities) and the SCRA (in respect of securities only being allowed to be listed on licensed stock exchanges).

Some issuances of virtual currency tokens may also amount to collective investment schemes, which are regulated under the Securities and Exchange Board of India Act 1992.[8]

ii Deposits

Since many token sales involve the acceptance of money or other tokens, it is relevant to analyse what regulations other than securities regulations (e.g., for tokens that do not qualify as securities) apply in such sales.

The regulations under the Companies Act and the Companies (Acceptance of Deposits) Rules 2014 (Deposits Rules) specify when the receipt of money, by way of deposit or loan or in any other form, by a company would be termed a deposit, and also provides certain exemptions from its applicability. For example, any amount received in the course of business as an advance for the supply of goods or services would not be a deposit if the advance is appropriated against the supply of such goods or services within 365 days. If a company is deemed to be accepting deposits, a variety of compliance steps under the Companies Act and its rules, along with RBI regulations, would be triggered. Only the receipt of money, and not virtual currency, would trigger these steps.

Further, after the issuance of the Banning of Unregulated Deposit Schemes Ordinance 2019, virtual currency token issuers will need to ensure, to be outside the purview of the Ordinance, that any money received should not be liable to be returned.[9]

iii Regulation as commodities

If virtual currencies are classified as commodities, the activity of operating an exchange for trading virtual currencies may be regulated as a commodities exchange, which can have implications under India's regulation on inward foreign direct investment (FDI), that is, the Consolidated FDI Policy Circular of 2017 (the FDI Policy) and the Foreign Exchange Management (Transfer or Issue of Security by a Person Resident outside India) Regulations 2017 (TISPRO).

Within the commodity space, there are two relevant concepts: a commodities spot exchange, which deals with ready delivery, and a commodities derivative exchange, which deals with derivative contracts. The FDI Policy restricts the amount of foreign investment

8 This will be the case if: (i) the contributions, or payments made by the investors, by whatever name called, are pooled and utilized for the purposes of the scheme or arrangement; (ii) the contributions or payments are made to such scheme or arrangement by the investors with a view to receive profits, income, produce or property, whether movable or immovable, from such scheme or arrangement; (iii) the property, contribution or investment forming part of scheme or arrangement, whether identifiable or not, is managed on behalf of the investors; and (iv)the investors do not have day-to-day control over the management and operation of the scheme or arrangement.

9 The term deposit includes 'an amount of money received by way of an advance or loan or in any other form, by any deposit taker with a promise to return whether after a specified period or otherwise, either in cash or in kind or in the form of a specified service, with or without any benefit in the form of interest, bonus, profit or in any other form, but does not include . . . [certain enumerated categories]'. The Ordinance provides a schedule of regulated deposit schemes, and all unregulated deposit schemes are prohibited.

into commodity spot exchanges to up to 49 per cent of the share capital, without government approval. The SCRA requires that any exchange facilitating commodity derivatives needs to be a recognised stock exchange (i.e., a licensed entity).

As the law stands, virtual currencies should not be regulated as commodities. According to a Securities and Exchange Board of India (SEBI) Circular[10] read with a central government notification[11] under the SCRA, the central government has notified certain goods for the purpose of the term commodity derivative under the SCRA and does not include any virtual currency. While this notification is only applicable to commodity derivatives and not ready delivery contracts, it provides the closest guidance on the point of what may be considered a commodity exchange at the moment.

However, the central government may at any time choose to notify virtual currencies (in general, or any class of them) as commodities under the above notification. This would bring derivatives contracts in virtual currencies within the SCRA (and hence, SEBI's jurisdiction). For spot trading, FDI would then be restricted to 49 per cent of the capital. There is currently no separate licensing regime for commodities spot exchanges.

iv FDI in Indian virtual currency-based businesses

India is a country with capital controls, where the inflow of foreign exchange into and outside the country is regulated under the Foreign Exchange Management Act 1999 (FEMA). The FDI Policy and TISPRO, made under FEMA, regulate FDI in Indian entities.

Most business models facilitating the buying and selling of virtual currencies can be characterised as e-commerce marketplaces, in which foreign investment is permitted up to 100 per cent of the capital, without government approval. The term e-commerce has been defined by TISPRO and the FDI Policy to mean 'buying and selling of goods and services including digital products over digital and electronic networks'. As discussed in Section X, virtual currencies such as Bitcoin and Ether can be characterised as goods or digital products.

However, as discussed in Section III, the operations of Indian virtual currency businesses – at least insofar as they interact with fiat currency through regulated banking and payment channels – have been severely restricted by the VC Circular. The result is that FDI issues, as a matter of practicality, are currently rendered moot, as foreign investors may not seek to invest in such companies due to the legal climate surrounding virtual currencies in India.

III BANKING AND MONEY TRANSMISSION

i Prohibition on dealing in virtual currencies

As mentioned above, the VC Circular prohibits regulated financial institutions (including banks and payment processors) from dealing with virtual currencies or providing services for facilitating any person or entity in dealing with or settling virtual currencies.[12] Entities were given a three-month window, which expired on 6 July 2018, to close any existing relationships that dealt with virtual currencies. Although the VC Circular is currently being challenged before the Supreme Court, it continues to operate in full force and effect as at the time of writing.

10 SEBI/HO/CDMRD/DMP/CIR/P/2016/105.

11 S.O. 3068(E) (Ministry of Finance, Department of Economic Affairs).

12 https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11243&Mode=0.

The effect of the VC Circular is that Indian users and businesses will not be able to use regulated banking and payment channels to deal with virtual currency. As a result, subject to a contrary decision by the courts, the VC Circular continues to severely hamper the virtual currency ecosystem in India as the means to transact between fiat currencies and virtual currencies has become heavily restricted. Traders can no longer buy virtual currencies through regulated electronic payments, and can no longer directly convert their virtual currency to Indian rupees through the banking system. They are, however, still able to use physical cash to trade in virtual currencies and to carry on trading between different virtual currencies (i.e., crypto-to-crypto trading). The lack of access to the regulated financial sector is likely to drive existing Indian businesses to explore alternative avenues, such as potentially moving abroad.

The concerns stated by the RBI in the policy statement accompanying the VC Circular were consumer protection, money laundering and market integrity. The VC Circular may actually exacerbate these concerns, as a localised cash market is harder to supervise and regulate than a transparent market working through banking channels. In addition, the VC Circular is susceptible to attack on the grounds of it infringing various fundamental rights under the Constitution.

ii Payment and Settlement Systems Act 2007

As many virtual currencies are used as a means of value exchange, questions arise as to whether any authorisation or compliance is required under the Payment and Settlement Systems Act 2007 (the PSS Act). Under Section 2(1)(i) of the PSS Act, a payment system is defined as 'a system that enables payment to be effected between a payer and a beneficiary'. If virtual currency-based systems do form payment systems, any person commencing or operating them will require the authorisation of the RBI under Section 4(1) of the PSS Act.

There is nothing in the PSS Act to exclude virtual currency, since only the term payment is referred to, as opposed to currency, legal tender or money. Therefore, it needs to be judged whether a particular cryptocurrency-based system enables payment to be effected between a payer and a beneficiary, or a person to commence or operate such system.

Arguably, many virtual currencies are not part of a system that enables payment to be effected between a payer and a beneficiary. A user may, for example, merely buy virtual currency using fiat currency for investment purposes and never choose to make any payment with it, and then dispose of it in return for fiat currency. There would be no payment, payer or beneficiary in this connection, and it would resemble the sale and purchase of an asset like gold. Further, that the value underlying the virtual currency is not backed or guaranteed by the issuing entity or any other party (i.e., holders of virtual currencies cannot redeem them for value to the issuer (other than as a sale through ordinary market channels)) supports the view that a virtual currency is likely not to be considered a payment system.

Under this view, virtual currencies can be characterised as goods or digital products that people are trading just as they would any other digital products, such as music files or e-books.

Furthermore, owing to the decentralised nature of many virtual currencies, including Bitcoin, the issuers who do commence systems as a matter of practicality cannot be identified. This would mean even if decentralised virtual currencies amount to payment systems, regulators may be unable to pursue the issuers, as they are anonymous. In addition, as is the case with decentralised virtual currencies, entities without power, influence or control over a system are unlikely to be liable for operating it, as the ledger functions independently of any operator.

Even if there is a centralised issuer, that issuer may merely create and release tokens, which are then listed on virtual currency exchanges: the issuer may not play a payment, clearing or settlement role. In this case, a virtual currency can be seen as a licence to use the particular virtual currency ledger and the licence is freely tradeable in the open market.

However, a counterargument to the above analysis can be made that a virtual currency blockchain does create a technology to enable the transfer of value from person to person, and hence enables payment to be effected between parties. According to this argument, many virtual currency blockchains may amount to payment systems, requiring the entities commencing or operating them to obtain authorisation under the PSS Act.

To date, in light of the VC Circular and the government's intent to eliminate the use of crypto assets (i.e., virtual currencies) 'as part of the payment system', as stated in the Finance Minister's 2018 Budget Speech, it is unlikely that a virtual currency business operating a payment system will successfully obtain authorisation under the PSS Act.

IV ANTI-MONEY LAUNDERING

It is often difficult for regulators to track virtual currency transactions owing to their pseudonymous nature. While wallet identities can be tracked in the blockchain, these wallet identities cannot be easily traced to individual identities. This ability to transfer something of value over the internet that can evade the conventional financial monitoring framework has raised alarm in the eyes of regulators, as they are unable to track the flow of funds that could be used for money laundering purposes.

Currently, know your customer (KYC) and anti-money laundering (AML) norms are set out under a range of different legislation and RBI directions. However, these norms do not apply specifically to virtual currency-based businesses (unless they are otherwise-regulated financial institutions). KYC/AML norms under various laws (e.g., the Prevention of Money-Laundering Act 2002 and the RBI Master Direction – Know Your Customer (KYC) Direction 2016) only apply to businesses regulated by the RBI and other regulators such as SEBI. Therefore, businesses dealing with security-related virtual currencies, as discussed in Section II, or operating payment systems, as discussed in Section III, may be subject to KYC/AML requirements.

Although KYC norms do not appear to apply to most virtual currency-related businesses, it is advisable for these businesses to follow KYC measures on the lines followed by regulated entities, especially if they accept retail users. This would enable such businesses to effectively respond to law enforcement investigations and requests for information, so as to avoid allegations of being complicit in money laundering or other fraudulent activities.

V REGULATION OF EXCHANGES

Although there is no specific regulation of the activity of virtual currency exchanges and trading platforms, the ability of such businesses to function has been severely restricted by the VC Circular. Order book exchanges will be affected, as the people party to transactions can no longer rely on the regulated banking system to convert fiat currency into virtual currency. Similarly, over-the-counter exchanges that have relied on the regulated banking system will no longer be able to do so.

Exchanges can therefore only deal with physical cash, which is impractical, or possibly facilitate exclusively crypto-to-crypto trading.

VI REGULATION OF MINERS

There is no law that specifically regulates the activity of virtual currency mining. Mining can be considered a software development activity that generates value in the form of a newly generated virtual currency (sometimes known as the block reward). Fully domestic mining as an activity therefore should only be subject to laws of general application.

While there is no judicial precedent on this issue, FEMA and its regulations may be relevant where the block reward is sent to a virtual wallet address in India and subsequently transferred abroad to a foreign wallet (see Section X). However, an arrangement where an Indian entity only provides the physical mining infrastructure and the newly generated virtual currency is availed directly by a wallet address that is held by a non-resident entity abroad should not attract the export and import-related legal obligations under FEMA. In such a situation, as the virtual currency was never held in India, there is no transfer of a virtual currency from India to a foreign country.

VII REGULATION OF ISSUERS AND SPONSORS

i Effect of VC Circular on issuers

The VC Circular restricts domestic and international entities from issuing virtual currency in exchange for fiat currency to be received through the banking system. Issuers may still issue virtual currency in consideration of other virtual currency, subject to FEMA (see subsection ii, below).

ii Securities, deposits and collective investment schemes

If a virtual currency being issued amounts to a security, deposit or collective investment scheme, the applicable legal requirements for such issuance and related ongoing compliance will be triggered.

iii Import and export regulations

The purchase, whether through fiat currency or virtual currency, by Indian residents of virtual currencies issued by international entities is subject to the import and export regulations under FEMA. Cross-border crypto-to-crypto transactions may fall afoul of FEMA from an Indian resident's perspective (see Section X).

iv ICOs

Security tokens

Indian entities issuing tokens amounting to securities under Indian law must comply with the relevant obligations under the Companies Act and the SCRA, as discussed in Section II. For example, under Sections 23 and 24 of the Companies Act, if more than 200 people subscribe to a token sale, it may be deemed a public issue that would be regulated by SEBI.[13]

Utility tokens

Issuing tokens in exchange for money or other tokens that merely act as an advance against future services (often known as utility tokens) is workable subject to – for cross-border

13 Rule 14(2) of the Companies (Prospectus and Allotment Securities) Rules 2014.

issuances – the FEMA issues discussed in Section X. However, if such advance is not appropriated against the actual services within 365 days, the amount may be considered a deposit under the Companies Act and the Deposits Rules, as discussed in Section II. Thus, utility token issuers wishing to avoid the restrictions on deposits can contractually ensure that the services are supplied within the required 365-day period.

Payment tokens

These tokens are intended to be used as a means of payment for trading goods or services, as a form of money or value. Unlike utility tokens, they do not give rise to claims for goods or services against their issuer.

From an Indian law perspective, if the blockchain relating to a token forms a payment system requiring authorisation under the PSS Act, then, as discussed in Section III.ii, the entity that commences or operates such a system may be required to be authorised by the RBI.

VIII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

There are no laws specifically targeting fraud in the virtual currency sector.

However, although it may be a common misconception in India that virtual currency businesses are operating in a completely unregulated space, this is not the case. Various laws of general application, such as the Indian Penal Code 1860 (IPC), the Prize Chits and Money Circulation Schemes (Banning) Act 1978 (the Prize Chits Act) and the Consumer Protection Act 1986 (CPA), will act against fraudulent business activity. Action has already been taken by authorities under the IPC and Prize Chits Act against fraudulent virtual currency-based businesses.[14] The IPC and the Prize Chits Act are criminal laws, while the CPA provides a civil remedy.

Sections 415 to 420 of the IPC criminalise cheating. If any person (thus including a virtual currency business) 'fraudulently induces [a deceived person] to deliver any property to any person', and that act causes or is likely to cause damage to the deceived person, he or she can be penalised under Sections 417 and 420. Similarly, the Prize Chits Act penalises schemes for the making of quick or easy money (money circulation schemes) and various types of prize distribution schemes (prize chits).

The CPA protects consumers against unfair trade practices, deficiencies in services and defects in goods. Unfair trade practices include false or misleading advertising. As a result, if any virtual currency business makes misrepresentations to consumers or provides deficient services, consumers will have recourse under the CPA.

IX TAX

In India, taxes may be on income (direct taxes) or expenditure (indirect taxes). Taxation of virtual currency-related activity can therefore be discussed under two heads: income tax (direct tax) and goods and services tax (GST) (indirect tax).

14 https://timesofindia.indiatimes.com/city/navi-mumbai/one-coin-fraud-18-in-cop-custody/articleshow/58439996.cms.

i Direct tax

Taxation of income is governed by the provisions of the Income Tax Act 1961 (ITA). Under the ITA, Indian residents are subject to tax in India on their worldwide income, whereas non-residents are taxed only on income sourced in India. However, non-residents who are residents of a country with which India has signed a tax treaty have the option of being taxed as per the tax treaty or the ITA, whichever is more beneficial.

Under the ITA, the key issue is whether income from virtual currency is treated as capital gains or profits and gains of business or profession. For instance, if a seller is a trader by occupation, the income should be taxed as business income. If it is not business income, it would be taxed in the nature of capital gains. However, this is not yet clear under Indian law, which makes it difficult to conclude how virtual currencies may be taxed. The ITA and its associated rules do not specifically refer to the treatment of virtual currencies, and there have been no judicial precedents in this regard.

Rather than taking a blanket view, when interpreting the ITA the facts and circumstances of each transaction should be kept in mind, because individuals and corporates may deal with virtual currencies in a variety of contexts, sometimes as capital assets and sometimes in the course of business.

The income tax authorities recently sent notices to several persons dealing in virtual currency, asking for explanations regarding their virtual currency gains.[15]

ii Indirect tax

The relevant laws concerning GST are the Central Goods and Services Tax Act 2017, the Integrated Goods and Services Tax Act 2017 and the respective State Goods and Services Tax Acts, which each have different jurisdictional ambits.

GST is payable on:

a sales of goods where goods are sold within one state in India;
b sales of goods where goods are transported from one state to another state;
c the provision of services within one state in India; and
d the provision of services from one state to another state in India.

The Tariff Schedule for Goods currently contains no specific category for virtual currencies, but does contain a residuary category of goods. Virtual currencies may therefore (assuming they are treated as goods for the reasons discussed in Section X) fall within the residuary category. Under the GST regime, GST is chargeable on transactions where goods are supplied in the course or furtherance of business. As there are a multitude of virtual currencies and each transaction varies in nature, determinations must be made on a case-by-case basis as to whether GST is to be paid. Persons selling goods in the course or furtherance of business and requiring GST registration (which registration depends on persons meeting an annual revenue threshold) are required to include GST in their sale invoices.

Additionally, GST should be payable with respect to services provided (e.g., services of a trading exchange) in connection with the sale and purchase of virtual currencies. Where

15 https://www.ndtv.com/business/income-tax-i-t-department-sends-notices-to-cryptocurrency-investors-cbdt-chairman-budget-1809377.

a person casually sells virtual currencies as a hobby, there should be no GST consequences. Sales of virtual currencies where they were initially held as an investment should also attract no GST liability.

Double taxation issues may arise where consumers might be subject to GST while purchasing virtual currencies, and again on their use in exchange for other goods and services that are in turn subject to GST. These issues have yet to have been accounted for by the GST regime.

It should be noted that the above analysis is based on our analysis of GST provisions as they apply generally, and is not specific government guidance on the application of GST to virtual currencies. Recent reports suggest that the Central Board of Indirect Taxes and Customs and the GST Council are deliberating whether and how to bring virtual currencies within the GST regime.[16]

X OTHER ISSUES

i Foreign exchange control

Cross-border transfers of virtual currencies, or cross-border remittances for the purchase or sale of the same, raise questions under FEMA.

Nature of virtual currencies under FEMA

There is no express definition of goods under FEMA. However, according to the Foreign Exchange Management (Export of Goods & Services) Regulations 2015, goods and software are treated alike, and 'software means any computer program, database, drawing, design, audio/video signals, any information by whatever name called in or on any medium other than in or on any physical medium'. As virtual currencies are information, it would appear that they fall within the aforesaid definition of software.

Further, in the case of *Tata Consultancy Services v. State of Andhra Pradesh*,[17] in a decision of a constitution bench of the Supreme Court of India, the Court heard whether certain software would fall within the meaning of goods under a state sales tax law. The majority held that the term 'goods' as used in the Constitution of India and under the Sales Tax Act is 'very wide and includes all types of movable properties, whether those properties be tangible or intangible', 'the moment copies are made and marketed, it becomes goods', and 'a transaction sale of computer software is clearly a sale of 'goods' within the meaning of the [relevant Sales Tax Act]', and 'the term "all materials, articles and commodities" includes both tangible and intangible/incorporeal property which is capable of abstraction, consumption and use and which can be transmitted, transferred, delivered, stored, possessed etc'. In the concurring opinion by Honourable Justice Sinha, a three-part test was laid down for when a software would become goods.[18]

16 https://www.bloombergquint.com/gst/2018/05/23/india-mulls-gst-on-trading-of-virtual-currencies.

17 *Tata Consultancy Services v. State of Andhra Pradesh* (2004).

18 'Goods may be tangible property or intangible property. It would become goods provided it has the attributes thereof having regard to (a) its utility; (b) capable of being bought and sold; and (c) capable of transmitted, transferred, delivered, stored and possessed. If a software whether customized or non-customized satisfies these attributes, the same would be goods.'

While the judgment was not in the context of a virtual currency or the definition of goods under FEMA, it provides useful interpretational guidance, since the term goods has not been defined under FEMA.

Virtual currencies are intangible, and are made and marketed and stored on physical servers. They are capable of being bought and sold, as well as transmitted, transferred, delivered, stored and possessed. It may be argued that virtual currencies do not possess utility. However, virtual currencies such as Bitcoin and Ethereum are used for various purposes, including being a store of value, a means of exchange (including for micro-payments) and decentralised applications. Demand for such virtual currencies further indicates their utility. Therefore, based on the text of the law as it stands, virtual currencies such as Bitcoin and Ether are closest in nature to goods under FEMA.

On the other hand, the definition of currency under FEMA is an enumerated list, and includes 'any instrument which can be used to create a financial liability'. Virtual currencies are not named under any of the enumerated categories, and in the case of virtual currencies such as Bitcoin, there is no entity that is accepting financial liability in connection with the instrument. The RBI, in response to a right to information request, has also stated that it does not classify virtual currencies as currencies under FEMA, and no guidelines have been framed on virtual currencies under FEMA. Therefore, it is also possible that the RBI does not consider virtual currencies as 'goods' under FEMA.

It should be noted that there has been no express classification of virtual currencies under FEMA, and the above discussion is only intended to highlight some plausible interpretations as at the time of writing.

Cross-border transactions in virtual currencies

If a virtual currency is sent outside India by Indian residents as payment for services rendered or goods (including other virtual currencies) sold by a non-resident entity, then the transaction is likely to be characterised as an export of goods regulated under the Foreign Exchange Management (Export of Goods & Services) Regulations 2015 and the Master Directions on Export of Goods and Services (together, the Export Regulations). The Export Regulations require, inter alia, that the full value of any exports be received only via authorised banking channels (i.e., in fiat currency) and that any set-off of import payments against export receivables only happen through a process facilitated by the authorised bank. This means that cross-border barter would not be permitted. Thus, the cross-border transfer by Indian residents of virtual currencies without receiving fiat currencies through authorised banking channels is likely to violate the Export Regulations.

The export-related obligations are on the exporter: that is, usually the Indian resident and not the foreign recipient. As such, foreign recipients, unless they specifically target Indian residents, may be able to ring-fence themselves from the above provisions.

Previously, the import-related provisions under FEMA could be used to potentially justify some types of outward remittances of fiat currency for the purchase of virtual currency. However, as the position now stands as a result of the VC Circular, banks are obliged to refuse the drawing of foreign currency for the purpose of importing virtual currencies. Thus, the import of virtual currencies into India using an outward remittance of fiat currency is likely to be refused by banks.

ii Stablecoins

Stablecoins are units of value that are usually issued by an identifiable entity, and, as the name suggests, are intended to be relatively immune to price swings.[19] This is achieved by the stablecoins being 'backed' by underlying fiat currencies or other traditional assets like gold. A stablecoin issuer may operate by maintaining a reserve of these assets at a given ratio to every unit of cryptocurrency issued. The issuer would generally allow holders of the stablecoin to redeem each stablecoin for its equivalent value in fiat currency. Some examples of stablecoins currently in the market are TrueUSD and Tether, which are attempting to be pegged in price to the US dollar. Recent announcements of proposed new stablecoins by various large enterprises show that stablecoins are gathering mainstream corporate momentum.

There is no Indian law that is specifically applicable to stablecoins. The following issues should be analysed:

a whether a given stablecoin would amount to currency under FEMA, since the term currency includes any 'instrument by whatever name called that can be used to create a financial liability';[20]

b whether a given stablecoin system would amount to a payment system under the PSS Act (i.e., a system that enables payment between a payer and a beneficiary); and

c whether a given stablecoin would amount to a virtual currency as defined under the VC Circular.

These issues are interesting questions in the context of Indian law and should be examined carefully on a case-by-case basis, as each stablecoin may have varying legal characteristics.

XI LOOKING AHEAD

The law in India on virtual currencies is in flux. There is a pending Supreme Court case against the VC Circular, as well as a multi-stakeholder government committee that has now submitted its report to the government, as discussed in Section I. In our view, the report's recommendation of an outright ban, along with criminal penalties, is excessive, as the risks involved with virtual currencies can be addressed with less invasive measures. International bodies such as the G20 and the Financial Action Task Force, and leading jurisdictions such as the European Union, Singapore, the United Kingdom and the United States, have all proposed regulatory approaches to address the risks, so that the benefits are not lost out on.

Prior to the committee report, the government made several pro-blockchain statements in various reports and press statements, but continually cautioned against the risks associated with virtual currencies.

In our view, blockchain as a system would be rendered either impotent or severely restricted (depending on the blockchain implementation) without any virtual currency or crypto-token. This has been recognised by several global experts, including Ethereum co-founder Vitalik Buterin and author Andreas Antonopoulos. These tokens act as an incentive to blockchain participants to verify transactions, and hence preserve decentralisation, which is the very breakthrough of blockchain technology. As a result, it may not be a wise policy to try to promote blockchain on the one hand, and then severely restrict tokens on the other.

19 E.g., https://www.gdf.io/wp-content/uploads/2019/05/GDF-Stablecoin-Key-Considerations_9-MAY-SUMMIT-DISCUSSION.pdf.

20 https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10267&Mode=0.

The current stance espoused by the VC Circular appears to be borne from a negative impression that media reports may have created after incidents of fraud, such as the WannaCry ransomware, activities on the dark web and certain Ponzi schemes. However, virtual currencies also bring with them several benefits, most notably disintermediation and cost savings. Outright restrictions on this technology are impractical and might be relatively straightforward to circumvent. Rather, as with all disruptive technologies, balanced regulation should be adopted to mitigate the risks and promote the benefits. It is our hope that any impending government decision recognises this fact, and adopts a nuanced framework towards this.

Some uncertainty may continue to prevail in India until industry and regulatory understanding matures both domestically and globally; however, our long-term view is positive. The implementation of successful regulatory models in other jurisdictions should also hasten progress towards a balanced regime.

Chapter 14

IRELAND

Maura McLaughlin, Pearse Ryan, Caroline Devlin and Declan McBride[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

The Central Bank of Ireland (CBI) is the authority responsible for the regulation of financial services in Ireland. To date, the CBI has not issued specific guidance dealing with the status or the legality or illegality of virtual currencies or blockchain, and neither has any government department or other public authority. They have also remained largely silent on the applicability of existing financial regulation regarding this new and emerging area. However, the CBI has issued a warning on the dangers associated with cryptocurrencies as well as an Alert on Initial Coin Offerings to warn investors about the risk of losing part or all of their invested money (see Section II).

The Department of Finance issued a discussion paper on virtual currencies and blockchain technology in March 2018, stating that it believes that no single state agency has the capabilities to address all the risks and opportunities in these two areas. The Department is also in the process of establishing an interdepartmental working group whose task it will be to deal with the various issues involved and consider any policy recommendations that will be potentially necessary.

A notable exception to the lack of clear guidance being issued is the Irish Revenue Commissioners. While there are no specific rules dealing with the taxation of virtual currencies, the Revenue Commissioners published information on the taxation of virtual currency transactions in 2018 (see Section IX).

II SECURITIES AND INVESTMENT LAWS

There is no specific virtual currency regulation in Ireland, and regulators have yet to indicate the extent to which existing securities regulation will apply to virtual currencies. The CBI is the competent authority for the purposes of securities law in Ireland, including regarding prospectus, transparency, market abuse and markets in financial instruments law. The principal legislation to be aware of in respect of virtual currencies has its roots in European Union law, and includes the Prospectus Directive, the 2014 European Union Markets in Financial Instruments Directive (MiFID II) and the Alternative Investment Fund Managers Directive.

1 Maura McLaughlin, Pearse Ryan and Caroline Devlin are partners, and Declan McBride is of counsel, at Arthur Cox.

The CBI has not only published its own warnings in relation to initial coin offerings (ICOs) and virtual currencies, but has also contributed to European Securities and Markets Authority (ESMA) warnings to both consumers and firms engaged in ICOs.

In respect of the application of securities laws to virtual currency regulation, we expect that the CBI will focus on the recognised EU concepts of transferable security and financial instruments as defined in MiFID II, and the characteristics that they view as bringing virtual currencies within those definitions. Depending on their structure, virtual currencies could be classified as transferable securities requiring the publication of a prospectus (or availing of an exemption) prior to their being offered to the public. A pure, decentralised cryptocurrency is unlikely to be a transferable security, while a token with characteristics similar to a traditional share or bond may be. It is also possible that true utility tokens intended for exclusive use on a platform or service will not be transferable securities. The definition of transferable security is non-exhaustive, and it is for each issuer and their advisers to determine whether their cryptocurrency or token is a transferable security.

As in many jurisdictions, the regulatory environment in relation to cryptocurrencies and their interaction with securities law is not yet settled, and ESMA acknowledges that, depending on how an ICO is structured, it may fall outside the regulated space entirely.

III BANKING AND MONEY TRANSMISSION

In Ireland, virtual currency is not regarded as either money or fiat currency. Therefore, virtual currency is typically viewed as being outside the scope of many traditional financial regulatory regimes: for example, deposit taking, electronic money or payment systems.

There is a risk that certain ancillary services in connection with a virtual currency could be subject to regulation as a form of money remittance or transmission under the Payment Services Directive (PSD), or, where the PSD does not apply, under the Irish regulatory regime for money transmission. For example, the operator of a virtual currency platform who settles payments of fiat currency between the buyers and sellers of virtual currency could be viewed as being engaged in the regulated activities of money remittance or transmission. There are a number of exemptions that may be applicable where, for example, the platform operator is acting as a commercial agent or where the platform could be viewed as a securities settlement system. The application of an exemption would depend on the features of the trading platform.

IV ANTI-MONEY LAUNDERING

The application of existing Irish anti-money laundering requirements to virtual currency is unclear due to uncertainty surrounding the regulatory status of virtual currency. Where a virtual currency or any activity relating to it is subject to regulation (e.g., it has the characteristics of a transferable security), Irish anti-money laundering requirements will apply.

The Fifth Anti-Money Laundering Directive (AMLD5) will impose new anti-money laundering requirements on virtual currency exchanges and custodians operating in Europe. AMLD5 has not yet been implemented in Ireland.

V REGULATION OF EXCHANGES

The operation of a multilateral system that brings together multiple third parties buying and selling financial instruments is a regulated activity under MiFID II that would require an authorisation. There is a risk that a virtual currency exchange could require authorisation under MIFID II where the virtual currencies are financial instruments within the meaning of MIFID II (see Section II). Depending on their structure, virtual currencies could be classified as transferable securities for the purposes of MIFID II. The risk increases where the virtual currency has features similar to a share or a bond.

VI REGULATION OF MINERS

There are no restrictions in Ireland on the mining of virtual currency. Where a virtual currency is a form of transferable security, mining activity could be viewed as a form of securities settlement system. However, as mining is carried out on a decentralised basis, it does not fit neatly into any existing regime for securities settlement. On that basis, we would view mining as an unregulated activity under Irish law.

VII REGULATION OF ISSUERS AND SPONSORS

There are no specific regulations applicable to virtual currency issuers or sponsors in Ireland. Rather, they are subject to the existing regulatory frameworks governing traditional securities. In the event that an issuer's virtual currency is a transferable security (which must be determined on a case-by-case basis), the issuer must prepare (and have the CBI approve) a prospectus prior to offering the token for sale to the public, assuming that the sale of the virtual currency would not proceed as an exempt offer pursuant to an exemption contained within the Prospectus Directive. The CBI has stated that it has received initial enquiries from certain virtual currency issuers and sponsors to review such a prospectus; however, we are not yet aware of any token issuers who are engaging with the CBI regarding a formal prospectus.

In the event that a virtual currency does not constitute a transferable security, the requirements of the Prospectus Directive will not apply to its issuance, although ordinary contractual principles and civil liability would continue to be relevant for issuers and sponsors.

See also Section II.

VIII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

As stated previously, there is no specific regulation in Ireland dealing with cryptocurrencies or blockchain technology generally. While the same is also true of the area of criminal and civil fraud and enforcement, it is important to be aware of existing financial services regulation covering areas into which certain activities relating to cryptocurrencies and blockchain might fall.

There is the possibility that various ancillary services connected with cryptocurrencies could be considered regulated activities under either the PSD or other Irish money transmission regulations. Irish anti-money laundering legislation will apply in cases where, for example, a cryptocurrency is considered a transferable security (see Section IV). AMLD5 will impose new regulation on cryptocurrency exchanges in Europe, but has yet to be transposed into Irish law.

As stated above, the CBI has issued a warning in relation to ICOs. While virtual currencies have not yet been classified as securities by the CBI, there has also been no conclusive statement to the contrary. In the absence of final clarification, it is important to be aware that any person breaching the Prospectus (Directive 2003/71/EC) Regulations 2005 by offering securities to the public without publication of a prospectus (for an offer not subject to an exemption) is liable on summary conviction to a maximum fine of €5,000 and 12 months' imprisonment, or on indictment to a maximum fine not exceeding €1 million or imprisonment for five years, as there is the possibility that ICOs can be considered to be such an offering of securities to the public, depending on their structure (see also Sections II and VII).

IX TAX

There are no specific rules for dealings in cryptocurrencies, and the normal basic principles apply. This was confirmed in a publication issued by the Revenue Commissioners in May 2018. The taxation of dealings in cryptocurrencies will depend on the nature of the activities. Thus, the receipt of a cryptocurrency (by way of barter) in lieu of cash for goods or services rendered may be treated as an income or capital receipt, and in turn may or may not be trading, all of which depends on the underlying activity that generated the cryptocurrency. This requires a normal review of the facts. While cryptocurrencies themselves can be difficult to value, the value of a cryptocurrency on the date of a transaction is the relevant figure to be considered for tax purposes. The Revenue Commissioners recognise the practical difficulties in valuation given that there is no one exchange: a practical and reasonable approach is needed, and taxpayers are required to keep contemporaneous records, as this information often cannot generally be verified at a later date.

Dealing in cryptocurrencies of themselves will depend on the nature and level of activity of the dealer. Occasional investment in and disposals of cryptocurrencies would likely be treated as a capital receipt, currently taxed under capital gains tax at a rate of 33 per cent. Where there is significant and regular dealing, this could be considered to be trading, which for a company would be taxed at 12.5 per cent, or at the marginal higher rates for individuals. The actual tax position will depend on an analysis of the specifics of each transaction, and would need a case-by-case consideration, as is normal in any activity.

No Irish VAT arises on the transfer of cryptocurrencies. This follows the ruling in the *Hedqvist* European Court of Justice case in 2014, and the Revenue Commissioners have confirmed that this accords with their view. It is worth bearing in mind that where a cryptocurrency is exchanged for goods and services, while there is no VAT on the supply of that cryptocurrency, the goods or services given in exchange may themselves attract VAT in the normal way.

Irish stamp duty should not arise generally on a transfer of cryptocurrencies, although as stamp duty is a tax on documents, the manner in which the transfer takes place would be worth monitoring to ensure that a stampable document has not been created.

The territoriality aspect of cryptocurrencies is still an evolving area. Irish resident (and for individuals, ordinarily resident) persons will usually be liable to tax in Ireland on their worldwide income and gains (subject to any reliefs or exemptions, including double tax treaty reliefs). A non-resident person will generally only be subject to tax on Irish-sourced income or gains, or profits from an Irish trade. (In the case of individuals, tax may also apply where

amounts are remitted into Ireland.) It is evident, therefore, that understanding the source or situs of cryptocurrencies is of significance in international dealings. This is likely to be an area that will be developed further.

Applying general principles and no special rules to cryptocurrencies allows taxpayers to conduct their activities with a level of certainty, and the Revenue Commissioners guidance is a welcome development.

X OTHER ISSUES

Given the importance of the investment funds industry to Ireland as a destination for international financial services, the implications for the virtual currencies sector need to be considered.

Investment managers are not generally restricted from owning and investing cryptocurrencies, and the licensing requirements do not differ from the usual requirements in this area. Nonetheless, it needs to be borne in mind that the CBI has yet to state its position on the classification of cryptocurrencies, which will potentially change the situation.

XI LOOKING AHEAD

Virtual currencies, and blockchain technology generally, are important areas of innovation and part of a growing technology ecosystem in Ireland. Their importance is exemplified in the setting up of Blockchain Ireland,[2] a group dedicated to promoting and providing information on DLT and blockchain in Ireland that is chaired by the Industrial Development Authority and with broad public and private sector membership, and also by the CBI announcement that it is in the process of establishing a fintech and innovation hub to enable companies to engage directly with the CBI.

It can therefore be expected that the CBI and government departments and public authorities will issue more guidance on the application of existing regulations to, and classification of, these new and emerging technologies in the short to medium term.

The transposition of the AMLD5 will also have an important impact on the way cryptocurrency exchanges are regulated in Ireland.

2 https://www.blockchainireland.net/.

Chapter 15

JAPAN

Ken Kawai and Takeshi Nagase[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

Japan has emerged as one of the largest cryptoasset markets globally, and was the first country to establish a regulatory framework for cryptoassets.[2] In addition to enabling the registration of cryptoasset exchange service providers (exchange providers) wishing to provide cryptoasset exchange services (exchange services) to residents in Japan, this framework seeks to protect cryptoasset exchange customers and to prevent cryptoasset-related money laundering and terrorism financing.

The upsurge of the Japanese cryptoasset market was, however, disrupted in January 2018, when one of the largest cryptoasset exchanges in Japan announced losses of approximately US$530 million from a cyberattack on its network. Adding to the negative publicity, cryptoassets were also increasingly being used for speculative purposes, rather than as a means of settlement.

To remedy the situation, the Financial Services Agency of Japan (FSA) in March 2018 established a Study Group on Crypto Asset Exchange Business, etc. (the Study Group) to assess the adequacy of regulatory measures in addressing issues surrounding exchange services. This was followed by the publication of the Study Group's report (the Report) on 21 December 2018. In addition to summarising the results of the Study Group's deliberations, the Report also proposed a new legal framework for the governance of cryptoassets. This led to the introduction of a bill for the revision of certain legislation governing cryptoassets (the Bill). Tabled before the Diet on 15 March 2019, the Bill contains proposed revisions to the Payment Services Act (PSA) (the PSA Revisions), based mainly on the proposals in the Report. At the same time, the Bill proposes revisions to the Financial Instruments and Exchange ACT (FIEA) (the FIEA Revisions) and to the Act on Sales, etc. of Financial Instruments (ASFI) (the ASFI Revisions), primarily for purposes of strengthening the regulatory framework surrounding cryptoassets. The Bill was passed by both chambers of the Diet on 31 May 2019, and will come into force within a year of its introduction. It is expected to significantly reshape the regulatory landscape surrounding cryptoassets in Japan.

The key provisions of the FIEA Revisions are to: (1) establish electronically recorded transferable rights (ERTRs) and regulations applicable thereto; (2) introduce regulations governing cryptoasset derivative transactions; and (3) introduce regulations governing unfair acts in cryptoasset or cryptoasset derivative transactions.

---

1 Ken Kawai is a partner and Takeshi Nagase is a senior associate at Anderson Mori & Tomotsune.

2 As noted in Section V, the term 'virtual currency' has been revised to 'cryptoasset' under the PSA Revisions. For the purposes of this chapter, only the term 'cryptoasset' is used.

The key provisions of the PSA Revisions are to: (1) revise the term 'virtual currency' to 'cryptoasset'; (2) enhance regulations governing cryptoasset custody services; and (3) tighten regulations governing exchange services.

The ASFI Revisions apply the ASFI to cryptoasset sales and similar transactions.

II SECURITIES AND INVESTMENT LAWS

i Establishment of ERTRs and regulations applicable thereto

Definition of ERTRs

The FIEA Revisions introduced the concept of ERTRs to clarify the scope of tokens governed by the FIEA.

ERTRs refer to the rights set forth in Article 2, Paragraph 2 of the FIEA that are represented by proprietary value, transferable by means of an electronic data processing system (but limited only to proprietary values recorded in electronic devices or otherwise by electronic means), but excluding those rights that have been specifically excluded by the relevant Cabinet Office Ordinance in light of their negotiability and other factors. Article 2, Paragraph 2 of the FIEA refers to rights of various kinds, and includes tokens issued in security token offerings (STOs). These tokens are, in principle, expected to also constitute collective investment scheme interests (CISIs) under the FIEA. CISIs are deemed to be formed in arrangements where the following three requirements are met: (1) investors (i.e., right holders) invest or contribute cash or other assets to a business; (2) the cash or other assets contributed by investors are invested in the business; and (3) investors have the right to receive dividends of profits or assets generated from investments in the business. Tokens issued under STOs would constitute ERTRs if the three requirements above are satisfied.

Disclosure requirements

As a result of the application of disclosure requirements to ERTRs, issuers of ERTRs are in principle required, upon making a public offering or secondary distribution, to file a securities registration statement and issue a prospectus. Any person who causes other persons to acquire ERTRs or who sells ERTRs to other persons through a public offering or secondary distribution must deliver a prospectus to the other persons in advance or at the time of the acquisition or sale.

Licensing (registration) requirements

As ERTRs are expected to constitute Paragraph 1 securities, a person acting as a broker, an agency or an intermediary of selling or purchasing ERTRS or handling a public offering of ERTRs in the course of a business is required to undergo registration as a Type I financial instruments business operator.

In connection with the above, the FIEA Revisions do not amend the language in Article 2, Paragraph 8, Item 7 of the FIEA, which provides the definitions of 'public offering' and 'private placement'. Accordingly, any ERTR issuer that solicits the acquisition of the ERTR (i.e., undertaking an STO) will be required to undergo registration as a Type II financial instruments business operator, unless it qualifies as a specially permitted business for qualified institutional investors.

ii Introduction of regulations governing cryptoasset derivative transactions

Regulations governing cryptoasset derivative transactions were introduced by the FIEA Revisions to protect users and to ensure that such transactions are appropriately conducted. Specifically, for the purposes of subjecting derivative transactions involving financial instruments or financial indicators to certain entry regulations and rules of conduct issued under the FIEA, cryptoassets have been inserted in the definition of 'financial instruments' under the FIEA Revisions. Furthermore, the prices, interest rates and other aspects of cryptoassets have been incorporated into the definition of 'financial indicators'.

As cryptoassets will be included in the definition of financial instruments, the conduct of over-the-counter derivative transactions related to cryptoassets or intermediary or brokerage activities in relation thereto will also constitute Type I financial instruments business.

iii Introduction of prohibitions against unfair acts in cryptoasset or cryptoasset derivative transactions

In respect of cryptoasset spot transactions and cryptoasset derivative transactions, the FIEA Revisions contain prohibitions against the following: wrongful acts; dissemination of rumours, fraudulence, assault or intimidation; and market manipulation. These prohibitions (which are without limits as to the violating party) are intended to enhance protection of users and to prevent obtainment of unjust benefits. Breach is punishable by penalties.

Insider trading, however, is not regulated under the FIEA Revisions, owing to difficulties both with the formulation of a clear concept of cryptoasset issuers and with the identification of undisclosed material facts.

III BANKING AND MONEY TRANSMISSION

i Approach of the central bank

Cryptoassets are neither deemed money nor equated with fiat currency. No cryptoasset is backed by the government or the Bank of Japan (the central bank).

ii Money transmission

Only licensed banks or registered fund transfer business operators are permitted to engage in money remittance transactions as a business. The Supreme Court, in a case precedent, has defined money remittance transactions to mean 'the planned or actual transfer of funds, as requested by customers, through utilisation of a fund transfer system without physical transportation of cash between physically distant parties'. As funds do not include cryptoassets, however, a cryptoasset remittance transaction is unlikely to be deemed a money remittance transaction.

IV ANTI-MONEY LAUNDERING

To prevent cryptoasset-related money laundering and terrorism financing, the Act on Prevention of Transfer of Criminal Proceeds (APTCP) requires exchange providers to implement know your customer (KYC) and other preventative measures. The APTCP applies to registered exchange providers, and generally requires them to:

a verify and record the identity of customers when conducting certain transactions (that is, to implement the KYC process);

b record transactions with customers;
c report suspicious transactions to the FSA; and
d take measures to keep information regarding customer verification up to date, provide education and training for employees, and develop other systems necessary for the proper conduct of the processes described in points (a) to (c).

Under the APTCP, exchange providers must conduct the KYC process when undertaking any of the following:

a executing a master agreement with a customer for providing that customer with regular cryptoasset exchange, management and similar services in respect of his or her money or cryptoassets;
b transferring cryptoassets into funds or exchanging them for other kinds of assets (or transactions similar thereto), where the receipt and payment of cryptoassets exceeding ¥2 million in value is involved; or
c where the exchange provider manages a customer's cryptoassets, transferring the cryptoassets at the customer's request if their value exceeds ¥100,000.

V REGULATION OF EXCHANGES

i Regulation of exchange services

The PSA and APTCP were primarily intended to regulate exchange services, with a particular focus on protecting customers and preventing cryptoasset-related money laundering and terrorism financing. Pursuant to the PSA, those wishing to provide exchange services have to be registered with the Prime Minister as exchange providers.[3] To qualify, applicants must be either a stock company or a foreign exchange provider with an office and representative in Japan. Accordingly, a foreign applicant is required to establish either a subsidiary (in the form of a stock company) or a branch in Japan as a prerequisite to registration. In addition, applicants are required to have:

a at least ¥10 million in capital as well as net assets with a positive value;
b a satisfactory organisational structure and appropriate operational systems to enable the proper provision of exchange services; and
c appropriate systems to ensure compliance with applicable laws and regulations.

The PSA also provides legislative definitions of 'exchange services' and 'cryptoasset'. Article 2, Paragraph 7 of the PSA defines exchange services as engagement in any of the following activities as a business:

a the sale or purchase of cryptoassets, or the exchange of a cryptoasset for another cryptoasset;
b intermediating, brokering or acting as an agent in respect of the activities listed in point (a); or
c the management of customers' money or cryptoassets in connection with the activities listed in points (a) and (b).

3 The registration will be carried out through the FSA and the relevant local finance bureau, which acts as the Prime Minister's delegate.

It was highlighted in the Report that cryptoasset custody services share common risks with exchange services, including risks relating to leakage of users' cryptoassets, bankruptcy of service providers, and money laundering and terrorism financing. To address this, the PSA Revisions stipulate that the management of cryptoassets for the benefit of another person constitutes an exchange service, 'unless otherwise specifically stipulated under any other law in cases where the relevant management activity is performed in the course of a business'. As a result, a cryptoasset custody service also constitutes an exchange service, even if it does not involve any of the acts listed in points (a) and (b) above.

A cryptoasset is defined in Article 2, Paragraph 5 of the PSA as:

a a proprietary value that may be used to pay an unspecified person the price of any goods purchased or borrowed or any services provided, where the proprietary value may be:
- sold to or purchased from an unspecified person, provided the sale and purchase is recorded on electronic or other devices through electronic means; and
- transferred through an electronic data processing system; or

b a proprietary value that may be exchanged reciprocally for the proprietary value specified in point (a) with an unspecified person, where the proprietary value may be transferred through an electronic data processing system.

Pursuant to Article 2, Paragraph 5 of the PSA Revisions, the term 'virtual currency' has been revised to 'cryptoasset'. However, the existing definition of 'virtual currency' will remain unchanged. Accordingly, it is generally understood that the change in reference from 'virtual currency' to 'cryptoasset' will result in no substantive change to the legal interpretation of the term.

ii Principal regulations applicable to the operation of exchange providers

Exchange providers are required to:

a take the measures necessary to ensure the safe management of information available to them;

b provide sufficient information to customers;

c take the measures necessary for the protection of customers and the proper provision of services;

d segregate the property of customers from their own property and subject such segregation to regular audits by a certified public accountant or audit firm; and

e establish internal management systems to enable the provision of fair and appropriate responses to customer complaints, and implement measures for the resolution of disputes through financial alternative dispute resolution proceedings.

iii Additional regulations under the PSA Revisions

Under the PSA Revisions, the following changes are proposed to be made to the current regulatory system governing exchange providers, both to enhance user protection and to clarify the rules relating to exchange providers:

a expansion of grounds on which applications for registration as an exchange provider may be rejected;

b introduction of a system of advance notification for any proposed amendment to certain aspects of the relevant cryptoasset, such as its name;

c introduction of regulations governing advertisements and solicitation in respect of exchange services;

d introduction of disclosure requirements where cryptoassets are exchanged (or where certain similar transactions are undertaken) via the grant of credit to users;
e enhancement of the obligation on exchange providers to preserve users' assets; and
f grant of rights to users to enable their receipt of preferential payment when claiming for the return of cryptoassets.

With respect to point (e), above, an exchange provider is required under the PSA Revisions to both manage the money of users separately from its own money, and to entrust users' money to a trust company or any other similar entity in accordance with the provisions of the relevant Cabinet Office Ordinance. In other words, an Exchange Provider is required not only to manage the money of users in bank accounts separately from its own, but also to entrust such money to a trust company or trust bank, acting as trustee.

In addition, the PSA Revisions require an exchange provider to manage a user's cryptoassets separately from other user cryptoassets in the manner specified in the relevant Cabinet Office Ordinance, to enhance user protection. Although the relevant Cabinet Office Ordinance has not yet been issued, we understand from the explanatory material prepared by the FSA (the FSA Explanatory Paper)[4] that an exchange provider will be required 'to manage the cryptoasset of users (other than cryptoassets required for the smooth performance of Exchange Services) through highly reliable methods, such as cold wallets'.

Further, pursuant to the PSA Revisions, an exchange provider is required to:

a hold for its own account cryptoassets of the same kind and quantity as those user cryptoassets that are subject to 'requirements specified by the relevant Cabinet office Ordinance as being necessary for ensuring users' convenience and smooth performance of cryptoasset exchange services' (performance assurance cryptoassets); and
b manage performance assurance cryptoassets separately from its own cryptoassets.

In other words, when an exchange provider manages its user cryptoassets in hot wallets, it would likely be required to (1) hold its own cryptoassets of the same kind and quantity as the user cryptoassets managed in hot wallets and (2) manage performance assurance cryptoassets in cold wallets separately from its own cryptoassets.

VI REGULATION OF MINERS

As the mining of cryptoassets does not fall within the definition of exchange service, mining activities are not regulated under existing Japanese regulations. However, interests in mining schemes formulated as CISIs or in cloud mining schemes may be deemed securities under the FIEA and could therefore be subject to its provisions.

VII REGULATION OF ISSUERS AND SPONSORS

i Regulation of initial coin offering tokens and token issuers

Tokens issued by way of an inital coin offering (ICO) take many forms, and the Japanese regulations applicable to a token vary depending on the ICO scheme involved.

4 The FSA Explanatory Paper can be found at: https://www.fsa.go.jp/common/diet/198/02/setsumei.pdf.

Cryptoasset-type tokens

A token that falls within the definition of a cryptoasset will be subject to cryptoasset-related regulations under the PSA. A token that is subject to the PSA must be sold by or through an exchange provider.

On 25 June 2019, the Japan Virtual Currency Exchange Association (JVCEA), a self-regulatory organisation established under the PSA, published a draft of self-regulatory rules and guidelines for ICOs of virtual currency-type tokens entitled 'Rules for Selling New Virtual Currency' (the ICO Rules). Based on the ICO Rules, ICOs may be categorised into two types: (1) where an exchange provider issues new tokens and sells these tokens by itself; and (2) where a token issuer delegates the sale of newly issued tokens to exchange providers. Generally, in addition to ensuring the security of newly issued tokens, including the blockchain, smart contract, wallet tool and other aspects thereof, the ICO Rules require that the following be satisfied for all ICOs:

a maintenance of a business structure that facilitates review of the business for which funds are raised via an ICO;

b disclosure of information on the token issuer, the token issued, the proposed use of proceeds raised and other matters;

c segregation of the management of ICO proceeds (both fiat and cryptoassets) from the management of the issuer's own funds;

d proper account treatment and financial disclosure of ICO proceeds; and

e proper valuation of newly issued tokens.

Securities-type tokens

As noted in Section II.i, where distributions are paid to token holders on the profits of a token issuer's business and calculated based on the ratio of a token holder's token ownership, the token involved may constitute an ERTR and consequently subject the token issuer to the provisions of the FIEA.

As ERTRs are expected to constitute Paragraph 1 securities, a broker, an agency or an intermediary selling or purchasing ERTRS or handling a public offering of ERTRs in the course of business will be required to undergo registration as a Type I financial instruments business operator.

In addition, any ERTR issuer that solicits the acquisition of ERTRs (i.e., undertaking an STO), will be required to undergo registration as a Type II financial instruments business operator, unless it qualifies as a specially permitted business for qualified institutional investors.

Prepaid card-type tokens

Tokens that are similar to prepaid cards, in the sense of being usable as consideration for goods or services provided by token issuers, may be regarded as prepaid payment instruments, and accordingly could be subject to applicable regulations under the PSA. (A token subject to the prepaid payment instrument regulations under the PSA would not simultaneously be subject to the PSA regulations applicable to cryptoasset (and vice versa).)

ii Regulation of sponsors

As one of the primary purposes of cryptoasset regulation in Japan is the protection of cryptoasset exchange customers, sponsors of ICO issuers are not regulated by the PSA or other laws in respect of cryptoassets.

VIII CRIMINAL AND CIVIL PENALTIES

i Penal provisions applicable to exchange providers

The existing penal provisions found in the PSA are applicable to exchange providers. The following is a summary of some of the major violations under the PSA, and the penalties applicable to these violations.

a Imprisonment with penal labour for a term not exceeding three years or a fine not exceeding ¥3 million, or both, is imposed for:
- providing exchange services without registration;
- registration through fraudulent means; or
- name lending.

b Imprisonment with penal labour for a term not exceeding two years or a fine not exceeding ¥3 million, or both, is imposed for:
- a violation of the obligation to segregate customers' funds and cryptoasset from an exchange provider's funds and cryptoasset; or
- a violation of any order for the suspension of exchange services.

c Imprisonment with penal labour for a term not exceeding one year or a fine not exceeding ¥3 million, or both, is imposed for:
- failure to give public notice of a business assignment, merger, demerger, company split or discontinuance of business, or dissolution in respect of an exchange provider, or giving false public notice thereof;
- a violation of the obligation to prepare and maintain books and documents, or the preparation of false books or documents;
- failure to submit the required report (and any required attachment thereto) for each business year to the Prime Minister, or submission of a report containing false statements;
- failure to comply with an order of the Prime Minister to submit reports or materials, or the submission of false reports or materials; or
- refusal to respond to questions or provision of false responses at an on-site inspection, or refusing to provide cooperation in respect of the inspection.

d Imprisonment with penal labour for a term not exceeding six months or a fine not exceeding ¥500,000, or both, is imposed for any false statement in a registration application or attachments thereto.

e A fine not exceeding ¥1 million is imposed for violating an order for the improvement of business operations.

f Imprisonment for a term not exceeding six months or a fine not exceeding ¥500,000, or both, is imposed for any failure to make the required disclosure regarding advertisement or solicitation in respect of exchange services.

g Imprisonment for a term not exceeding one year or a fine not exceeding ¥3 million, or both, is imposed any misrepresentation or any representation under a cryptoasset exchange agreement[5] that will likely lead to an inaccurate understanding of the nature or any other aspects of a cryptoasset.

h Imprisonment for a term not exceeding six months or a fine not exceeding ¥500,000, or both, is imposed for:

- any misrepresentation or representation in an advertisement concerning an exchange service that will likely lead to an inaccurate understanding of the nature or any other aspects of a cryptoasset; or
- any representation under a cryptoasset exchange agreement or in an advertisement concerning an exchange service, to induce the sale or purchase of a cryptoasset or the exchange of a cryptoasset for another cryptoasset that is (1) not for the purpose of using the relevant cryptoasset as a means of payment, but (2) for the exclusive purpose of promoting the interests in a particular cryptoasset.

ii Civil fraud

The PSA contains no specific regulation for the prevention of unfair trading or sale of tokens. However, the Civil Code or Penal Code of Japan, and certain consumer protection laws and regulations,[6] are applicable to such activities, except where the relevant token is deemed a security under the FIEA, in which case the FIEA provisions regulating unfair trading of securities will apply.

In addition, as a result of the PSA and FIEA Revisions, the ASFI was also proposed to be amended to render it applicable to acts that result in the acquisition of cryptoassets. Without these amendments to the ASFI, customers wishing to claim against exchange providers will be required to establish a claim in tort. To address this unsatisfactory situation, the ASFI Revisions expressly impose accountability on exchange providers, including presuming the amount of damages that such service providers would owe, to reduce the burden of proof on the part of service users.

IX TAX

The treatment of consumption tax in respect of cryptoassets has been a hot topic in Japan. In the past, sales of cryptoassets were subject to Japanese consumption tax to the extent that the office of the transferor was located in Japan. However, this position changed in 2017 following amendments to applicable tax laws. Under the amended tax laws, consumption tax is no longer imposable on a sale of cryptoassets after 1 July 2017 if the relevant cryptoasset is deemed a cryptoasset under the PSA, such as Bitcoin. Additionally, it was announced by the National Tax Agency of Japan that gains from the sale or use of cryptoassets will be treated as miscellaneous income, such that gains from the sale or usage of cryptoasset cannot be offset against losses incurred elsewhere.

5 A 'cryptoasset exchange agreement' means an agreement between a cryptoasset exchange service provider and a user of cryptoasset exchange services under which cryptoasset exchange services are provided to, or interest in such services are solicited from, the user.

6 Such as the Act on Specified Commercial Transactions, the Consumer Contract Act and the Act against Unjustifiable Premiums and Misleading Representations.

X OTHER ISSUES

Under the Foreign Exchange and Foreign Trade Act of Japan, a person who makes any payment from or receives any payment in Japan in excess of ¥30 million is required to notify the Minister of Finance of the payment or receipt. This notification requirement was extended to cover cryptoassets. Specifically, it was announced by the government on 18 May 2018 that the Minister of Finance must be notified of payments or receipts of cryptoassets with a market value exceeding ¥30 million as of the payment date.

XI LOOKING AHEAD

The Bill, containing the PSA Revisions, FIEA Revisions, and ASFI Revisions, will introduce a new legal framework for the governance of cryptoassets. Although the framework will likely impose heavier regulatory burdens on exchange providers, it will also bring certain advantages, such as a more orderly structured cryptoasset industry and enhanced user protection. These benefits, together with the FIEA Revisions that will allow cryptoasset derivative transactions and STOs, are expected to facilitate greater growth in the Japanese cryptoasset market.

Chapter 16

KOREA

Jung Min Lee, Joon Young Kim and Samuel Yim[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

There is considerable public interest in cryptocurrencies and blockchain in Korea.[2] For example, on 16 January 2018, a petition to the President entitled Opposing Cryptocurrency Regulation garnered more than 200,000 signatures.[3] On 14 February 2018, the government responded to the petition by stating that it considers the transactional transparency of cryptocurrencies to be of paramount importance, but that it will also promote blockchain technology.

As such, the government conceptually differentiates policies related to cryptocurrency from those of blockchain technology. Although some regulations have been introduced to curb speculative investment in cryptocurrency, the government has highlighted the innovative nature of blockchain technology in many different industries. It has also expressed its interest in fostering, promoting and investing in blockchain technology as part of its strategic and economic plans for Korea to be a leader in the Fourth Industrial Revolution.

However, there is no coherent insight on how cryptocurrencies would be classified under Korean law. The Financial Supervisory Service issued a press release on 23 June 2017 to announce its views on what cryptocurrencies are not from a financial regulatory perspective:[4] namely, cryptocurrencies are not considered fiat currencies, prepaid electronic means or electronic currencies, or financial investment instruments. Unfortunately, the press release did not provide any guidance on how cryptocurrencies are classified and in what legal form. In addition, cryptocurrencies are not insured by the Korean Deposit Insurance Corporation.[5]

The government is largely concerned with the protection of investors and consumers of cryptocurrency. It has shown particular concern regarding cryptocurrency-related illegal activities, such as multilevel schemes and money laundering; however, it has repeatedly stated that the regulation of cryptocurrency transactions does not signify endorsement or institutionalisation of cryptocurrencies.[6]

---

1 Jung Min Lee and Joon Young Kim are senior attorneys and Samuel Yim is a senior foreign attorney at Kim & Chang.

2 In this chapter, Korea refers to South Korea.

3 http://www.hani.co.kr/arti/economy/finance/832276.html.

4 Financial Supervisory Service, press release, 23 June 2017, http://m.fss.or.kr:8000/fss/board/bodoBoardDetail.do?seqNo=20581&gubun=01&mId=M01050200000000.

5 id.

6 See, e.g., FSC, press release, 28 May 2018, https://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=1&sch1=subject&sword=%EA%B0%80%EC%83%81%ED%86%B5%ED%99%94&r_url=&menu=7210100&no=32491.

The Supreme Court of Korea ruled on 30 May 2018 that cryptocurrencies can be confiscated as criminal proceeds.[7] This decision represents the first time the Supreme Court has recognised cryptocurrency as property. However, given the narrow scope of its interpretation, it is unclear what impact this ruling will have on subsequent cryptocurrency regulation.

Classification of cryptocurrencies from a legal perspective has just begun in Korea and will likely develop in the near future. Other Korean regulatory authorities may have a different view from the Financial Supervisory Service's announcement and the legal classification of cryptocurrencies. As a result, there is currently no law or clear guidance from any regulatory authority in Korea that provides clarity on the legal issues relating to cryptocurrencies and how they will be treated under Korean law.

II SECURITIES AND INVESTMENT LAWS

The main legal framework governing securities and investment in Korea is the Financial Investment Services and Capital Markets Act (FSCMA). There is no existing regulatory regime or statute that incorporates cryptocurrency into Korean securities and investment laws.

The FSCMA defines securities as:

> *financial investment products for which investors do not owe any obligation to pay anything in addition to the money or any other valuables paid at the time of acquiring such instruments (excluding obligations to pay where an investor assumes such an obligation by exercising a right to effectuate the purchase and sale of an underlying asset), provided that there are certain securities, such as investment contract securities, which are only recognised as securities under the FSCMA when meeting certain conditions under the FSCMA.*[8]

On the other hand, the FCSMA defines financial investment products as:

> *a right acquired by an agreement to pay, at the present time or a specific time in the future, money or any other valuables, for the purpose of earning a profit or avoiding a loss, where there is a risk that the total amount of such money or any other valuables, paid or payable, to acquire such right (excluding any sums specified in the Enforcement Decree, such as sales commissions) may exceed the total amount of money or any other valuables recovered or recoverable from the right (including any sums specified in Enforcement Decree, such as termination fees).*[9]

It is currently unclear whether cryptocurrencies qualify as securities or financial investment products under the FSCMA. In a series of press releases, Korean financial authorities have taken the position that cryptocurrencies or cryptocurrency assets are not a financial investment

7 http://news.joins.com/article/22668491.

8 FSCMA Article 4.

9 id., Article 3.

product under the FSCMA.[10] However, these announcements were made in the context of cautioning potential investors, and thus do not adequately address whether cryptocurrencies qualify as financial investment products under the FSCMA.

There is no explicit prohibition on the registration of cryptocurrency-related investment funds. A licence must be acquired to provide advice on financial investment products in Korea. Since an investment fund's underlying asset need not be financial investment products under the FSCMA, an investment fund may, in theory, include cryptocurrencies or cryptocurrency assets as its underlying assets. However, it is unclear whether the Korean financial regulators will be receptive to such investment funds. To date, there are no cryptocurrency-based investment vehicles or funds registered with the Korean financial regulatory agencies.

On 1 September 2017, the Financial Services Commission (FSC) announced a ban on margin trading, prohibiting individuals from borrowing funds or cryptocurrencies from cryptocurrency exchanges to sell them.[11] The FSC has declared that this practice violates existing Korean lending and credit laws. It has further directed financial institutions to halt all transactions and partnerships that enable margin trading.

III BANKING AND MONEY TRANSMISSION

On 4 September 2017, the FSC announced that it would initiate an identification policy for accounts in cryptocurrency exchanges that requires cross-checking user names and account numbers. On 30 January 2018, the FSC introduced the Real Name Verification System.[12] Under the Real Name Verification System, users who want to make a cryptocurrency transaction must have a bank account under their real name at the same bank with the cryptocurrency exchange. Existing anonymous account users can only withdraw money and may not make any further deposits. The Real Name Verification System further bans minors (under the age of 18) and foreigners from opening new cryptocurrency accounts.

There are no explicit border restrictions or obligations to declare cryptocurrency holdings. However, for fiat currencies, the Foreign Exchange Transaction Act (FETA) and the Foreign Exchange Transactions Regulations (FETR) regulate the remittance of funds out of Korea to overseas accounts. Generally, there must be a legal basis, along with supporting documents as prescribed under the FETA, to repatriate funds overseas. Examples of a legal basis include loan repayments, dividend payments and sale proceeds payments. The FETA prescribes certain procedures and documents for each type of transaction listed in the FETA for both the remitter of funds and the bank handling the remittance. Each type of transaction has different procedures and requirements to remit funds overseas. Generally, under the FETA, all outbound remittance in an amount exceeding US$3,000 per transaction or a yearly aggregate limit of US$50,000 must be reported to and approved by the Bank of Korea (BOK).

10 FSC, press release, 13 December 2017, https://www.fsc.go.kr/info/ntc_news_view.jsp?menu=7210100&bbsid=BBS0030&no=32202; Financial Supervisory Service, press release, 23 June 2017, http://m.fss.or.kr:8000/fss/board/bodoBoardDetail.do?seqNo=20581&gubun=01&mId=M01050200000000.

11 FSC, press release, 28 December 2017, https://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=1&sch1=subject&sword=%EA%B0%80%EC%83%81%ED%86%B5%ED%99%94&r_url=&menu=7210100&no=32230.

12 FSC, press release, 28 December, 2018, https://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=1&sch1=subject&sword=%EA%B0%80%EC%83%81%ED%86%B5%ED%99%94&r_url=&menu=7210100&no=32230.

There are no guidelines regarding cryptocurrencies under the FETA or the FETR. In practice, however, Korean banks decline to process wire transfers overseas when related to cryptocurrency trading, even if the amount is below the monetary limits and would not trigger the reporting requirements to the BOK or designated foreign exchange bank under the FETA.

Moreover, for overseas payments using cryptocurrencies, there are no reporting requirements at this time to any Korean regulatory agency. However, there are requirements being developed by the Korean financial regulators that may require a filing requirement with the BOK for foreign exchange purposes.

On 9 January, 2018, the BOK launched a task force on cryptocurrency and is reviewing a central bank-backed cryptocurrency as part of the project. In addition, various local governments in Korea are exploring the option of issuing their own cryptocurrency.

IV ANTI-MONEY LAUNDERING

The main legal framework governing anti-money laundering is the Act on Reporting and Use of Certain Financial Transaction Information (the AML Act). In addition, the Real Name Verification System seeks to prevent money laundering. The Korea Financial Intelligence Unit is primarily responsible for enforcing anti-money laundering obligations. Currently, cryptocurrency exchanges are not directly subject to anti-money laundering requirements under the AML Act; instead, the financial regulators enforce anti-money laundering requirements through financial institutions that are linked to cryptocurrency exchanges. There are proposed bills seeking to subject cryptocurrency exchanges to the requirements of the AML Act (see subsection iii).

Financial institutions doing business with companies that handle cryptocurrencies are subject to the Financial Intelligence Unit's Anti-Money Laundering Guidelines for Cryptocurrencies (the AML Guidelines),[13] which cover:

a the identification of cryptocurrency exchanges;
b internal controls;
c the denial of transactions; and
d sanctions for violations of the provisions of the AML Guidelines.

The AML Guidelines further provide that the financial regulators may issue correction orders or business suspension orders pursuant to the AML Act if a financial institution violates a provision of the AML Guidelines.

The AML Guidelines initially took effect on 30 January 2018, with an applicable period of 12 months with the possibility of renewal. This guideline is enforceable for financial institutions that transact with cryptocurrency companies. The notable provisions of the amended AML Guidelines are as follows.

13 FSC, press release, 27 June 2018, https://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=1&sch1=subject&sword=%EA%B0%80%EC%83%81%ED%86%B5%ED%99%94&r_url=&menu=7210100&no=32548.

i Requirement of real-name verification for fiat withdrawal from and deposit to cryptocurrency exchanges

Fiat withdrawals from and deposits to a cryptocurrency exchange are available only if the exchange user's bank account is verified under the Real Name Verification System provided by financial institutions (e.g., banks), as explained above. Financial institutions may decline transactions with cryptocurrency exchanges that do not comply with this requirement. The system also bans minors (those under the age of 18) and foreigners from opening new cryptocurrency accounts.

ii Due diligence process for customer identification

The AML Guidelines mandate that financial institutions adopt a process whereby they can identify if their clients are cryptocurrency exchanges or other cryptocurrency-related businesses. If a financial institution identifies a client as a cryptocurrency-related business, it must verify certain additional information enumerated in the AML Guidelines. Examples of this additional information include whether the cryptocurrency exchange checks the identity of its users, maintains a separate transaction record for each user and is in compliance with the cryptocurrency-related policies issued by the government. In addition, financial institutions must perform additional checks every six months and share information with other financial institutions. Furthermore, financial institutions must refuse new transactions or promptly stop processing existing transactions if they cannot confirm the identity of a client.

iii Suspicious transaction reports

If transactions seem suspicious, financial institutions must review and file a suspicious transaction report. Financial institutions must also appoint a staff member dedicated to monitoring suspicious cryptocurrency transactions. Suspicious transaction types include:

a financial transactions between cryptocurrency exchanges and corporate entities or organisations;

b financial transactions between a cryptocurrency exchange and a single user where the amount of the transactions is 10 million won or more within one day, or 20 million won or more within seven days; and

c if the number of financial transactions between a cryptocurrency exchange and a single user reaches five times or more within one day, or seven times or more within seven days.

In April 2018, the FSC monitored compliance with the AML Guidelines. Based on the results, it amended the AML Guidelines in June 2018, which took effect in July 2018. The amended Guidelines will remain effective for two years and their key requirements are as follows:

a financial institutions shall enhance monitoring for accounts of cryptocurrency companies that are used for operating expenses, and conduct enhanced customer due diligence in case it identifies a suspicious transaction;

b financial institutions shall share the list of foreign cryptocurrency companies; and

c if a financial institution refuses to transact with a certain cryptocurrency company, the financial institution shall specify the timing and grounds for its refusal.

Currently, there are several cryptocurrency bills proposed at the National Assembly. These bills generally cover, among other things, licensing requirements for cryptocurrency businesses,

anti-money laundering requirements, consumer protection, cybersecurity requirements for cryptocurrency exchanges and damage compensation for consumer losses. It is unclear when or if these pending bills, in their current form, will be enacted into law.[14]

V REGULATION OF EXCHANGES

Cryptocurrency exchanges do not require financial licences, nor are they subject to the AML Act. However, the various proposed bills pending at the National Assembly seek to require cryptocurrency exchanges to obtain financial licences and to impose anti-money laundering requirements directly on the exchanges.

Regulation of cryptocurrency exchanges in Korea primarily takes the form of self-regulation. The Korea Blockchain Association (KBA) is a trade association of cryptocurrency exchanges that self-regulates cryptocurrency exchanges.[15] As the KBA's regulation only binds its members, non-member exchanges would not be subject to the KBA's regulation. As part of its self-regulation, KBA requires that member exchanges abide by the Commercial Act and maintain equity of at least 2 billion won. The KBA also mandates that the exchanges deposit all their monetary deposits with financial institutions and use cold storage for at least 70 per cent of their cryptocurrency deposits to protect investors' funds. The KBA's regulation also mainly covers:

a increasing the transparency of initial coin offerings (ICOs);
b strengthening the verification of account holders' identification;
c operating offline customer centres;
d strengthening the ethics of executives and employees; and
e forming independent committees on self-regulation.

On 16 April 2018, the KBA announced plans to review its member cryptocurrency exchanges according to the self-regulation provisions.[16] Upon review of 12 member exchanges, it announced on 11 July 2018 that all exchanges have met the minimum requirements of the self-regulation provisions.[17]

In addition, the government indirectly regulates cryptocurrency exchanges through existing laws. As cryptocurrency exchanges are registered as corporations, they are subject to various cybersecurity and privacy laws that are also applicable to other corporations. The Ministry of Science and ICT (MSIT) has been reviewing the cybersecurity measures adopted by cryptocurrency exchanges since September 2017.[18] The MSIT requires exchanges with total sales over 10 billion won and over 1 million daily visitors to acquire an information security

14 Korea Blockchain Association, press release, 15 December 2017, http://www.kblockchain.org/site/program/board/basicboard/view?menuid=001004002&pagesize=10&boardtypeid=4&boardid=116.

15 Korea Blockchain Association, press release, 15 December 2017, http://www.kblockchain.org/site/program/board/basicboard/view?menuid=001004002&pagesize=10&boardtypeid=4&boardid=116.

16 Korea Blockchain Association, press release, 16 April 2018, http://www.kblockchain.org/site/program/board/basicboard/view?menuid=001004002&pagesize=10&boardtypeid=4&boardid=176.

17 Yonhap News, 11 July 2018, http://www.yonhapnews.co.kr/bulletin/2018/07/11/0200000000AKR20180711083051002.HTML?input=1195m.

18 Ministry of Science and ICT, press release, 21 December 2017, http://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=1370974.

management system pursuant to the Act on Promotion of Information and Communications Network Utilisation and Information Protection. As of December 2018, the four largest exchanges are subject to this requirement.

In addition, cryptocurrency exchanges may be required to register a chief information security officer (CISO) with the MSIT. The MSIT will cooperate with CISOs to minimise further damage in the event of hacking attacks or other cybersecurity threats. The Korea Internet and Security Agency also plans to monitor and promptly address the dissemination of malicious codes within, and distributed denial-of-service attacks against, cryptocurrency exchanges.

VI REGULATION OF MINERS

There is no law or regulation explicitly regulating mining of Bitcoins or other cryptocurrencies. However, based on statements from Korean financial regulatory authorities, it appears that mining itself may not be illegal per se. In a 22 June 2017 press release, the Financial Supervisory Service noted that retail mining would be unsuccessful owing to limited computing power, which may imply that retail mining would not be illegal.[19] Similarly, an Office for Government Policy Coordination press release issued on 22 December 2017 implies that mining itself would not be illegal.[20] In that press release, the government noted that mining in industrial complexes while taking advantage of discounted electricity fees is illegal and that the Ministry of Trade, Industry and Energy has already requested a local government to monitor sudden spikes in electricity use. These statements seem to imply that what is illegal is the misuse of discounted electricity, not mining itself.

Subsequently, on 31 January 2019, the government announced the result of its monitoring of the ICO practice in Korea and its proposed approach to regulate ICOs. In this announcement, it stated that it had identified companies bypassing its prohibition on ICOs by performing ICOs through offshore companies in foreign jurisdictions (such as Singapore) while raising funds from domestic investors. The government found that this practice substantively constitutes domestic ICOs, albeit in the form of a foreign ICO, and further stated that domestic investors were at significant risk as a result of this because the companies performing the ICOs did not disclose substantial information for the investors to make an informed decision.

In addition, the government also deemed that certain ICO projects may violate the FSCMA if they involve the issuance and transaction of peer-to-peer collateralised loan tokens, the sale of cryptocurrencies investment funds or the operation of unauthorised financial investment business by providing investment services with IPO tokens.

As ICOs pose a high investment risk and lack a global regulatory framework, the government announced that it will take a conservative approach in legalising them. Further,

19 Financial Supervisory Service, press release, 22 June 2017, http://www.fss.or.kr/fss/kr/promo/bodobbs_view.jsp?seqno=20581&no=1&s_title=%B0%A1%BB%F3%C5%EB%C8%AD&s_kind=title&page=2.

20 Office for Government Policy Coordination, press release, 22 December 2017, http://www.korea.kr/briefing/pressReleaseView.do?newsId=156244619&pageIndex=1&repCodeType=&repCode=&startDate=2008-02-29&2018-07-20&srchWord=%EA%B0%80%EC%83%81%ED%86%B5%ED%99%94.

it maintained an equivocal position on whether it will publish an ICO guideline, as doing so may give the market the impression that it has officially approved domestic ICOs, which is not the case.[21]

VII REGULATION OF ISSUERS AND SPONSORS

A government task force on cryptocurrency, composed of, among others, financial regulators, foreign exchange regulators and tax regulators, issued a press release on 4 September 2017 entitled Status and Direction for Cryptocurrency.[22] The press release states that the Korean regulators will penalise acts of ICOs as violations of the FSCMA where cryptocurrencies are issued in the form of securities, such as investment contract securities, and the issuer has not complied with the offering restrictions under the FSCMA. Although the Korean regulators' initial position was to penalise ICOs in the form of securities issuances (i.e., in cases where the token is classified as a security), the regulators subsequently took a stricter position in another press release on 29 September 2017, announcing their new policy that any types of ICOs (including those in the form of securities) would be prohibited.[23]

If coins or tokens qualify as securities under the FSCMA, ICOs will be subject to offering or sales restrictions in Korea. Under the FSCMA, an offer or sale of securities to 50 or more non-accredited investors (excluding professional investors) would be regarded as a public offering and be subject to offering restrictions under the FSCMA. In a public offering of securities in Korea, an onshore or offshore issuer must file a securities registration statement for the securities to be offered in Korea with the FSC.

In contrast, if coins or tokens are not securities under the FSCMA, then ICOs would not be subject to securities offering restrictions under the FSCMA, and there would be no grounds for the prohibition of ICOs unless they trigger a violation of other existing Korean laws or regulations. However, given the stance of the Korean financial regulatory authorities, it is possible that they would take an expansive view of the existing laws and regulations and cause difficulties for issuers.

Fundraising activities are subject to the Act on the Regulation of Conducting Fund-Raising Business Without Permission (the Fund-Raising Business Act). This Act prohibits guaranteeing a return of the original investment amount or an amount exceeding an original investment amount when raising funds.[24] In addition, making any indication or advertising of one's business so as to carry on prohibited acts constitutes a violation of the Fund-Raising Business Act.[25] Thus, when marketing or promoting an ICO, if an issuer promises a return of the original investment amount or an amount exceeding the original investment amount, it will likely be in violation of Fund-Raising Business Act. The regulatory

21 FSC, press release, 4 September 2017, https://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=2&sch1=subject&sword=%EA%B0%80%EC%83%81&r_url=&menu=7210100&no=32027.

22 FSC, press release, 4 September 2017, https://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=2&sch1=subject&sword=%EA%B0%80%EC%83%81&r_url=&menu=7210100&no=32027.

23 FSC, press release, 29 September 2017, https://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=2&sch1=subject&sword=%EA%B0%80%EC%83%81&r_url=&menu=7210100&no=32085.

24 Act on the Regulation of Conducting Fund-Raising Business Without Permission, Articles 2 to 3.

25 id., Article 4.

authorities have indicated that they will seek to amend the Fund-Raising Business Act so that all cryptocurrency-related fundraising activities are violations of the Act. However, it is currently unclear whether this amendment would pass.

VIII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

Chapter XXXIX (Article 347 et seq.) of the Criminal Act governs fraud, whereas tort law under Article 750 of the Civil Act governs civil fraud. The government has been actively investigating and prosecuting fraud and other criminal acts related to cryptocurrency. For example, on 10 May 2018, the head of a multilevel scheme that advertised that the company turns profit by purchasing Bitcoins in countries with lower prices and selling them in countries with higher prices was convicted of fraud and sentenced to seven years in prison.[26] Similarly, a board member of the company was convicted of the same crime and was sentenced to four years in prison. The company offered 20 per cent of the new investment amount from new participants to the referee participant and provided other incentives to participants who were successful in attracting more investments. The court stated that the company received funds by defrauding customers even though there was no guarantee of recovering the original investment. In addition, there have also been investigations and prosecutions of fraudulent acts of cryptocurrency exchanges.

In a press release dated 28 December 2017, the government stated that it will continue to investigate and prosecute illegal acts related to cryptocurrency, and will seek to impose the maximum penalties allowed by the relevant laws.[27] The government further announced in 2018 that it will focus on the following:

a multilevel fraud schemes and the undertaking of fundraising activities without permission;
b investment fraud related to cryptocurrency mining;
c violations of the FETA;
d concealment of criminal proceeds via money laundering, etc.; and
e illegal acts of cryptocurrency exchanges.

IX TAX

The Ministry of Strategy and Finance has announced that plans for the taxation of cryptocurrencies are being developed, but no decisions have been made. When the government introduced the Real Name Verification System on 30 January 2018, it listed data collection for taxation purposes as a benefit of the system, implying taxation. To date, however, the government continues to state that taxation is still under discussion, and no decisions have been made in this regard.

Meanwhile, the National Tax Service has published its preliminary assessment of taxation on cryptocurrencies following its annual forum in 2017.[28] This assessment is not an official policy, but it is the only published position or research on cryptocurrency taxation

26 Herald Corporation, http://news.heraldcorp.com/view.php?ud=20180510000071.

27 FSC, press release, 28 December 2017, https://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=1&sch1=subject&sword=%EA%B0%80%EC%83%81%ED%86%B5%ED%99%94&r_url=&menu=7210100&no=32230.

28 National Tax Service, press release, 5 December 2017.

by the government. The National Tax Service's assessment noted that cryptocurrencies are hybrid products that have characteristics of, inter alia, fiat, securities and goods. Based on this determination, the National Tax Service has made a preliminary assessment of taxation on cryptocurrencies under the existing tax laws as summarised in the table below.

Type	Rate (%)	Assessment	Notes
Corporate income tax	11–27.5	Taxable under current law	Need accounting standards for categorisation and valuation of cryptocurrency
Income tax	6.6–46.2	Taxable under current law	Need accounting standards for categorisation and valuation of cryptocurrency
Corporate or individual VAT	10	Undecided	If cryptocurrency is viewed as means of payment, then no tax; if cryptocurrency is viewed as goods, then levying VAT is advisable
Capital gains tax	6.6–46.2	Undecided, but for retail investors, levying capital gains tax is advisable	N/A
Inheritance and gift tax	10–50	Taxable under current law	Cryptocurrency is a property with economic value, and thus taxable; need valuation standards for cryptocurrency

In addition, the National Tax Service has noted that to increase transaction transparency and to prevent tax avoidance, strengthening the regulation of cryptocurrencies is required. It gave the examples of the introduction of a registration requirement for cryptocurrency exchanges, the implementation of the Real Name Verification System, and the imposition of anti-money laundering requirements and reporting requirements on cryptocurrency exchanges.

X OTHER ISSUES

If the use of cryptocurrency increases in money laundering or for other criminal purposes, and in light of the Supreme Court's decision holding that the government may seize cryptocurrency as criminal proceeds, the seizure of cryptocurrencies may increase. Typically, seized properties are sold through public auction with the proceeds going to the government. The Korea Asset Management Corporation, which manages Onbid, a public auction system, has indicated that public auctions would be possible for cryptocurrencies, noting cryptocurrencies' similarities to securities.[29] However, given the volatility of the price of cryptocurrencies, it may not be advisable to dispose of seized cryptocurrencies through a regular public auction process. The government has yet to decide how it will dispose of the cryptocurrencies seized in connection with the Supreme Court case.

Another issue that arises as the use of cryptocurrency increases is consumer protection. The Act on the Regulation of Terms and Conditions (the T&C Act) governs terms and conditions in contracts. The Korea Fair Trade Commission (KFTC) has indicated that placing limitations on the withdrawal of funds or having excessive waiver provisions may be a violation of the T&C Act.[30] It has also indicated that, if necessary, it would issue corrective orders and impose penalties for this practice.

29 However, the Korea Asset Management Corporation is not in charge of regulating the finance sector, and thus its view of whether cryptocurrency is or is similar to a security cannot be viewed as the government's position on whether cryptocurrency is a security under the FSCMA.

30 Newspim, http://www.newspim.com/news/view/20180117000099.

On 5 April 2018, the KFTC announced that it had reviewed the terms and conditions of user agreements of 12 cryptocurrency exchanges.[31] The review called for changes of 14 terms and conditions that the KFTC deemed unfair. The following changes were voluntary: the deletion of terms and conditions that allowed for the monetisation of cryptocurrencies of members who did not log in for six months or more; and the deletion or amendment of terms and conditions that allowed the indemnification of damages in cryptocurrency or won points, which is virtual won money in the accounts of users in cryptocurrency exchanges to purchase cryptocurrencies. In addition, the KFTC issued corrective recommendations to the exchanges covering 12 types of terms and conditions, including:

a unfair limitations on the withdrawal of funds;
b arbitrary restrictions on the use of services;
c responsibility over user identifiers and passwords; and
d broad waiver provisions.

Furthermore, the KFTC noted the increase in the online advertisement of cryptocurrencies, and that the industry needs to self-regulate to avoid excessive advertisement.

XI LOOKING AHEAD

The government recognises the innovative nature of blockchain technology and its potential impact on the Korean economy. Although it has been hesitant to endorse or institutionalise cryptocurrencies, and has repeatedly warned investors about the potential dangers of investing in them, it has expressed interest in fostering, promoting and investing in blockchain technology as part of its strategic and economic plans. Furthermore, while the central government appears to be uneasy about cryptocurrencies, some local governments have shown interest in issuing their own cryptocurrencies.

A number of proposed pieces of legislation covering cryptocurrencies are pending at the National Assembly. These bills generally cover licensing requirements, anti-money laundering requirements, consumer protection, cybersecurity requirements and compensation for consumer losses. For example, a bill entitled the Special Act on Cryptocurrency Business seeks to, inter alia:

a impose a requirement that a licence be obtained for cryptocurrency exchanges and cryptocurrency-related businesses;
b impose record-keeping obligations;
c explicitly incorporate cryptocurrency businesses into the AML Act and other laws regulating financial institutions; and
d mandate the adoption of cybersecurity measures, among other things.

If passed, these bills may provide a more coherent framework for the regulation of cryptocurrencies and other related issues.

31 KFTC, press release, 5 April 2018.

Chapter 17

LUXEMBOURG

Jean-Louis Schiltz and Nadia Manzari[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

As a globally recognised financial centre with international outreach, Luxembourg has positioned itself as a world leader in the sphere of digital financial services and as a financial technology hub.[2] It has always considered innovation as an essential driver for the development of financial services and the financial sector in general. With this mindset, it has recently adopted a law that states clearly that securities can be legally held and transferred through distributed ledger technologies,[3] thus adding one more layer to its long tradition of 'innovation through law', of which legal certainty is one of the essential pillars. It was also the first country in Europe to license virtual currency exchange platforms as payment institutions.

On 19 April 2016, the Minister of Finance authorised Bitstamp Europe SA, a platform allowing its clients to exchange Bitcoins, euros and US dollars. If the issuing of virtual currencies as such is not subject to authorisation, the service provided by the intermediary – receiving funds from the buyer of Bitcoin to transfer them afterwards to the seller – is covered by the authorisation as a payment institution. This authorisation echoed the opinion of the Financial Sector Supervisory Commission (CSSF), which in 2014 was the first regulator of the financial sector that was in favour of the regulation of platforms for the exchange of virtual currencies when exercising an activity of the financial sector.[4] In a press release dated 14 February 2014, the CSSF considered that activities such as the issuing of means of payments in the form of virtual or other currencies, the provision of payment services using virtual or other currencies, and the creation of a market (platform) to trade virtual or other currencies, are to be defined as being financial activities, and that any person wishing to establish in Luxembourg to carry out such an activity has to receive a ministerial authorisation. bitFlyer, a Japanese virtual currencies exchange platform, was granted a licence in January 2018.

A consumer warning on virtual currencies issued by the CSSF on 14 March 2018 reiterated this position by asserting that, even though there is currently no legal framework in Luxembourg that specifically applies to virtual currencies, it should be borne in mind that any provision of financial sector services by a natural or legal person requires an authorisation by the Minister of Finance.[5]

---

1 Jean-Louis Schiltz is the senior partner and Nadia Manzari is a partner at Schiltz & Schiltz SA.

2 LFF FinTech: http://luxembourgforfinance.com/en/products-services/fintech.

3 Law of 1 March 2019 amending the law of 1 August 2001 concerning the circulation of securities.

4 CSSF annual report 2016.

5 CSSF Warning regarding Virtual Currencies of 14 March 2018.

In another consumer warning on initial coin offerings (ICOs) and tokens, issued on the same date, the CSSF acknowledges that raising funds from the public in the form of initial coin offerings (ICOs) is not subject to a specific regulation, and does not benefit from any guarantee or other form of regulatory protection. The CSSF considers further that despite the lack of specific regulations applying to ICOs, the activities related thereto or relating to the creation of tokens, and the collection and raising of funds may, depending on their characteristics, be subject to certain legal provisions and thus to a number of supervisory requirements.[6]

The CSSF specifies in the warning that it will:

> *assess such fundraising activities by extending its analysis to the objectives pursued in order to assess whether it could be a scheme to circumvent or avoid financial sector regulations, notably the provisions of the Law of 10 July 2005 on prospectuses for securities and the Law of 5 April 1993 on the financial sector. The CSSF considers that for any fundraising, the initiators of such ICOs are required to establish anti-money laundering and terrorist financing procedures.*

II SECURITIES AND INVESTMENT LAWS

In its warning on ICOs, the CSSF has not provided for a classification of tokens or cryptocurrencies underlying ICOs as financial instruments or otherwise. The CSSF at the same time acknowledges that this type of activity might be subject to supervisory requirements in Luxembourg.

The CSSF warning is in line with the European Securities and Markets Authority (ESMA) position on ICOs.[7] ESMA also considers that firms involved in ICOs must give careful consideration to whether their activities constitute regulated activities. If this is the case, firms have to comply with the relevant legislation, and any failure to comply with the applicable rules would constitute a breach.

Actors who would like to provide services related to tokens, be it dealing with tokens or publicly offering those tokens within a regulated financial framework, should be allowed to do so as long as all applicable legal requirements are fulfilled.

According to an ESMA paper dated November 2017, the features and purpose of coins or tokens vary across ICOs. Some coins or tokens serve to access or purchase a service or product that the issuer develops using the proceeds of the ICO. Others provide voting rights or a share in the future revenues of the issuing venture. Some have no tangible value. Some coins or tokens are traded or may be exchanged, or both, for traditional or virtual currencies at specialised coin exchanges after issuance.[8]

ICO campaigns are conducted online, using the internet and social media. The coins or tokens are typically created and disseminated using distributed ledger or blockchain technology. ICOs are used to raise funds for a variety of projects, including but not limited to businesses leveraging on a distributed ledger. Virtually anyone who has access to the internet can participate in an ICO.[9]

6 CSSF Warning regarding initial coin offerings ('ICOs') and tokens of 14 March 2018.

7 ESMA statements of 13 November 2017 ESMA 50-157-828.

8 ibid.

9 ibid.

Commonly, the following three types of tokens can be identified within an ICO context:[10]

a Payment or cryptocurrency tokens: these are intended to be used, now or in the future, as a means of payment for acquiring goods or services, or as a means of money or value transfer. Cryptocurrencies give rise to no claims on their issuer.[11] Payment tokens are subject to the Law of 10 November 2009 on payment services.[12]

b Utility tokens: these provide access digitally to an application or service by means of a blockchain-based infrastructure.[13]

c Asset tokens: these represent assets such as a debt or equity claim on the issuer. Asset tokens promise, for example, a share in a future company's earnings or future capital flows. In terms of their economic function, therefore, these tokens are analogous to equities, bonds or derivatives. Tokens that enable physical assets to be traded on a blockchain also fall into this category.[14]

Taking as a starting point the CSSF's warning on ICOs, and in particular the statement that asset tokens might be subject to regulatory supervision in line with the position taken by several European countries with regard to ICOs,[15] it is our view that, depending on the nature of the token, an ICO could fall, among others, within the remit of the Law of 5 April 1993 on the financial sector, the Law of 30 May 2018 on markets in financial instruments, the Law of 17 December 2017 relating to undertakings for collective investment and the Law of 10 July 2005 on prospectuses for securities.

We therefore consider that asset tokens need to be analysed with respect to the concept of financial instruments and the laws and regulations applicable thereto.[16] Depending on the structure of a token, the latter may qualify as a transferable security, a unit in a collective investment undertaking or a token could serve as the underlying asset for a derivative contract.

Tokenisation of securities in Luxembourg has recently been given a serious push by the legislator through the adoption of the law of 1 March 2019 amending the law of 1 August 2001 concerning the circulation of securities. In its new Article 18 *bis*, the law provides that securities can be held using distributed ledger technologies and these technologies can also be used to register transfers.

10 Swiss Financial Market Supervisory Authority (FINMA) Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs) of 16 February 2018.

11 ibid.

12 Law of 10 November 2009 on payment services, on the activity of electronic money institution and settlement finality in payment and securities settlement systems – as modified by the law 20 July 2018.

13 FINMA Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs) of 16 February 2018.

14 ibid.

15 Germany Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) advisory letter WA 11-QB 4100-2017/0010, France Draft Law 'Relatif à la croissance et la transformation des entreprises' dated 19 June 2018, FINMA Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs) of 16 February 2018.

16 Article 1(19) of the law of 5 April 1993 and Annex II Section B of the same law.

i Transferable security

The Law of 30 May 2018 on markets in financial instruments[17] defines transferable securities as those classes of securities that are negotiable on the capital market, with the exception of instruments of payment, such as:

a shares in companies and other securities equivalent to shares in companies, partnerships or other entities, and depositary receipts in respect of shares;

b bonds or other forms of securitised debt, including depositary receipts in respect of such securities; and

c any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities or other indices or measures.

According to this definition, if a token is transferable, negotiable and embodies certain rights, it can prima facie be defined as a security:

a With regard to transferability, the Finance Working Group of the Blockchain Bundesverband considers in its statement[18] that transferability means that units can be assigned to another person, irrespective of the existence or not of a certificate that registers or documents the existence of the units. These concepts can be applied *mutatis mutandis* for Luxembourg. The important point is that the transfer can be made and registered without the need for a written document.[19]

b With regard to negotiability, such term needs to be analysed against the classical background of negotiability of securities. Securities are in particular negotiable when they are traded on exchanges or platforms.[20]

c As to the rights attached to the tokens, these need to be share-type rights, bond-type rights or rights that allow for the acquisition or sale of the above-mentioned type of security or rights related thereto.

A three-factor test can be applied to a token to determine whether it qualifies as a security:[21]

a The first factor is related to the economic rationale behind the issuing of the token. Why is the token issued? What is the project behind? Is it a business or economic project? What is the objective of the issuer?

b The second factor is related to the rights of the token owner. Are these share-type or bond-type rights?

17 Article 1(55) implementing Article 4(1)(44) of Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014.

18 Finance Working Group of the Blockchain Bundesverband Statement on Token Regulation with A Focus On Token Sales.

19 This is in line with Luxembourg law, which largely recognises unmaterialised securities, the Law of 1 August 2001 and the Law of 6 April 2013 on dematerialised securities.

20 See also BaFin advisory letter WA 11-QB 4100-2017/0010, which considers that 'trading platforms for cryptocurrencies can, in principle, be deemed financial or capital markets within the meaning of the definition of a security'.

21 Similar to the Howey Test created by the US Supreme Court for determining whether certain transactions qualify as investment contracts. See ICOs and financial regulation, presentation by Jean-Louis Schiltz at the Bourse de Luxembourg on 4 October 2017 and at the University of Münster on 7 November 2017.

c The third factor is linked to the purpose of the buyer or seller. Why is he or she buying the token? Is the holder participating in the profits made? Does he or she have an interest in the economic and financial development of the company or the project?

This test will be relevant and will assist in determining whether a token is a security. In practice, it could well be that the second and third factors (points (b) and (c) above) coincide in many instances.

The investment substance has to be considered. If in substance a token corresponds to a security and produces effects similar to those of a security, it has to be regulated like a security.[22] It should not be possible to argue that, because of the innovative character of tokens and due to their underlying technology, they would be exempted from complying with financial regulation, specifically but not only with regard to investor protection and anti-money laundering (AML) and counter-terrorism financing (CTF) aspects.[23]

ii Unit in a collective investment undertaking

A token could also be structured in such a way as to qualify as a unit in an investment fund, as defined by the Law of 17 December 2010 relating to undertakings for collective investment. A token could also be based on or represent a unit in a collective investment undertaking.

iii Underlying asset for a derivative contract

A token could also be used as an underlying asset for a derivative contract.[24] In that case, the derivative contract would classify as a financial instrument.[25]

In line with the ESMA paper, one of the conclusions of the qualification of tokens as financial instruments is that the firms involved in ICOs conduct regulated investment activities such as placing, dealing in or advising on financial instruments, or managing or marketing collective investment schemes.[26]

For instance, virtual currency exchange platforms that intend to allow trading of tokens, qualifying as financial instruments, on their platforms would need to be authorised as a multilateral trading facility under the law of 5 April 1993 on the financial sector.[27]

In conclusion, depending on the exact qualification of the token and on the financial service provided, the following regulations may apply:

a Law of 10 July 2005 on prospectuses for securities;
b Law of 5 April 1993 on the financial sector;
c Law of 30 May 2018 on markets in financial instruments;
d Law of 17 December 2010 relating to undertakings for collective investment;

22 This is in line with the FINMA approach, which, in assessing ICOs, looks at the economic function and purpose of the tokens that are issued. In other words, if it looks like a duck, swims like a duck, and quacks like a duck, then FINMA will treat it like a duck. So, using the duck test: payment tokens like Bitcoin or their newer cousins look like means of payment and are therefore subject to AML requirements. As asset tokens look like securities, they therefore fall under securities law. Keynote at the Swiss–UK Dialogue held on 13 March 2018 in London, Mark Branson FINMA Chief Executive Officer.

23 See Keynote at the Swiss–UK Dialogue held on 13 March 2018 in London, Mark Branson FINMA chief executive officer.

24 Point (4), (9) or (10) of Annex II Section B of the Law of 5 April 1993 on the financial sector.

25 Germany BaFin advisory letter WA 11-QB 4100-2017/0010.

26 ESMA statements of 13 November 2017.

27 Article 24-9 of the Law of 5 April 1993 on the financial sector.

e Law of 12 July 2013 on alternative investment fund managers; and
f Law of 12 November 2004 on the fight against money laundering and terrorist financing.

III BANKING AND MONEY TRANSMISSION

A money remittance business equivalent to a money services business (MSB) in the United States is regulated in Luxembourg by the Law of 10 November 2009 on payment services. Unlike MSBs in the United States, Luxembourg payment institutions are fully regulated.[28]

IV ANTI-MONEY LAUNDERING

The Law of 12 November 2004 on the fight against money laundering and terrorist financing applies to tokens as soon as they fall under the scope of financial sector regulation.

Virtual currency exchange platforms also have to comply with the Law of 12 November 2004, and more specifically with the requirements related to customer due diligence obligations, obligations of adequate internal organisation and the obligation to cooperate with the authorities.[29]

V REGULATION OF EXCHANGES

Virtual currency exchange platforms willing to establish in Luxembourg are required to obtain a licence as a payment institution. This requirement applies to platforms allowing for the exchange from virtual currencies to fiat currencies, and vice versa. It is important to highlight that only the fund flows that qualify as payment services are subject to regulation.

All legal requirements under the Law on payment services apply, meaning that exchange platforms will have to submit an application to the CSSF for authorisation as a payment institution. The Law on payment services furthermore requires that payment institutions, after having been granted the authorisation, need to comply on a permanent basis with the conditions for granting the authorisation, and to fulfil the reporting requirements to the CSSF.

i Authorisation procedure

According to the Law on payment services, no person other than a payment service provider shall be allowed to provide payment services in Luxembourg.

Like any payment institution, exchange platforms providing for virtual-to-fiat currency exchanges (and vice versa) willing to establish in Luxembourg will have to provide the CSSF with all the information required by law and listed in the application for authorisation form published on the CSSF website and implementing the European Banking Authority Guidelines.[30]

28 As we understand, payment institutions are basically subject to the Financial Crimes Enforcement Network requirements (i.e., AML and CTF) regulations.

29 See Section V.

30 Guidelines on the information to be provided for the authorisation of payment institutions and for the registration of account information service providers under Article 5(5) of Directive (EU) 2015/2366.

The authorisation form requires applicants to submit:

a identification details;
b a programme of operations;
c a business plan;
d the structural organisation of the business;
e evidence of the initial capital; and
f measures to safeguard the funds of payment services users.

Additionally, applicants have to submit to the CSSF:

a their governance and internal control mechanisms;
b their procedure for monitoring, handling and following up on security incidents and security-related customer complaints; and
c a process for the filing, monitoring and tracking of, and the restricting of access to, sensitive payment data and business continuity arrangements.

The form also requires the submission of:

a the principles and definitions applicable to the collection of statistical data on performance, transactions and fraud;
b a security policy document; and
c internal control mechanisms to comply with the obligations in relation to AML and CTF.

Furthermore, the CSSF shall require information on persons with qualifying holdings in the applicant to allow the CSSF to proceed to assess the identity and suitability of the directors and persons responsible for the management of the payment institution. The identity of the statutory auditors also has to be provided.

The CSSF application form requires that the information provided by applicants is true, complete, accurate and up to date, and that the applicants comply with all the provisions of the application form.

With regard to the level of detail of the information provided, it needs to be proportionate to the applicant's size and internal organisation, and to the nature, scope, complexity and risk of the services that the applicant intends to provide.

From a practical point of view, it needs to be emphasised that due to the innovative character of the services provided by virtual currency exchange platforms, specifically owing to the distributed ledger technology underlying virtual currencies and the fact that pure virtual currency transfers are currently not monitored by public authorities within the European Union, providers of those services should pay particular attention to information technology (IT), and AML and CTF risks, and in general the risks linked to their product.

ii Post-authorisation requirements

Once a licence is granted, virtual currency exchange platforms have to comply with the legal requirements set out by the Law on payment services on a permanent basis. Article 11 of the Law requires that, to ensure the sound and prudent management of a payment institution, it shall dispose for the performance of payment services of a robust internal governance arrangement that includes:

a a clear organisational structure with well-defined, transparent and consistent lines of responsibility;

b effective processes to identify, manage, monitor and report the risks they are or might be exposed to; and

c adequate internal control mechanisms, including sound administrative and accounting procedures as well as control and security arrangements for information-processing systems.

The arrangement, processes and mechanisms shall be comprehensive and proportionate to the nature, scale and complexity of the payment services provided by the payment institution.

Several CSSF circulars further define the obligations of a payment institution while operating in and out of Luxembourg.

Specific emphasis needs to be given to the requirement regarding entities' central administration. According to CSSF Circular 95/120, a payment institution must not only have a registered office in Luxembourg, but also has to have its central administration, including its decision-making centre and its head office, in Luxembourg. The Circular also explicitly requires that the persons responsible for the management, and the managers of various business and administrative functions or the various departments or divisions existing within the institution, in principle have to be permanently present on site as a matter of principle.

CSSF circulars also clarify the legal requirements with regard to the administrative and accounting organisation of a payment institution, as well as its internal control and compliance functions, and outsourcing requirements.[31]

Particular attention needs to be paid by exchange platforms to the circulars relating to institutions' IT security and the security of internet payments. Payment institutions are authorised to use cloud computing resources provided by an external cloud services provider to run their business.[32] For all practical purposes this is important because most, if not all, exchanges rely on cloud solutions.

Payment institutions must provide periodic reports to the CSSF. Circular 11/511 refers to the periodic reporting scheme for payments institutions.

After the end of the financial year, a short-form report as well as the final version of the periodic reporting tables and the internal audit and control reports have to be submitted to the CSSF. One month after the ordinary general meeting, a long-form audit report has to be submitted to the CSSF with a number of other corporate documents.

The compliance of payment institutions with all the requirements set out above is assessed in the context of the off-site prudential supervision and is subject to regular on-site inspections.

VI REGULATION OF MINERS

There are no specific licensing requirements for miners under Luxembourg law. However, if a miner exercises its activities in a professional way, he or she would have to apply for an ordinary business licence and hence be considered as a professional service provider.

31 Circular IML 96/126, Circular IML 98/143 (as amended by Circular CSSF 04/155), Circular CSSF 04/155.

32 Circular CSSF 17/654 clarifies the regulatory framework governing IT outsourcing relying on a cloud computing infrastructure provided by an external provider.

VII REGULATION OF ISSUERS AND SPONSORS

As discussed in Section II, if ICO tokens qualify as financial instruments, the firms involved in ICOs are conducting regulated financial activities in Luxembourg and therefore need to comply with relevant regulations.

An issuer of a token qualifying as a financial instrument will, for instance, be required to publish a prospectus according to the Law of 10 July 2005 on prospectuses for securities. Additionally, the new EU Prospectus Regulation will be applicable.[33]

It is relevant in this context that as of 21 July 2018, the Prospectus Regulation exempts security offers to the public with a total consideration in the European Union of less than €1 million, calculated over 12 months from the obligation to publish a prospectus.[34] The European legislator indeed considers that the costs of producing a prospectus are likely to be disproportionate to the envisaged proceeds of the offer.[35]

An additional exemption may apply, as the Prospectus Regulation offers Member States the option not to require the publication of a prospectus for offers of securities to the public not exceeding €8 million over 12 months, but only to the extent such offering is limited to one single Member State and such offerings shall not benefit from the passporting regime.[36]

Other exemptions shall also apply as of 21 July 2019. They relate, for example, to:

a offers made to qualified investors, or offers addressed to fewer than 150 persons per Member State (other than qualified investors);

b offers of securities whose denomination per unit amounts to at least €100,000; or

c offers addressed to investors who acquire securities for a total consideration of at least €100,000 per investor for each separate offer.[37]

Issuers will have to comply with the Law of 12 November 2004 on the fight against money laundering and terrorist financing.

Additionally, ordinary civil and commercial law provisions will apply to issuers.

VIII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

Most, if not all, of the laws referred to in this chapter contain provisions on enforcement carrying administrative as well as criminal sanctions. Ordinary civil, consumer protection, commercial and criminal law can also be applied in the context of fraud and enforcement.

33 Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market, and repealing Directive 2003/71/EC.

34 Article 1(3) of Regulation (EU) 2017/1129.

35 Recital 13 of Regulation (EU) 2017/1129.

36 Article 1(3) of the Regulation (EU) 2017/1129 is a Member State option. Draft Law 7328 aims to implement this option into Luxembourg law.

37 Article 1(4) of the Regulation (EU) 2017/1129.

IX TAX

Regarding direct taxation, the tax administration issued a circular on 26 July 2018,[38] the essential parts of which can be summarised as follows:

a virtual currencies are intangible assets for accounting and tax purposes;

b professionals mining or selling virtual currencies are subject to ordinary taxation; and

c in a non-professional environment, profits made through transactions whereby a virtual currency is exchanged against another currency (fiat or virtual), or whereby a virtual currency is used to pay for goods or services, are subject to taxation under the rules applying to speculation profits if the virtual currency transferred has been held for less than six months.

For indirect taxes, financial services are, in line with well-established EU law principles, not subject to VAT. The exchange of fiat currency against virtual currency itself shall not be subject to VAT as per the *Hedqvist* ruling of the European Court of Justice.[39]

X OTHER ISSUES

If a token corresponds to the definition of electronic money – that is, in substance a monetary value represented by a claim on the issuer, which is electronically stored and issued on receipt of funds for the purpose of making payment transactions, and is accepted by a natural or legal person other than the issuer – the issuer would have to apply for an e-money licence.[40]

Tokens backed by fiat currencies and designed solely in a way to be used as a payment instrument would fall under the remit of this definition.

The licensing process applicable to e-money issuers is similar to the process applicable to applicants for a payment institution licence.[41] Just like payment institutions, e-money institutions have to comply with the legal requirements set out by the Law on payment services on a permanent basis. CSSF circulars clarify the legal requirements.

XI LOOKING AHEAD

With distributed ledger technologies and cryptocurrencies here to stay,[42] since 2014 Luxembourg has shown its capacity to innovate in the sphere of fintech. We firmly believe that Luxembourg will also become an EU hub for regulated token offerings in the future.

38 Circulaire du directeur des contributions L.I.R. No. 14/5 – 99/3 – 99 *bis*/3 of 26 July 2018.

39 Court of Justice of the European Union Press Release No. 128/15 Luxembourg, 22 October 2015, Case C 264/14 *Skatteverket v. David Hedqvist*. This was confirmed by Circular No. 787 of 11 June 2018 of the Direction de l'Administration et des Domaines.

40 Article 1(29) of the Law on payment services.

41 Article 24-1 et seq. of the Law on payment services.

42 Luxembourg Finance Minister Speech in Hong Kong dated 16 January 2018.

Chapter 18

MALTA

Ian Gauci, Cherise Abela Grech, Terence Cassar and Bernice Saliba[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

Malta remains at the forefront of the major developments taking place within the blockchain and cryptocurrency scene, both within the European Union and globally. In 2016, the Maltese government set up a Blockchain Taskforce to help create and implement a national blockchain strategy aimed at materialising the opportunities of distributed ledger technology (DLT) and of setting the necessary safeguards. This strategy eventually resulted in three new laws relevant to the sector being published in 2018: the Virtual Financial Assets Act, Chapter 590 of the Laws of Malta (the VFA Act), the Innovative Technology Arrangements and Services Act, Cap 592 of the Laws of Malta (ITASA), and the Malta Digital Innovation Authority Act, Cap 591 of the Laws of Malta (the MDIA Act).

Considering the size of Malta's gaming sector, it is natural to link this thriving sector to the future of DLT; Malta was a trailblazer in the gaming sector and in its regulation of gaming law, creating a robust framework wherein licensees can operate in a well-regulated and flexible atmosphere.

Malta has not only enacted three full pieces of legislation but various stakeholders and authorities continue to release guidelines to assist in the application and implementation of these new laws. For instance, the Malta Gaming Authority has issued a position on virtual currencies and their adoption within the Maltese gaming context and has created a sandbox for the use of certain cryptocurrencies by MGA licensees. The Malta Financial Services Authority (MFSA) has also issued three Rulebooks covering the role of virtual financial asset (VFA) agents, issuers of initial coin offerings (ICOs) and providers of crypto services. Following the coming into force of the VFA Act and the finalisation of the aforementioned Rulebooks, the MFSA has recently approved the first batch of VFA agents and launched the application forms for prospective crypto services (VFA service providers) and issuers to respectively initiate the licensing process and white paper registration.

II SECURITIES AND INVESTMENT LAWS

Investment services rendered in relation to securities and financial instruments, whether traditional or dependent upon DLT, are regulated by the Maltese Investment Services Act,

1 Ian Gauci is a managing partner, Cherise Abela Grech and Terence Cassar are senior associates, and Bernice Saliba is a junior associate at GTG Advocates.

Chapter 370 of the Laws of Malta and the Markets in Financial Instruments Directive (MiFID). On the other hand, the VFA Act aims to regulate DLT assets, which are to be distinguished from financial instruments, electronic money and virtual tokens.

The VFA Act defines virtual tokens as a form of digital medium recordation whose utility, value or application is restricted solely to the acquisition of goods or services, either solely within a DLT platform on or in relation to which it was issued or within a limited network of DLT platforms. If a virtual token is or can be converted into another DLT asset type, it is treated as the DLT asset type into which it is or may be converted, unless its technical set-up prohibits the virtual token's conversion.

Electronic money is regulated in accordance with the Financial Institutions Act (Chapter 376 Laws of Malta) and specifically Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions.

The term VFA is defined as any form of digital medium recordation that is used as a digital medium of exchange, unit of account or store of value, and that is not electronic money, a financial instrument or a virtual token. Thus, primarily, the VFA Act aims to regulate assets that do not fall within the parameters of traditional security legislation.

To offer legal clarity regarding this distinction, the MFSA created the Financial Instrument Test. The Test must be applied to each DLT asset (i.e., financial instruments, electronic money or virtual tokens dependant on DLT) to determine its nature and the respective applicable legal framework based on the token's features.

Once the type of DLT asset is determined, the following legal regime will be applicable:

a virtual tokens are not regulated by any specific body of law in Malta;

b financial instruments are defined as set out in the MiFID and thus regulated by financial services legislation;

c electronic money is regulated in Malta by the Financial Institutions Act; and

d VFAs are regulated by the VFA Act.

The Test is expected to be carried out compulsorily within the context of an ICO for VFAs, referred to as an initial VFA offering (IVFAO) by the issuer and his or her VFA agent. It must also be carried out by persons providing any service or performing any activity within the context of the VFA Act or traditional financial services legislation in relation to DLT assets whose classification has not been determined. Given that the type of DLT asset may change during its lifetime, the MFSA may at any time order the conduct of the Test again to obtain an update on the determination of a DLT asset. If the DLT asset is not issued in or from Malta, the Test must be conducted before any service involving the asset is provided in Malta.

If a DLT asset, such as a securitised token, is considered to be a financial instrument by the Financial Instrument Test, then it is to be regulated by financial services legislation. In this case, rather than conducting an IVFAO or ICO, the issuer would need to assess whether the security token offering qualifies as an offer to the public or not. If it is deemed to constitute an offer to the public, then a prospectus must be drafted and registered with the authority in line with the Prospectus Regulation (as of 21 July 2019).

III BANKING AND MONEY TRANSMISSION

When addressing the holding of cryptocurrencies between issuer and investor during the undertaking of a VFA service, the VFA Act makes reference to wallets.

The VFA Act addresses custodian and nominee services and defines them as a VFA service licensable under the Act. Under the VFA Act, acting as a custodian or nominee holder of VFAs or private cryptographic keys, or both, or if in conducting such activities the nominee is holding such assets or keys on behalf of another person, these are considered to be VFA services.

According to the VFA Act, an issuer must provide a detailed description of the issuer's wallet or wallets used in the white paper along with a description of the 'security safeguards against cyber threats to the underlying protocol, to any off-chain activities and to any wallets used by the issuer'. The Act thus addresses security measures that are paramount to the existence and reliability of a wallet. The Act does not impose any requirements in terms of the actual technology to be used when hosting such wallets, thus ensuring the intended neutrality of the law.

If a DLT asset is classified as electronic money, it continues to be regulated by the Financial Institutions Act, and ancillary rules and regulations.

The provision of banking services in relation to cryptocurrencies, and more specifically VFAs, continues to be regulated by financial services legislation through the Banking Act, and ancillary rules and regulations.

IV ANTI-MONEY LAUNDERING

Money laundering is criminalised primarily by means of the Prevention of Money Laundering Act and the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR). The PMLFTR contain detailed provisions on the measures and procedures to be maintained and applied by subject persons.

As with all new technologies, there are often hurdles that stand between advancement and stasis. Anti-money laundering could be considered to be one such hurdle in the sphere of cryptocurrency regulation. Concerns about money laundering and the funding of terrorism are often the rationale behind the banning of virtual currencies entirely. One of the primary risks noted by the authorities, along with regulators around the globe, is the anonymous and pseudo-anonymous nature of cryptocurrencies.

The Prevention of Money Laundering Act and the PMLFTR are supplemented by the Implementing Procedures issued by the Financial Intelligence Analysis Unit (FIAU). The Implementing Procedures are binding on subject persons, and failure to comply is subject to an administrative penalty.

The term subject persons is defined in the PMLFTR as 'any legal or natural person carrying out either relevant financial business or relevant activity'. The terms relevant activity and relevant financial business are further defined and, as yet, make no specific reference to virtual currencies or issuers thereof. The VFA Act therefore has extended the term subject person to include issuers of VFAs conducting an IVFAO as well as those offering VFA services. The VFA Regulations also set out that the term includes persons who are acting under an exemption from the requirement of a VFA licence. This therefore means that the provisions of the PMLFTR as well as the FIAU Implementing Procedures regulate the procedures and measures to be adopted by such persons under the VFA Act with regards to anti-money laundering and countering the funding of terrorism.

Subject persons, therefore, as defined in both the PMLFTR and the VFA Act, must take appropriate steps to identify the risks of money laundering and the funding of terrorism that could arise out of their business activities. This risk assessment must be properly documented, as the FIAU may demand this documentation.

Subject persons under the VFA Act are required to appoint and have a money laundering reporting officer (MLRO) in place at all times. The role is an onerous one and can only be held by individuals who fully understand the extent of the responsibilities attached to it. The MLRO must be a senior employee or a member of the board of administration.

In 2016, the European Commission proposed a fifth revision of the Anti-Money Laundering Directive. The proposal included measures that aimed to enhance the powers of the European Union in the fight against money laundering, as well as to introduce safeguards in the area of virtual currencies.

One of the changes that affected the cryptocurrency sphere was the extension of the scope of the Directive to cover both wallet providers and exchange service providers. Perhaps the most important change that came about through this revision was the inclusion of a definition of virtual currencies. This definition ensures that providers of exchange services and custodian wallet providers would also have to comply with the Directive.

The definition states that virtual currencies are 'a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency, and does not possess a legal status of currency or money, but is accepted by natural or legal persons, as a means of exchange, and which can be transferred, stored and traded electronically'. This definition ensures that the concepts of electronic money and funds are entirely separate to that of virtual currencies.

The preamble to the Fifth Anti-Money Laundering Directive, which was adopted in April 2018, also provides further clarity, stating that virtual currencies may be used as a means of exchange, for investment purposes, as store-of-value products or in online casinos. It is important to note that the Fifth Anti-Money Laundering Directive also limits itself to regulating fiat-to-crypto exchanges and not crypto-to-crypto exchanges.

The FIAU has issued a consultation document that is intended to be an updated version of the current Implementing Procedures, with the purpose of extending their scope to the VFA legal framework.

V REGULATION OF EXCHANGES

The VFA Act regulates virtual exchanges established in Malta to protect investors from fraud and market abuse to combat money laundering and the financing of terrorism activities, and to ensure that exchanges operate using reliable technology.

The VFA Act only allows VFAs to be admitted on VFA exchanges. Indeed, DLT assets that are qualified as financial instruments through the Financial Instrument Test must be exchanged on traditional financial markets. Virtual tokens as defined in the VFA Act cannot be exchanged on a DLT exchange; in fact, if a virtual token is traded on a DLT exchange it would change the nature of a virtual token, causing it to be regulated either by the VFA Act or traditional financial services laws.

Operating a VFA exchange is expressly considered as one of the VFA services listed in the Act. As a VFA service provider, the operator of a VFA exchange must therefore comply with all the requirements governing the offer of a VFA service. It must:

a be a legal person established in Malta;

b establish different entities if it wishes to conduct activities incompatible with its VFA licence;

c select a VFA agent approved by the MFSA to act as liaison between the exchange and the MFSA during the licensing process, and to ensure that the provisions of the Act are properly complied with;

d apply, through its VFA agent, and obtain a licence granted by the MFSA, and comply with the rules and regulations applicable to licence holders;

e conduct the Financial Instrument Test on all the DLT assets listed on the exchange both when admitting that asset for trading onto the exchange and when the asset changes in nature;

f circulate advertisements that are accurate and consistent;

g appoint a MLRO who must be a senior employee of the licensee, its compliance officer or a member of the board of administration;

h appoint a compliance officer responsible for the compliance function of the exchange and for any reporting required by the MFSA Rules; and

i comply with all the relevant regulations made in application of the Act, such as the MFSA Rules.

The operator of a VFA exchange may offer other VFA services provided it holds a licence to do so. However, a VFA licence holder may not offer VFA services that are not covered by the licence held by the VFA licensee and may not conduct other business activities requiring a licence under Maltese law unless it establishes separate entities for these activities. This segregation of activities, particularly when offering both services under the VFA Act and services under the financial services framework, is intended to better protect investors' assets.

The MFSA may require access to all information related to any asset traded on a VFA exchange. As the competent authority, it may decide or demand that a VFA exchange discontinue or suspend the trading of an asset, and even any derivative related to it, if the asset no longer complies with the definition of a VFA, if it believes or suspects that a provision of the Act has been infringed, or if the orderly transaction of business is being prevented.

The Act also regulates the advertisement of the admission of a VFA to trading on a VFA exchange. Advertisements must be clearly identifiable as such, and may not include inaccurate or misleading information. The information must also be consistent with the required contents of the white paper. Furthermore, no person other than a VFA licence holder may issue an advertisement relating to a VFA service in or from Malta unless its contents have been vetted and approved by the licence holder's board of administration.

A VFA exchange must ensure that it is equipped with effective systems of detecting possible market abuse. Any suspicion of market abuse must be reported immediately to the MFSA. This refers to instances of insider dealing, unlawful disclosure of inside information and market manipulation when dealing with VFAs.

VI REGULATION OF MINERS

The VFA Act is drafted with technology neutrality in mind, and its application is therefore not based on the way a coin is created (whether by proof of work, proof of stake or other consensus mechanisms).

Nevertheless, miners remain generally unregulated within the context of Maltese law. Reference is, however, made to miners within the 'Guidelines for the VAT Treatment of

transactions or arrangements involving DLT Assets', which provide that should miners receive payment for other activities, such as services in connection with the verification of a specific transaction, these services are deemed to be a chargeable event, with applicable Maltese VAT standard rates.

VII REGULATION OF ISSUERS AND SPONSORS

The VFA establishes legal definitions of numerous cryptocurrency and DLT-related concepts, offering legal certainty to business promoters and investors alike. The concept of an initial coin offering is termed an IVFAO, which excludes the issue of a virtual token and a financial instrument.

Any person wishing to offer a VFA to the public in or from Malta, or wishing to apply for the VFA's admission to trading on a DLT exchange, must draw up a white paper in line with the VFA Act and register it with the MFSA 10 working days before the date of its circulation in any way whatsoever. Thus, to conduct an IVFAO, it would be necessary to conduct the Financial Instrument Test to ensure that the DLT asset is in fact a VFA. The Test is discussed at length in Section II.

The issuer must be a legal person managed by at least two individuals to ensure the principle of dual control and to appoint a board of administrators, an MLRO, an auditor and, where necessary, a custodian and a systems auditor. Issuers are also required to:

a conduct their business with honesty and integrity;
b communicate with investors in a fair, clear and non-misleading manner;
c conduct their business with due skill, care and diligence;
d identify and manage any conflict of interest that may arise;
e have effective arrangements in place for the protection of investors' funds;
f have effective administrative arrangements; and
g maintain all their systems and security access protocols to appropriate international standards.

The white paper must describe the IVFAO project in simple and informative terms and must be registered with the competent authority (the MFSA). The MFSA may, in certain specific cases, prohibit or suspend an IVFAO.

The white paper issued for an IVFAO must include information that, according to the particular nature of the issuer and of the VFAs offered to the public, is necessary to enable investors to make an informed assessment of the prospects of the issuer, the proposed project and the features of the VFA. The white paper may not contain a condition requiring or binding an investor to waive compliance with any requirement under the VFA Act, or purporting to affect the investor with notice of any contract, document or matter not specifically referred to in the white paper. The VFA agent is required to confirm that the white paper complies with the requirements of the VFA Act.

The VFA agent is also required to advise and guide the issuer as to its responsibilities and obligations under the VFA Act. The VFA agent must also receive and retain all documentation and information to demonstrate how, and to what extent, the issuer has satisfied the requirements prescribed in the VFA Act and of any ancillary rules or regulations insofar as they apply to any offer or admission to trading. This includes ensuring that the issuer is

considered to be a fit and proper person to carry out such activities, and demonstrating how the issuer has complied and, as far as it can be determined, will comply with its continuing obligations under the VFA Act.

Before issuing an IVFAO, the issuer must also provide a copy of the audited annual accounts for the past three financial years and a confirmation by its systems auditor that its technology arrangement complies with the qualitative standards and guidelines issued by the Malta Digital Innovation Authority (MDIA), a new DLT regulator created by the government.

The VFA Act also regulates the advertisement of any IVFAO. Such advertisement must be clearly identifiable as such, and may not include inaccurate or misleading information. The information must also be consistent with the required contents of the white paper.

VIII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

The VFA Act, together with the Virtual Financial Asset Regulations and the ancillary MFSA Rulebooks, confer the minister responsible for the regulation of financial services and the MFSA with powers to protect investors' interests while also overseeing the orderly transaction of business, primarily that of IVFAOs and VFA service providers.

Issuers of VFAs are liable for damages sustained by a person as a direct consequence of that person having bought VFAs, either as part of an IVFAO by the issuer or on a DLT exchange, on the basis of any false information contained in a white paper, on a website or in an advertisement. A statement included in a white paper, on a website or in an advertisement is deemed to be untrue if it is misleading or otherwise inaccurate or inconsistent, either wilfully or in consequence of gross negligence, in the form and context in which it is included.

The MFSA may suspend or terminate the trading of a VFA if this is in the interest of the VFA exchange, investors or the general public. Conversely, to avoid causing significant damage to investors' interests or the orderly functioning of a VFA exchange, the VFA exchange may suspend or remove from trading a VFA that no longer complies with the definition of a VFA or with its by-laws.

The MFSA may impose unilateral decisions on any issuer of an IVFAO and on any VFA agent or VFA service provider. It is thus empowered to:

a request information from any person;
b order the review of the determination of a DLT asset and submit this determination to a test;
c appoint inspectors to investigate and report on the activities of an issuer, VFA agent or VFA service provider;
d order an issuer or service provider to cease operations or appoint a person to advise him or her, take charge of his or her assets, or even control his or her business;
e order the suspension or the discontinuation of the trading of a VFA; and
f impose administrative penalties.

Where a VFA licence holder, or the secretary, a member of the board of administration or any other person responsible for a licence holder, contravenes or fails to comply with any of the licence conditions, or he or she is deemed to be in breach of the VFA Act, regulations or rules, including through a failure to cooperate in an investigation, the MFSA may impose an administrative penalty of up to €150,000 by notice in writing and without recourse to a court hearing.

In the public interest, most decisions made by the competent authority are subject to appeal in front of the Financial Services Tribunal.

IX TAX

The VFA Act does not put in place any specific tax regime in relation to cryptocurrencies, and more specifically VFAs. However, the VFA Act provides that regulations may be drawn up by the responsible minister to address certain tax matters, thus allowing for further regulation outside the main Act. In fact, the Maltese Inland Revenue Department has issued guidelines for the treatment of VAT for transactions involving DLT, guidelines on the Income Tax Treatment of transactions or arrangements involving DLT Assets, and Guidelines for the purpose of the Duty on Documents and Transfers Act. The guidelines address the various types of DLT Assets that exist, including the treatment of hybrid tokens.

Under the Income Tax Rules, the guidelines provide that any payment carried out in cryptocurrencies is to be treated as payment made or received in other currencies. However, generally, to determine duty on document transfers, this determination is to be made on a case-by-case basis. Charging of VAT depends on whether a specific good or service is identified.

On other matters ancillary to tax, the responsible minister can issue regulations to be able to organise compensation schemes for investments, and those schemes are exempt from the payment of income tax as of their date of establishment.

Furthermore, the First Schedule of the VFA Act provides that when drawing up a white paper to offer a VFA, any applicable tax that might apply to that VFA is to be included in the white paper.

X OTHER ISSUES

The VFA Act does more than just regulate the roles of issuers and exchanges; in fact, the Second Schedule of the VFA Act refers to other services that, when provided in relation to VFAs, constitute a licensable activity under the VFA Act. These include:

a the receipt and transmission of orders;
b the execution of orders on behalf of other persons;
c dealing on own account;
d portfolio management;
e custodian and nominee services;
f investment advice; and
g the placing of VFAs.

Following the entry into force of the Act, these activities require a licence to operate in or from Malta, and must comply with the ongoing obligations set out in the Act.

The accompanying Regulations to the Act and MFSA rules emerging from the Rulebook contain detailed provisions on the licensing requirements for VFA service providers and the licensing process.

The Regulations provide for four classes of licences, which each have varying minimum capital requirements.

All prospective VFA service providers must be set up as a legal person managed by at least two individuals to ensure the principle of dual control; this was, in fact, one of the

changes carried out to the VFA legal framework with the adoption of the third Rulebook for VFA Service Providers. Prospective VFA service providers must appoint a money laundering reporting officer and a compliance officer. The VFA service provider may also be required to appoint a systems auditor in relation to its innovative technology arrangement. The VFA service provider must also establish a cybersecurity framework, maintain adequate risk management policies and procedures, safeguard clients' rights in relation to virtual financial assets and money, and keep records of all its services and transactions.

The VFA Act also regulates the role of the VFA agent who is responsible for representing a prospective VFA service provider before the MFSA, and who acts as an intermediary between the authority and the provider. An issuer of VFAs or any VFA service provider seeking licensing or authorisation under the Maltese regime is required to appoint a VFA agent to apply on his or her behalf.

An application for a VFA services licence may only be done through a VFA agent. The VFA agent is required, diligently and with utmost good faith, to submit full and correct information whenever it is required to do so; and to support the MFSA in carrying out its reviews to establish that the applicant is a fit and proper person to provide the VFA service, that it has a good reputation, that it is competent and solvent, and that it will comply with and observe the requirements of the VFA Act, and any regulations made and rules issued thereunder and that are applicable to it.

The government has also created a new DLT regulator, the MDIA. The MDIA will be tasked with issuing certifications for innovative technology arrangements, which are primarily regulated under the ITASA. Innovative Technology Arrangements include types of DLT, smart contracts and DAOs. The ITASA's certification regime is a voluntary one, unless an Innovative Technology Arrangement is used with VFAs.

XI LOOKING AHEAD

The VFA Act and ancillary regulations and rules were drafted with technology neutrality in mind to be able to keep abreast with technological advancements in this field. As Malta begins to regulate cryptocurrency-related activities through its licensing regime, the regulator will undoubtedly respond to the industry's requirements, and assess the efficiency and applicability of the legal regime to consider any possible amendments for its improvement. The government is now also looking ahead, having already set up an artificial intelligence (AI) taskforce and outlined the first details of Malta's AI policy focusing on investment, start-ups and innovation, and public sector adoption and private sector adoption.

Chapter 19

NEW ZEALAND

Deemple Budhia and Tom Hunt[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

Virtual currencies and services related to virtual currencies in New Zealand are regulated by existing, technology-neutral legislation. Given that the rights and functions created in respect of virtual currencies are flexible, each virtual currency or service associated with virtual currencies will be regulated according to its specific properties.

For the purposes of this chapter, the term virtual currencies includes all digital tokens that are recorded on a blockchain ledger.

II SECURITIES AND INVESTMENT LAWS

The Financial Markets Authority (FMA) has responsibility for the regulation of financial products in New Zealand, and the Financial Markets Conduct Act 2013 (FMCA) is the principal piece of legislation that regulates financial products. The primary purposes of the FMCA are to promote the confident and informed participation of businesses, investors and consumers in New Zealand's financial markets, and to promote and facilitate the development of fair, efficient and transparent financial markets.

Offers of financial products in New Zealand are regulated by the FMCA and regulations made under the FMCA (the Regulations). The FMCA and the Regulations:

a impose fair dealing obligations on conduct in both the retail and wholesale financial markets;

b set out the disclosure requirements for offers of financial products;

c set out a regime of exclusions and wholesale investor categories in connection with the disclosure requirements;

d set out the governance rules that apply to financial products; and

e impose licensing regimes.

In general under the FMCA, issuers of financial products must comply with various fair dealing obligations and certain disclosure, governance and operational obligations (subject to certain exceptions). The fair dealing provisions are concerned with misleading or deceptive conduct, and false, misleading or unsubstantiated representations. Failure to comply with the appropriate obligations may result in criminal or civil liability, or both, under the FMCA, and may result in material financial penalties, imprisonment, or both.

---

1 Deemple Budhia and Tom Hunt are partners at Russell McVeagh. The authors would like to acknowledge the contributions of Hamish Journeaux, Michael van de Water and Young-chan Jung.

At a high level (and subject to the detail below), the disclosure and governance provisions of the FMCA will only apply to the offer of a virtual currency if:

a it is offered in New Zealand;

b it is made under a regulated offer; and

c the relevant virtual currency falls within one of the categories of financial product in the FMCA, or is otherwise designated as a financial product by the FMA.

i Offers in New Zealand

The obligations imposed under the FMCA apply to offers of financial products in New Zealand, regardless of where the issue occurs or where the issuer is based. An offer is deemed to have been offered in New Zealand if it is received by a person in New Zealand (including electronically), unless the issuer can demonstrate that it has taken all reasonable steps to ensure that persons in New Zealand to whom disclosure would otherwise be required under the FMCA may not accept the offer.

ii Regulated offers

An offer of financial products that requires disclosure under the FMCA is a regulated offer. An offer of financial products for issue requires disclosure to investors unless an exclusion applies to all persons to whom the offer is made. Certain specified offers of financial products for sale will also require disclosure to investors. The form and content of the disclosure required in relation to each financial product is set out in the Regulations and is tailored according to the characteristics of the particular financial product being offered.

The FMCA provides that a person must not make a regulated offer unless the issuer has prepared a product disclosure statement (PDS) for the offer, has lodged that PDS with the Registrar of Financial Service Providers (the Registrar) and has prepared an online register with the prescribed information.

An offer that is not a regulated offer will still be subject to the fair dealing provisions in the FMCA. As noted above, these provisions prevent people from making false or misleading statements or unsubstantiated representations. Similar obligations are imposed under the Fair Trading Act 1986.

iii Types of financial product

There are four categories of financial products under the FMCA: debt securities, equity securities, managed investment products and derivatives.

Virtual currencies are regulated by the FMCA only to the extent that a particular virtual currency meets the definition of one these categories of financial product. The FMCA sets out a hierarchy of financial products, such that a virtual currency that would prima facie satisfy the definition of more than one category of financial product will default into only one category.

Debt securities

A debt security is defined as a right to be repaid money, or paid interest on money, where that money is deposited, lent to or otherwise owing by any person. Importantly, for the purposes of the definition of debt security, money does not include money's worth. Several prominent virtual currencies, such as Bitcoin and Ether, do not constitute debt securities because there is not a right to be repaid money or to be paid interest by the issuer, or anyone else.

Equity securities

An equity security is narrowly defined in the FMCA as a share in a company, an industrial and provident society, or a building society, but does not include a debt security.

While a blockchain could mimic a traditional share register (with each unit of the virtual currency representing a single share, and shareholders being able to represent trades in those shares by trading in those units), the virtual currency itself would not constitute a share in a company, an industrial and provident society, or a building society. As such, a virtual currency could not be an equity security as defined in the FMCA. This is the case even where a virtual currency gives holders rights traditionally associated with equity (such as certain profit and governance rights).

Managed investment products

A managed investment product refers to an interest in a managed investment scheme, which is broadly defined to include any scheme:

a the purpose or effect of which is to enable participating investors to contribute money to the scheme to acquire an interest in the scheme;

b where the interests are rights to participate in or receive financial benefits produced principally by the efforts of others; and

c where participating investors do not have day-to-day control over the operation of the scheme.

If a product is classified as a debt security or an equity security it would not be a managed investment product.

If a virtual currency is classified as a managed investment product, the FMCA imposes significant disclosure and governance requirements on the underlying managed investment scheme. These requirements include registering the scheme with the Registrar; complying with reporting and governance requirements; and requiring the appointment of a licensed manager and licensed independent supervisor, each of which owe statutory duties of care to investors.

In practice, the nature of a virtual currency may make it impractical or impossible to fully comply with these additional requirements. For example, one of the functions of the manager of a managed investment scheme is to manage the scheme property and investments. This requirement is not compatible with a decentralised blockchain where the scheme property is held in (for example) an Ethereum account associated with a smart contract. If there were a manager who had overall control over this account, the decentralised nature of the blockchain and the autonomous nature of the smart contract would be undermined.

By way of example, the DAO and DAO tokens, which were the subject of a report in 2017 by the United States' Securities and Exchange Commission, could have been characterised as a managed investment scheme and managed investment products (respectively) under the FMCA.[2]

2 https://www.russellmcveagh.com/getattachment/Insights/August-2017/Initial-Coin-Offerings-not-immune-from-regulatio/Initial-Coin-Offerings.pdf.

Derivatives

A derivative is defined as an agreement under which consideration is, or may be, payable to another person at some future time and the amount of the consideration is ultimately determined, is derived from or varies by reference to (in whole or in part) the value or amount of something else (including an asset, interest rate, exchange rate, index or commodity). A derivative does not include, inter alia, a debt security, equity security or managed investment product. Certain virtual currencies that are tied to the value of fiat currencies, or that are tied to commodities such as gold (stablecoins), could constitute a derivative under the FMCA.

iv FMA designation and exemption powers

The FMA has certain designation powers under the FMCA, including the power to designate:

a that a security that would not otherwise be a financial product is a financial product of a particular kind. A security is an arrangement or facility that has, or is intended to have, the effect of a person making an investment or managing a financial risk. The FMA has expressed the view that all digital tokens issued in an initial coin offering (ICO) will constitute a security for the purposes of the FMCA; or

b that a financial product is, or is to become, a financial product of a particular kind. For example, if a virtual currency fell within the definition of managed investment product, the FMA could designate such interests as equity securities. In that case, the issuer would still be required to provide disclosure to investors, but would not be subject to the prescriptive governance obligations described above.

Alternatively, the FMA has the power to exempt any person or class of persons, or any transaction or class of transactions, from compliance with certain obligations imposed under the FMCA. For example, the FMA could exempt an issuer of a virtual currency classified as a managed investment product from some of the provisions that would otherwise apply to the issuer.

III BANKING AND MONEY TRANSMISSION

The Reserve Bank of New Zealand (RBNZ) has responsibility for the prudential regulation of registered banks, non-bank deposit takers and insurers in New Zealand. The RBNZ does not directly regulate virtual currencies. However, as New Zealand's central bank, the RBNZ is responsible for promoting the maintenance of a sound and efficient financial system.

Money transmission services in New Zealand are regulated separately by the Financial Service Providers (Registration and Dispute Resolution) Act 2008 (the FSP Act) and the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the AML/CFT Act). As the anti-money laundering regime is discussed in Section IV, this section is limited to the FSP Act.

Subject to certain limited exceptions, the FSP Act applies to any person who carries on the business of providing a financial service (a financial service provider) and:

a is ordinarily resident in New Zealand or has a place of business in New Zealand;

b is required to be a licensed provider under a licensing enactment (which includes registered banks, authorised financial advisers, licensed insurers and certain licensed supervisors); or

c is required to be registered under the FSP Act by any other enactment.

The core requirement of the FSP Act is that financial service providers must be registered for the relevant financial service on the Financial Service Providers Register (FSPR). Financial service providers that provide financial services to retail clients must also join an approved dispute resolution scheme, subject to certain limited exceptions.

The term financial service includes, inter alia, operating a money or value transfer service, and issuing and managing means of payment.

The FMA has issued guidance (the Guidance) stating that in the context of virtual currency services, exchanges, wallets and ICOs may be considered financial services under the FSP Act.[3] By way of example, exchanges allowing virtual currency trading will, according to the Guidance, be operating a value transfer service under the FSP Act. Similarly, the Guidance states, a wallet provider that stores virtual currency or money on behalf of others, and facilitates exchanges between virtual currencies or between money and virtual currencies, will also be operating a value transfer service. The Guidance also points out that trading of virtual currencies that are financial products may also trigger the need for a licence to operate a financial product market under the FMCA.

Enforcing the provisions of the FSP Act in relation to public blockchains is somewhat difficult in practice. The primary issue is that a public blockchain may not be managed by one particular entity, but instead may be managed by the relevant blockchain community. As the core requirement of the FSP Act is that financial service providers are registered, this may prove to be difficult as there may not be one person or organisation who is able to register.

IV ANTI-MONEY LAUNDERING

New Zealand's anti-money laundering regime is set out in the AML/CFT Act, which applies to reporting entities. A reporting entity includes, inter alia:

a financial institutions, which are defined as any person who, in the ordinary course of business, carries on one or more of the financial activities listed in the AML/CFT Act. Those financial activities include transferring money or value for, or on behalf of, a customer, issuing or managing the means of payment, and money or currency changing; and

b any other person or class of persons deemed to be a reporting entity under the regulations or any other enactment.

The AML/CFT Act imposes customer due diligence, reporting and record-keeping requirements on reporting entities. It also requires reporting entities to develop and maintain a risk assessment and a risk-based AML/CFT programme. The AML/CFT Act provides for external supervision of reporting entities by the FMA, the RBNZ or the Department of Internal Affairs. The functions of an AML/CFT supervisor are to, inter alia, monitor the level of risk of money laundering and the financing of terrorism involved across all the reporting entities it supervises; and monitor the reporting entities it supervises for compliance with the AML/CFT Act.

Obligations under the AML/CFT Act generally apply to a reporting entity only to the extent that it provides one of these financial activities to a customer. The term customer is

3 https://fma.govt.nz/compliance/cryptocurrencies/cryptocurrency-services/.

very broadly defined. By way of example, an exchange that allows virtual currency trading could be a reporting entity under the AML/CFT Act, and entities that trade on the exchange could be its customers.

The AML/CFT Act does not specify the territorial scope of the Act. The AML/CFT supervisors have issued guidance on the territorial scope, which states that the relevant financial activities caught by the AML/CFT Act 'must be carried on in New Zealand in the ordinary course of business', and that this implies a place of business in New Zealand. The guidance is difficult to apply to blockchain-based technologies where the technology is online and therefore is not necessarily carried on in New Zealand even though it is accessible to persons in New Zealand.

In the case of virtual currencies, compared to more conventional circumstances contemplated when the AML/CFT Act was enacted, it can be challenging to interpret the legislation to determine who constitutes a reporting entity and a customer. More practically, the inherent anonymity that comes with using many virtual currencies may impose significant challenges for reporting entities to realistically be able to conduct customer due diligence on customers.

In addition, the issues discussed above in relation to the FSP Act also apply to the AML/CFT Act. The lack of a clear owner or manager of a particular virtual currency may make it difficult for regulators to identify the entity that should be complying with the obligations under the AML/CFT Act, and to bring a claim for a breach of obligations.

V REGULATION OF EXCHANGES

Exchanges are regulated by the FMCA if the exchange constitutes a financial product market. The FMCA defines a financial product market as a facility by means of which:

a offers to acquire or dispose of financial products are made or accepted; or

b offers or invitations are made to acquire or dispose of financial products that are intended to result, or may reasonably be expected to result, directly or indirectly, in:
- the making of offers to acquire or dispose of financial products; or
- the acceptance of offers of that kind.

Virtual currency exchanges could therefore be regulated if the relevant virtual currency being exchanged constitutes a financial product under the FMCA.

A person must not operate, or represent to others that the person operates, a financial product market in New Zealand unless such person has a licence to operate the market under the FMCA or the market is exempt from licensing. A financial product market is taken to be operated in New Zealand if:

a it is operated by an entity that is incorporated or registered in New Zealand or by an individual who is ordinarily resident in New Zealand;

b all, or a significant part of, the facility for the financial product market is located in New Zealand; or

c the financial product market is promoted to investors in New Zealand by or on behalf of the operator of that market, or by or on behalf of an associated person of that operator. However, a financial product market is not promoted to investors in New Zealand merely because it is accessible by those investors.

As noted in Section III, the Guidance indicates that the FMA considers that the licensing regime under the FMCA could apply to virtual currency exchanges.

Licensed market operators must have FMA-approved market rules, and comply with certain disclosure and reporting obligations to ensure that every licensed market is a fair, orderly and transparent market.

VI REGULATION OF MINERS

Miners are not expressly regulated in New Zealand. However, there are certain criminal offences, discussed in Section VIII, which relate to accessing computer systems for dishonest purposes. In that case, miners who choose to improperly access the processing power of another person's computer system to mine a virtual currency would be committing an offence under New Zealand law.

VII REGULATION OF ISSUERS AND SPONSORS

New Zealand has a disclosure-based approach to the offer of financial products to the public. An offer of financial products for issue will require full disclosure to investors under the FMCA, unless an exclusion applies (as discussed in Section II.ii).

In addition, certain offers of financial products for sale (secondary sales) also require disclosure. For example, if financial products are issued (but not, inter alia, under a regulated offer) with a view to the original holder selling the products and the offer for sale is made within 12 months of the original issue date, that secondary offer will require disclosure.

As discussed in Section II.ii, for a regulated offer of financial products a PDS must be prepared, and certain information relating to the offer must be contained in a publicly available register entry for the offer. The PDS must be lodged with the Registrar, and the register entry must contain all material information not contained in the PDS. Material information means information that a reasonable person would expect to, or to be likely to, influence persons who commonly invest in financial products in deciding whether to acquire the financial products on offer, and is specific to the particular issuer or the particular financial product. Investors to whom disclosure is required must (subject to certain exceptions) be given the PDS before an application to acquire the relevant financial products under a regulated offer is accepted or the financial product is issued.

The Regulations set out detailed requirements for the timing, form and content of initial and ongoing disclosure for financial products, including limited disclosure for products offered under certain FMCA exclusions. The content requirements for a PDS are prescriptive and include prescribed statements and page or word limits. The Regulations impose different disclosure requirements for different types of financial products.

The FMCA includes an exclusion for offers to wholesale investors, which include:

a investment businesses;
b people who meet specified investment activity criteria;
c large entities (those with net assets of at least NZ$5 million or consolidated turnover over NZ$5 million in each of the two most recently completed financial years);
d government agencies;
e eligible investors;
f persons paying a minimum of NZ$750,000 for the financial products on offer;
g persons acquiring derivatives with a minimum notional value of NZ$5 million; and
h bona fide underwriters or sub-underwriters.

Even where an exclusion (including the wholesale investor exclusion) applies, certain disclosure requirements may still apply.As discussed above, the application of these provisions to offers of virtual currencies turns on whether they are a financial product or are designated a financial product by the FMA.

VIII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

The New Zealand courts have held that intangible property is capable of being property for the purposes of criminal law. Accordingly, under the Crimes Act 1961 (the Crimes Act) – the primary piece of legislation that prescribes criminal offences in New Zealand – there are a number of criminal offences that could apply to the use of virtual currencies. These include theft, obtaining property or causing loss by deception, as well as crimes involving computers.

It is an offence to obtain property or valuable consideration by deception, or cause loss to another person by deception. This could cover circumstances in which a person is scammed by a malicious issuer of an ICO (where the issuer purports to raise money for a project by issuing virtual currency in an ICO with no intention of honouring its obligation to deliver certain products or services to the investor who purchased the virtual currency). In this particular situation, the FMCA also provides for offences for misleading or deceptive conduct in relation to disclosure of information made by the issuer under the FMCA.

It is possible that the general offence of theft could also apply to virtual currencies. However, if that theft was procured by a person hacking another's computer or accounts, prosecution as a crime involving computers may also apply. These include accessing a computer system for dishonest purposes and accessing a computer system without authorisation. This could cover the recent trend of viruses that hijack a target computer's processing power for the purposes of mining virtual currencies. As with other parts of New Zealand law, this crime is not concerned specifically with virtual currencies, but is drafted broadly enough that the kind of activity above would be covered.

The New Zealand police have authority to investigate alleged crimes and to prosecute individuals charged with an offence under the Crimes Act in a court (with Crown solicitors as required). The New Zealand courts may impose fines, prison sentences and other penalties prescribed in the Crimes Act where an offender is found guilty (maximum penalties are prescribed by the Crimes Act).

As far as civil law is concerned, the same legal analysis is likely to apply whether cash or virtual currencies are obtained by fraudulent means. The difference is more likely to be practical, and in particular the practical difficulties of identifying, or enforcing a judgment against, the defendant.

In these circumstances, an innocent party may wish to consider remedies against third parties (who may be more readily identifiable). For example, if a third party comes into possession of fraudulently obtained virtual currency, and was not a purchaser for value, then a claim of knowing receipt, a proprietary restitutionary claim or a claim for unjust enrichment may be available. However, if the third party was a bona fide purchaser for value, then these remedies will likely not be available.

IX TAX

New Zealand has no specific tax regime for virtual currencies. Instead, the taxation of virtual currencies is governed by the existing legal framework. It is necessary to consider both the Income Tax Act 2007 and the Goods and Services Tax Act 1985 (the GST Act).

i Income tax

Broadly, a person may become subject to income tax on amounts derived from virtual currencies in circumstances where the amount is derived from:

a a business of the person and is not a capital receipt;

b carrying on or carrying out an undertaking or scheme entered into or devised for the purpose of making a profit; or

c disposing of personal property of the person if the property was acquired with the purpose of disposing of it.

The Inland Revenue Department (IRD) has issued limited guidance on the tax treatment of virtual currencies, in which it states that virtual currencies should be treated as personal property (not currency) for income tax purposes. The IRD has also engaged in public consultation on certain other discrete tax issues arising from the use of virtual currency, however no detailed guidance has yet been published.

In relation to provisions that refer to a person's purpose, it is the person's subjective dominant purpose at the time of acquiring the property that is relevant. Therefore, if at the time of acquiring virtual currency a person does so with the purpose of later disposing of it, any amounts derived from the disposal (e.g., for a sale or exchange) will be treated as income (and therefore be subject to income tax). The IRD's guidance suggests virtual currencies will generally be acquired with the purpose to sell or exchange because (in general) virtual currencies do not produce an income stream or any benefits, except when sold or exchanged. However, each amount derived from virtual currencies should be considered separately to determine whether the virtual currency was acquired for the purpose of disposal and whether the amounts derived from the disposal are income to which income tax will apply.

New Zealand has a regime known as the 'financial arrangements rules'. These rules require a party to a 'financial arrangement' to spread income and expenditure over the term of the financial arrangement for tax purposes. The financial arrangements rules disregard the traditional distinction between capital and revenue, and instead have regard to all consideration paid or received under the financial arrangement.

Broadly, a financial arrangement is an arrangement under which a person receives money in consideration for that person, or another person, providing money to any person (1) at a future time or (2) on the occurrence or non-occurrence of a future event.

A virtual currency or a transaction involving virtual currency may be subject to the financial arrangements rules if the definition of financial arrangement is satisfied.

ii Goods and services tax

Goods and services tax (GST) is imposed under the GST Act, and is charged on supplies in New Zealand of goods and services by a registered person in the course or furtherance of a taxable activity.

A person makes supplies in the course or furtherance of a taxable activity if the supplies are in the course of an activity (whether or not for pecuniary profit) carried on continuously

or regularly by the person involving the supply of goods and services for consideration. The term 'taxable activity' includes any activities of business or trade, and therefore it may be relevant to determine whether the supplier is a person carrying on business for income tax purposes.

For the purposes of GST, virtual currencies are best classified as choses in action, which are included in the definition of services. The sale of virtual currencies would therefore be a supply of services and subject to GST if the supply is made in New Zealand by a registered person, and in the course or furtherance of a taxable activity carried on by that person.

As virtual currencies are arguably services, not money, for the purposes of the GST Act, any transaction involving the exchange of virtual currency for goods or services will be treated as a barter transaction. Under the GST Act, this involves two separate supplies: the supply of virtual currency from person A to person B; and the supply of goods or services from person B to person A.

Therefore, GST could be chargeable in respect of the supply of goods and services (for which the payment in virtual currency is consideration) as well as the supply of the virtual currency. Given that the virtual currency is functionally a means of payment, this would seem to be the wrong outcome in policy terms. In 2017, Australia amended its GST legislation to address this issue; New Zealand is yet to announce whether it will follow suit.

Supplies made in New Zealand

In general, goods and services are deemed to be supplied in New Zealand if the supplier is resident in New Zealand, and are deemed to be supplied outside New Zealand if the supplier is a non-resident.

However the supply of a virtual currency may in many circumstances meet the definition of a remote service for the purposes of the GST Act. A remote service is defined as a service that, at the time of the performance of the service, has no necessary connection between the place where the service is physically performed and the location of the recipient of the services.

Where the services (the virtual currency) being supplied are remote services, the recipient of the services is a person resident in New Zealand, and the recipient of the service is not registered for GST, or is registered for GST but does not acquire the virtual currency for the purposes of carrying on his or her taxable activity, then a supply made by a non-resident is treated as being made in New Zealand unless the services are physically performed in New Zealand by a person who is in New Zealand at the time that the services are performed. In the context of virtual currencies, it is difficult to determine how the service could be physically performed, and therefore this exclusion is unlikely to apply. If the non-resident is, or is required to be, GST-registered (see below), non-residents will be required to account for GST on such supplies.

A non-resident person making supplies of remote services must treat the recipient of the supply as a person resident in New Zealand if any two items of a specified list of indicia are non-contradictory and support the conclusion that the person is resident in New Zealand. However, in cases where the non-resident also has certain evidence that the person is resident in a country other than New Zealand, the supplier must use the more reliable evidence to determine the person's residence.

Supplies made by a registered person

GST is only chargeable in respect of supplies made by a registered person. Broadly, a person is liable to be registered for GST if the total value of supplies made in New Zealand exceeds, or is expected to exceed, NZ$60,000 in a 12-month period. The registered person definition includes a person who is required to register for GST. Therefore, failure to register for GST does not exempt a person from compliance with obligations imposed under the GST Act. Persons selling virtual currencies exceeding NZ$60,000 in a 12-month period may therefore be liable to be registered.

If a non-resident who makes supplies of remote services determines that the recipient of the supply is a New Zealand resident (as described above), the supplier must treat the recipient as not being a registered person unless the recipient notifies the supplier that he or she is a registered person, or provides his or her registration number or New Zealand business number.

X LOOKING AHEAD

Public and regulator interest in virtual currencies continues to grow in New Zealand and globally. The FMA is the key regulator in New Zealand in respect of virtual currencies, and its position in respect of developments in this area has been clearly stated in the Guidance.

One of the purposes of the FMCA is to promote innovation and flexibility in the financial markets, and the FMA has stressed that its job is not to stop innovative businesses from succeeding. However, promoting innovation does not mean that the FMA will allow risks of new technology and products to be passed on to retail investors in a manner that investors do not understand. Accordingly, the FMA's position is that open and early communication is vital for persons seeking to launch blockchain-related products and technology in New Zealand.

i Territorial scope of the FSP Act

In April 2019, Parliament enacted the Financial Services Legislation Amendment Act 2019 (FSLAA), which will, inter alia, impose more stringent requirements for entities wanting to register on the FSPR. Entities will only be able to register if they are in the business of providing financial services to persons in New Zealand or otherwise required to be licensed or registered under any other New Zealand legislation.

These amendments are intended to prevent abuse of the FSPR by entities using registration on the FSPR to imply that they are subject to licensing or other regulatory obligations in New Zealand (which is often not the case). The provisions of the FSLAA affecting the scope of the FSP Act will come into force on the earlier of 1 May 2021 or a date appointed by the Governor-General.

ii Cryptopia

In January 2019, Cryptopia (a cryptocurrency exchange based in New Zealand) suffered a major security breach, with more than NZ$20 million of cryptocurrency reportedly stolen. At its height, Cryptopia had peak daily trading volumes greater than the New Zealand Stock Exchange.

Cryptopia was subsequently placed into liquidation on 14 May 2019. The liquidators have noted that significant direction will be required from the courts because of the lack of legal precedent on the treatment of crypto assets in a liquidation. The liquidators have also sought recognition of the New Zealand liquidation proceedings in the United States, and have filed a petition in a New York Bankruptcy Court to preserve information stored on servers in the United States.

Cryptopia has been working with the New Zealand police and digital forensic investigators from New Zealand and overseas to establish who is responsible for the security breach. While the identity of the hacker has yet to be established, the security breach is a timely reminder for cryptocurrency exchanges and other entities handling customers' money of the importance of having robust security arrangements in place.

Chapter 20

NORWAY

Klaus Henrik Wiese-Hansen and Vegard André Fiskerstrand[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

Virtual currencies are generally not considered to be legal currencies in Norway, as they fall outside the usual definition of money or currency. Moreover, there is no specific virtual currency legislation in Norway with respect to securities and investment laws, banking and money transmission, or the regulation of exchanges, miners, issuers or sponsors. Hence, businesses or persons operating or conducting virtual currency activities are not required to be licensed under the applicable financial services legislation.

On 15 October 2018, Norway implemented a new Anti-Money Laundering Act and a related regulation that expanded the scope of the legislation to apply for providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet providers (CWPs). Based on the ruling in a recent case (see Section IV.iii), banks may have justifiable grounds for refusing to perform payment services (by opening bank accounts, etc.) due to virtual currencies' high risk of being used for money laundering. However, this decision has been appealed and the Court of Appeal's ruling is expected before the end of 2019.

For tax purposes, virtual currencies are considered as assets and are therefore subject to capital gains tax and net wealth tax.

The Norwegian Parliament has resolved that electrical power used for mining of virtual currency should have a normal tax rate instead of a reduced tax rate. The Ministry of Finance will await clarification from the EFTA Surveillance Authority prior to implementation of the change because a reduced tax rate for data centres constitutes governmental assistance pursuant to Article 61(1) of the Act of 27 November 1992 No. 109 relating to implementation in Norwegian law of the main agreement on the European Economic Area (the EEA Act). See Section IX.v.

II SECURITIES AND INVESTMENT LAWS

i Overview

There are no specific securities and investment laws in Norway with respect to virtual currencies or the offering of such currencies.

On 20 November 2017, the Financial Supervisory Authority of Norway warned investors and firms about initial coin offerings (ICOs) because of the high risks of investment

1 Klaus Henrik Wiese-Hansen is a partner and Vegard André Fiskerstrand is an associate at Schjødt.

losses, fraud and money laundering.[2] Depending on its structure, an ICO may fall outside of the scope of applicable laws and regulations, in which case investors cannot benefit from the protection that these laws and regulations provide. Firms involved in ICOs should, according to the Financial Supervisory Authority, give careful consideration as to whether their activities constitute regulated activities or not. Moreover, the Financial Supervisory Authority has referred to two statements given by the European Securities and Markets Authority (ESMA) on 13 November 2017 relating to the risk of ICOs for investors[3] and rules applicable to firms involved in ICOs,[4] and has declared that its supervisory activities will be based on ESMA's assessments.

In the statement on the rules applicable to firms involved in ICOs, ESMA alerts firms involved in ICOs of the need to meet the relevant regulatory requirements, including considering whether their activities constitute regulated activities. It is the duty of firms themselves to consider the regulatory framework, seeking the necessary permissions and meeting the applicable requirements. Based on the Financial Supervisory Authority's statement, similar requirements will be applicable for such activities in Norway.

On this basis, the structure of ICOs will determine whether they fall outside the scope of the applicable rules. Where coins or tokens qualify as financial instruments it is, according to ESMA, likely that firms involved in ICOs are conducting regulated investment activities, such as placing, dealing in or advising on financial instruments, or managing or marketing collective investment schemes. They may also be involved in offering transferable securities to the public.

Because of the Agreement on the European Economic Area (EEA), Norway will at the outset have similar requirements as those under the applicable EU legislation. The lack of a full Norwegian EU membership implies, however, that the Norwegian legislation from time to time may differ from EU legislation, typically where Norway has yet to implement EU legislation into Norwegian law.

Below is a high-level summary of the applicable EU legislation that also applies in Norway.

ii Prospectus Regulation

The Prospectus Regulation is a key piece of EU legislation that also may be relevant for ICOs in Norway. It aims to ensure that adequate information is provided to investors from issuers raising money in the Norwegian market. Issuers may thus be required to publish a prospectus, subject to approval by a competent authority, before an offer of transferable securities to the public, or the admission to trading of such securities on a regulated marked situated or operating within an EU or EEA Member State occurs, unless certain exclusions or exemptions apply.

2 Financial Supervisory Authority of Norway (2018), ICOs – warning investors and firms (source: https://www.finanstilsynet.no/markedsadvarsler/2017/initial-coin-offerings-icoer---advarsel-til-investorer-og-foretak/).

3 ESMA (2017), Statement on risk of ICOs for investors (source: https://www.esma.europa.eu/sites/default/files/library/esma50-157-829_ico_statement_investors.pdf).

4 ESMA (2017), Statement on rules applicable to firms involved in ICOs (source: https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf).

The current applicable rules in Norway with respect to prospectus regulations are the Norwegian Securities Trading Act, which as of 21 July 2019 implemented the Prospectus Regulation, as amended.[5]

Virtual currencies generally do not qualify as transferable securities, and the prospectus requirements are generally not applicable for ICOs and similar offerings of virtual currencies.

iii Markets in Financial Instruments Directive

Rules similar to those under the Markets in Financial Instruments Directive (MiFID, as later amended through MiFID II) are implemented into Norwegian laws and regulations.[6] These rules aim to create a single market for investment services and activities, and to ensure a high degree of harmonised protection for investors in financial instruments. As described by ESMA in the statement regarding rules applicable to firms involved in ICOs, an investment firm that provides investment services in relation to financial instruments must comply with the applicable requirements. Where a coin or token qualifies as a financial instrument in the case of an ICO, the process by which the coin or token is created, distributed or traded is assumed likely to involve activities subject to the rules in MiFID II, such as placing, dealing in or advising on financial instruments. Depending on the services provided, organisational requirements, conduct of business rules and transparency requirements may apply. Similar requirements will apply in Norway in such cases.

iv Alternative Investment Fund Managers Directive

Rules similar to those under the Alternative Investment Fund Managers Directive are implemented into Norwegian law and regulations,[7] and set out rules for authorisation, ongoing operation, and the transparency of managers that manage or market alternative investment funds. Virtual currencies normally fall shy of the alternative investment fund managers legislation, but alternative investment funds that invest in virtual currencies can fall within the said legislation, depending on, inter alia, their structure.

III BANKING AND MONEY TRANSMISSION

Virtual currencies fall outside the scope of the usual definitions of money or currency in Norway, and will thus not be considered as a legal currency in Norway.

Virtual currency activities furthermore fall outside the scope of the Norwegian Financial Undertakings Act. Thus, activities related to virtual currencies are in general not considered as activities requiring a banking licence or a licence as a payment services provider.[8]

5 The Securities Trading Act of 29 June 2007 No. 75 implementing Regulation (EU) 2017/1129 and replacing the rules implemented from the Prospectus Directive.

6 The Securities Trading Act of 29 June 2007 No. 75 and regulation of 4 December 2017 No. 1913.

7 The Alternative Investment Fund Managers Act of 20 June 2014 No. 28 and the alternative investment fund managers regulation of 26 June 2016 No. 877.

8 The Norwegian Financial Undertakings Act of 10 April 2015 No. 17.

IV ANTI-MONEY LAUNDERING

i Implementation of a new Anti-Money Laundering Act and a related regulation

On 15 October 2018, a new Anti-Money Laundering Act and a related regulation entered into force in Norway.[9] The new legislation implemented the EU's Fourth Anti-Money Laundering Directive and advanced the implementation of certain provisions set out in Directive (EU) 2018/843 (amending the Fourth Anti-Money Laundering Directive),[10] and replaced the Anti-Money Laundering Act of 2009 (which implemented the EU's Third Anti-Money Laundering Directive).[11]

The new anti-money laundering legislation has, compared to the previous Anti-Money Laundering Act of 2009, expanded the scope to apply for providers engaged in exchange services between virtual currencies and fiat currencies, and wallet CWPs, as such providers now are considered as obliged entities. Activities relating to virtual currencies fell outside the scope Anti-Money Laundering Act of 2009, including activities relating to exchanges, mining and storage services for virtual currencies. Thus, the new legislation requires providers engaged in exchange services between virtual currencies and fiat currencies and CWPs to comply with mandatory anti-money laundering obligations, including conducting customer due diligence measures.

The Financial Supervisory Authority will supervise providers engaged in exchange services between virtual currencies and fiat currencies, and ensure that CWPs comply with the applicable anti-money laundering legislation. Providers conducting such activity in Norway are obliged to register with the Financial Supervisory Authority, including information about their name, organisational structure, registration number and offered service, as well as information about the general manager or person in a similar position, members of the board of directors and any contact persons.

ii Effects on financial services providers

The expanded scope of the anti-money laundering legislation (to include providers engaged in exchange services between virtual currencies and fiat currencies, and wallet CWPs) has had an impact on financial services providers. The legislation (similar to regulations and standards from the Financial Action Task Force and the European Union) does not permit financial services providers to refuse to offer financial services to certain groups or sectors solely based on the inherent risk of money laundering (de-risking). According to the Financial Supervisory Authority, financial services providers must assess the risk of money laundering or terrorist financing on a case-by-case basis and there must be justifiable grounds for refusing to offer financial services.[12] As financial services providers at the outset have a duty to contract, the Financial Supervisory Authority expects the former to permit market players engaged in exchange services and wallet CWPs to establish bank accounts, unless they have justifiable grounds to refuse to perform payment services.

9 The Anti-Money Laundering Act of 23 June 2018 No. 23, the Anti-Money Laundering Regulation of 14 September 2018 No. 1324.

10 Directive 2015/849/EC, Directive (EU) 2018/843.

11 The Anti-Money Laundering Act of 11 June 2009 No. 11, Directive 2005/60/EC.

12 Financial Supervisory Authority (2018), The Anti-Money Laundering Act applicable for virtual currency (source: https://www.finanstilsynet.no/tema/hvitvasking-og-terrorfinansiering/hvitvaskingslovens-anvendelse-for-virtuell-valuta/).

iii Case law

A bank has a general duty to contract, unless it has justifiable grounds to refuse by terminating a customer relationship or to refuse the establishment of a customer relationship. Pursuant to a judgment of 30 April 2018 from the Oslo District Court between a Nordic bank and a Norwegian investor[13] (with a business idea to incorporate a Norwegian virtual currency exchange firm[14]), a bank may refuse to perform payment services (by opening bank accounts) due to virtual currencies' high risk of being used for money laundering.

In this case, the Court ruled, after an overall assessment, that the risk of money laundering and transactions related to criminal offences was clearly elevated by Bitcoin trade, although Bitcoin trading may also be done under legitimate conditions. The Court found it clear that this risk constituted justifiable grounds for the bank to refuse its customer relationship pursuant to the Norwegian Financial Contracts Act. The Court also referred to a bank's duty to terminate customer relationships if they entail risks for transactions in connection with criminal offences pursuant to the Norwegian Anti-Money Laundering Act. As mentioned in Section I, this decision has been appealed and the Court of Appeal's ruling is expected before the end of 2019.

V REGULATION OF EXCHANGES

There is currently no specific regulation on virtual currency exchanges. Thus, operating these exchanges is not subject to financial services regulation and does not require a licence. The aforementioned apply both to decentralised exchanges with peer-to-peer solutions and to centralised exchanges. Unless they also are engaged in exchange services between virtual currencies and fiat currencies, or wallet CWPs, they are not required to register with the Financial Supervisory Authority to comply with any anti-money laundering obligations.

On 12 February 2018, the Financial Supervisory Authority[15] joined the European supervisory authorities (ESMA, the European Banking Authority and the European Insurance and Occupational Pensions Authority)[16] in warning consumers of the high risk related to investing in virtual currencies such as Bitcoin, Ether and Ripple. As virtual currencies are not regulated, are traded on unregulated marketplaces and lack transparency in pricing, the Financial Supervisory Authority considers virtual currencies unsuitable for short and long-term savings for most consumers.

Exchanges for buying and selling virtual currencies exist in Norway.[17] From publicly available information, it is also expected that virtual currency exchanges may be launched in Norway in the near future.

13 *Nordea Bank AB (publ), filial i Norge v. Sunde Bitmynthandel.*

14 Bitmynt AS.

15 Financial Supervisory Authority (2018) warns consumers about virtual currencies (source: https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2018/finanstilsynet-advarer-forbrukere-om-kryptovaluta/).

16 European Banking Authority (2017) warns consumers about virtual currencies (source: https://eba.europa.eu/-/esas-warn-consumers-of-risks-in-buying-virtual-currencies).

17 For example, Coinbase (source: https://www.coinbase.com/places/norway) and Bitnorex (source: http://www.bitnorex.no/).

VI REGULATION OF MINERS

There is no specific regulation of miners of virtual currencies, nor are there any specific licence requirements. General rules for conducting business activities will apply to miners of virtual currencies as well.

VII REGULATION OF ISSUERS AND SPONSORS

There are no specific laws or regulations that apply to issuers or sponsors of virtual currencies in Norway. Issuing or sponsoring a virtual currency is generally considered to be a legal activity, but they do not require any licence pursuant to financial regulation legislation.

VIII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

There are no specific criminal and civil fraud and enforcement rules with respect to virtual currencies in Norway.

A 'pump-and-dump' scheme, that is, talking up the price of an asset before dumping it for a profit at the expense of investors, is an old type of market fraud. Compared to a stock exchange, virtual currency exchanges are unregulated markets, which may mean that pump-and-dump schemes may be carried out with impunity. However, there have not been many examples of these schemes in Norway, which may be due to the relatively low numbers of completed ICOs.

General criminal and civil fraud and enforcement legislation may be applicable to fraudulent ICOs, although no specific rules exist with respect to virtual currency. The same applies for fake wallets, and pyramid or Ponzi schemes.

IX TAX

i Overview

Norwegian tax authorities consider virtual currencies as assets being subject to the general tax rules for wealth and sales taxes, but virtual currency transactions are not subject to value added tax (VAT).[18]

ii Wealth and sales taxes

For private individuals, capital gains from virtual currencies are taxable income and losses are deductible.[19] This applies to both mining and transactions. The current tax rate, which is determined annually, constitutes 22 per cent in 2019.[20]

18 Norwegian Tax Administration, tax and VAT treatment of virtual currencies (source: https://www.skatteetaten.no/en/business-and-organisation/reporting-and-industries/industries-special-regulations/internet/tax-and-vat-on-virtual-currencies/).

19 Cf. Norwegian Tax Act of 26 March 1999 No. 14 §§ 5-1 (2) and 6-2 (1).

20 Norwegian Parliament Tax Resolution of 12 December 2018 No. 1992.

Virtual currencies are considered to be assets of economic value, and are thus included in the calculation basis of net wealth for personal taxpayers, calculated as the total value as at 1 January of the tax assessment year.[21] This applies for all virtual currencies held by Norwegian tax residents, regardless of the location of the assets (i.e., inside or outside Norway).

For corporate taxpayers, taxable income shall include any benefit gained from work, assets or business activities.[22] Relevant conditions to determine whether an activity constitutes a business activity are its duration, extent, profitability, expense and risk.[23] Trading of virtual currencies may be considered a business activity if it is conducted regularly and a significant number of transactions are carried out.[24] Mining may be considered a business activity if it is carried out regularly and has a certain extent.[25]

iii VAT

The Norwegian tax authorities altered their VAT guidelines in 2017 and virtual currency transactions are not subject to VAT as exempt financial services.[26] Previously, the tax authorities assumed that the exchange of virtual currencies was not covered by the VAT exemption for financial services and therefore constituted taxable services.[27] Following a decision of the European Court of Justice on 22 October 2015,[28] which ruled that the corresponding service was exempt from VAT in the European Union, the Norwegian tax authorities reassessed the treatment of VAT, and in 2017 concluded that the services of exchanging Bitcoins were covered by the exemption for financial services.[29]

The Norwegian tax authorities assessed in a guideline in 2018 that mining of virtual currencies falls under the VAT exemption for financial services.[30] However, businesses that only convert data power for others for mining of virtual currency are subject to VAT.

The sale of remotely deliverable services to foreign registered businesses is zero-rated, which means that the services are still VAT-taxable but that the rate of VAT is zero per cent. It is the nature of the service (i.e., whether it can be remotely delivered) that determines whether it falls under the provision. Whether the service actually is associated with a location is not essential. According to an advance ruling from the Norwegian Tax Administration, data centre services are remotely deliverable, even though they may appear to be attached to a specific location in Norway (the data centre).

21 Norwegian Tax Administration, tax and VAT treatment of virtual currencies.

22 Cf. Norwegian Tax Act of 26 March 1999 No. 14 §§ 5-1 (1) and 6-2 (1).

23 Norwegian Tax-ABC (2018) (source: https://www.skatteetaten.no/en/rettskilder/type/handboker/skatte-abc/2018/).

24 Norwegian Tax Administration, tax and VAT treatment of virtual currencies.

25 ibid.

26 Norwegian Ministry of Finance (2017), Bitcoin exempted from VAT (source: https://www.regjeringen.no/no/aktuelt/bitcoin-er-unntatt-fra-merverdiavgift/id2538128/).

27 Norwegian Tax Administration (2013), Bitcoin – tax and VAT (source: https://www.skatteetaten.no/rettskilder/type/uttalelser/prinsipputtalelser/bruk-av-bitcoins--skatte--og-avgiftsmessige-konsekvenser/).

28 Case C-264/14.

29 Norwegian Ministry of Finance (2017), VAT exemption for financial services (source: https://www.regjeringen.no/no/dokumenter/merverdiavgift---unntaket-for-finansielle-tjenester/id2538129/).

30 Norwegian Tax Administration (2017), VAT mining of virtual currency (source: https://www.skatteetaten.no/contentassets/ed1de52af7cc45989a5338780159ad6f/kryptovaluta.pdf).

iv Tax for ICOs

Regarding how to handle tax and VAT for ICOs, the Norwegian tax authorities have expressed in guidelines that these matters must be assessed on a case-by-case basis, including whether the VAT exemption for financial services applies.[31]

v Electrical power tax

An electrical power tax is levied on all electric power suppliers, including for power supplied free of charge, and power distribution companies or generators used for internal purposes. Enterprises that transmit electrical power to consumers or generate electrical power must register as being liable for such tax. The liability to pay the tax arises upon the supply of electrical power to consumers and upon consumption for internal use.

There are two relevant tax rates that are determined annually by Parliament: a normal tax rate and a reduced tax rate. The normal tax rate for 2019 constitutes 0.1583 Norwegian kroner per kWh, while the reduced tax rate constitutes 0.0050 Norwegian kroner per kWh.[32]

A normal tax rate applies, inter alia, to power supplied to households, non-industrial commercial activities and administrative buildings in the industrial manufacturing sector. A reduced tax rate applies, inter alia, to electrical power that is supplied to data centres with an output in excess of 0.5 MW.[33] For a data centre to get a reduced rate, it must have the storage and processing of data or both as its main business activity. The Norwegian Tax Administration assessed in a guideline published on 9 August 2018 that data centres that are mining virtual currencies may benefit from the reduced tax rate.[34]

At the time of writing, there is, however, a political and legal debate in Norway regarding whether it is desirable to continue with a reduced tax rate for data centres that are mining virtual currencies and if it is possible to implement a normal tax rate for these businesses. On 31 October 2018, the Norwegian Tax Administration proposed that mining of virtual currency should have a normal tax rate instead of a reduced tax rate.[35] On this basis, Parliament resolved in the fiscal budget for 2019 that electrical power used for mining of virtual currency in a data centre should have a normal rate instead of a reduced rate and provided the Ministry of Finance with authorisation to the implement the resolution.[36] However, the industry questioned the legality of the amendment, because, as mentioned in Section I, a reduced tax rate for data centres constitute governmental assistance pursuant to Article 61(1) of the EEA Act. Thus, the Norwegian Tax Administration proposed in a consultation paper on

31 Norwegian Tax Administration, tax and VAT treatment of virtual currencies (source: https://www.skatteetaten.no/en/business-and-organisation/reporting-and-industries/industries-special-regulations/internet/tax-and-vat-on-virtual-currencies/).

32 Regulation of 12 December 2017 No. 2190 § 1, cf. special duty act of 19 May 1933 No. 11.

33 Regulation of 11 December 2001 No. 1451 § 3-12-6.

34 Norwegian Tax Administration (2018), Opinion on electrical power tax for data centres and mining of virtual currency (source: https://www.skatteetaten.no/rettskilder/type/uttalelser/prinsipputtalelser/tolkningsuttalelse-elektrisk-kraft-datasentre-kryptovaluta/).

35 Norwegian Tax Administration (2018), Reduced tax rate for data centres – mining of cryptocurrency (source: https://www.regjeringen.no/contentassets/bf295ae5c5984da59a4db62cc7168a84/brev_fra_skatteetaten_kryptovaluta.pdf).

36 Recommendation No. 391 S (2018-2019) Chapter 4.4 pursuant to Parliament Resolution of 5 December 2018 and Recommendation to the Parliament No. 3 S (2018-2019) Chapter 13.6 (source: https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Innstillinger/Stortinget/2018-2019/inns-201819-391s/?m=3).

16 May 2019 to change the scope of receivers of governmental assistance (which is assumed to be in accordance with relevant EU regulation).[37] According to the proposal, it shall apply a normal tax rate if (1) the purpose is mining of virtual currency (subjective element), (2) it is initiated as an activity or process (objective element), which (3) has a purpose to collect a reward (financial element). This change raises legal issues regarding governmental assistance and the Ministry of Finance will therefore wait for clarification from the EFTA Surveillance Authority before implementing the change.

Data centres that have a support function to an enterprise's main business (e.g., financial services) are excluded from the provision of a reduced tax rate.[38] The reduced rate is limited to power used for servers, cooling systems, pumps, lighting, safety devices, aggregates and devices that directly support a server's function.

XI LOOKING AHEAD

i Overview

There are currently no specific licence requirements for virtual currency exchanges, nor are there any specific securities and investment laws, or any specific regulation of miners, issuers and sponsors. The Norwegian financial regulation legislation must therefore be amended for virtual currency activities to fall inside its scope. Such amendments are generally not expected in the near future, but it is expected that Norwegian authorities will cooperate with countries participating in the European blockchain partnership (see subsection ii) if this regulation is implemented into Norwegian law at some point.

ii European blockchain partnership

Twenty-nine European countries, including Norway, have signed a declaration on the establishment of a European blockchain partnership to share experiences of and expertise in technical and regulatory fields, and to prepare for the launch of EU-wide blockchain applications across the digital single market.[39] Based on this partnership and the existing partnership under the EEA Agreement, it is expected that the Norwegian authorities will cooperate with the other participating countries in regulating virtual currencies going forward.

iii Central bank digital currency

On 18 May 2018, the Norwegian Central Bank published a working group paper with an overview of issues that it regards as relevant in an assessment of whether to introduce a central bank digital currency (CBDC) in Norway.[40]

37 Norwegian Tax Administration (2019), Consultation paper on electrical power tax by mining of virtual currency (source: https://www.skatteetaten.no/contentassets/0deaa9754e4846b984bc4caa493f8fb0/horingsnotat.pdf); Article 44 of Commission Regulation (EU) No. 651/2014 and Articles 5 and 17(a) of Directive 2003/96/EC.

38 Norwegian Tax Inspectorate (2018), Tax on electric power tax (source: https://www.skatteetaten.no/globalassets/rettskilder/avgiftsrundskriv/2018-elektrisk-kraft.pdf).

39 European Commission (2018), European countries join blockchain partnerships (source: https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership).

40 Norges Bank Paper No. 1, 2018 (source: https://static.norges-bank.no/contentassets/166efadb3d73419c8c50f9471be26402/nbpapers-1-2018-centralbankdigitalcurrencies.pdf?v=05/18/2018121950&ft=.pdf).

Introducing a CBDC would entail offering a digital liability on the Central Bank for use as a means of payment and a store of value, and would entail the creation of dedicated payment solutions the Central Bank would have full or partial responsibility for, but that it would not necessarily operate and maintain. Any decision of the Central Bank to take the initiative in introducing a CBDC must, according to the working group, be based on a socioeconomic cost–benefit analysis. Important elements in such an analysis will be the impacts on the payment system, financial stability and monetary policy.

In the working group's assessment, there are primarily two relevant models for organising a CBDC system. The first is an account-based model in which both value storage and transaction processing are centralised. In this model, money is held in accounts and moves from one account to another in the system. The working group sees this model as an advantageous back-up solution. The second model is a value-based model in which value storage and processing are decentralised. In this model, money will be stored locally in payment instruments, typically a card or another instrument being issued by a central third party. The working group sees this model as an advantageous, real, risk-free alternative to depositing money to store values. Hybrid variants that combine elements of both the models, such as a model based on distributed ledger technology, may also be a potential third alternative.

Introducing a CBDC may require certain changes in the Central Bank Act. An account-based solution may require amending provisions in the Act, under which entities may hold an account with the Central Bank. A value-based solution probably will not require any amendments as long as the solution is within the customary normal remit of the Central Bank.

The working group has expressed that the project's second phase will be to examine the purposes of a CBDC and the most relevant solutions in greater detail. This will make it possible to elaborate on the impacts of a CBDC and the cost–benefit analysis.

Chapter 21

PORTUGAL

Hélder Frias and Luís Alves Dias[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

In Portugal, there are no specific references to virtual currencies or the players in the virtual currencies market, such as virtual currency exchanges, virtual currency wallets, virtual currency miners and virtual currency issuers (virtual currency operators). This does not mean that virtual currencies or virtual currency operators are by all means unregulated, but rather that whether a specific virtual currency or virtual currency operator falls under the scope of a specific law or regulation is a matter of interpretation. A case-by-case assessment in light of the specific characteristics of the relevant virtual currency or of the relevant virtual currency operator and in light of the existing legal and regulatory framework is required to come to any conclusions.

Given the uncertainty surrounding the exact legal and regulatory framework applicable to virtual currencies and virtual currency operators, the potential financial impact, and the resemblance of virtual currencies or the operations or business models of some virtual currency operators with the legal concepts, functions and business models to those found in specific financial sectors, the Portuguese regulatory and supervisory authorities for the financial sector have been alert to the virtual currencies phenomenon and have issued several press releases highlighting the risks and uncertainties regarding virtual currencies and initial coin offerings (ICOs).

The Bank of Portugal (BoP), which is the Portuguese banking authority, has issued several press releases and warnings concerning virtual currencies. In November 2013, the BoP issued a press release warning against the risks of investing and holding Bitcoin and stating that Bitcoin was not subject to the BoP's supervision. In October 2014, the BoP stated that Bitcoin ATMs are not part of the Portuguese payments system and warned against the risks of investing in and holding virtual currencies. In March 2015, the BoP issued another press release highlighting the risks of investing in and holding virtual currencies and stating that virtual currencies are not legal tender in Portugal. In that same month, through Circular Letter No. 11/2015/DPG, the BoP recommended that Portuguese credit institutions, payment institutions and electronic money institutions refrain from buying, holding or selling virtual currencies, following the opinion of the European Central Bank (ECB) and the European Banking Authority on virtual currencies. In February 2018, the BoP issued a new press release warning against the above-mentioned risks once more.

In November 2017, the Portuguese Securities Market Commission (CMVM), which is the authority responsible for supervising and regulating securities and other financial instruments markets, as well as the activities of all entities that operate in those markets,

1 Hélder Frias is a senior associate and Luís Alves Dias is an associate at Uría Menéndez-Proença de Carvalho. The information in this chapter was accurate as at October 2018.

issued a press release highlighting the risks of investing in and holding virtual currencies. It further stated that virtual currencies are not regulated and are not subject to the CMVM's supervision, following ESMA's opinion on virtual currencies. In July 2018, the CMVM issued another press release providing some guidance on how they will assess the legal nature of virtual currencies (see Section II). In May 2018, the CMVM issued a press release regarding a specific ICO carried out in Portugal (see Section II).

The Portuguese Insurance and Pension Funds Supervisory Authority (ASF), which is responsible for the regulation and supervision of insurance, reinsurance and pension funds markets, has not yet issued a press release on virtual currencies.

Finally, the National Council of Financial Supervisors, comprising the BoP, the CMVM and the ASF, which was created to ensure enhanced coordination and articulation among those regulatory and supervisory authorities, issued a press release in July 2018 highlighting the risks of investing in and holding virtual currencies.

II SECURITIES AND INVESTMENT LAWS

Portuguese securities and investment laws do not specifically refer to virtual currencies. Therefore, whether a certain virtual currency falls under the scope of those laws is a matter of interpretation. In this regard, given the myriad different characteristics that virtual currencies may have, a case-by-case assessment is of the utmost importance.

To understand to what extent securities laws are applicable to a specific virtual currency (with the consequent impact upon the related virtual currency operators), one must answer the following question: do the characteristics of the relevant virtual currency make it a financial instrument regulated by securities laws?

For that purpose, and taking into account the different features that each virtual currency may have, grouping virtual currencies based on a specific number of common characteristics helps to provide a preliminary and generic introduction to this subject. Therefore, based on the approach followed by several regulatory bodies and authors throughout the world, we have adopted a quadripartite taxonomy of virtual currencies for the purpose of this section, as follows:

a cryptocurrencies, which are intended to be used as mediums of exchange, units of account or stores of value, and that, as such, do not give rise to any claim against the issuer or a third party;

b utility tokens, which are intended to provide access to a specific IT infrastructure, product, service or community, and which, as such, may give rise to a corresponding claim against the issuer or a third party (i.e., access to a service, a product, a platform, a community), but which do not translate into any right to future cash flows from the issuer or a third party, and consequently bear a resemblance to a pure consumer of goods, a services relationship, or both;

c security tokens, which represent specific rights against the issuer or a third party that are economically or functionally equivalent to financial instruments specified by law, including the right to receive a future share of the earnings or political rights (shares), renumerated claims (bonds), an amount equivalent to the value of an underlying asset or index (derivatives), etc., thus bearing a resemblance to a pure investment relationship; and

d hybrid tokens, which have a combination of the characteristics of more than one type of virtual currency described above.

The few Portuguese legal academics that have addressed this topic have concluded that security tokens are likely to be deemed atypical securities, and that some hybrid tokens (those that also have the characteristics of security tokens) may also be deemed atypical securities pursuant to Portuguese law. A case-by-case assessment must, however, be carried out to conclude whether a specific virtual currency qualifies as an atypical security.

On 23 July 2018, the CMVM issued a press release regarding ICOs stating that the assessment of the legal nature of the virtual currency to be issued is crucial to understanding which regulatory framework should apply. The CMVM also states that the assessment must be performed on a case-by-case basis, and that some virtual currencies might qualify as securities taking into account the legal concept of atypical securities. While highlighting the changing nature of virtual currencies, and as such leaving room for future changes in the CMVM's opinion, the CMVM clarifies that it will take into account the information made available by the issuer to potential investors and, in particular, any elements evidencing that the issuer may be bound to adopt a specific form of conduct from which the investor may have an expectation to gain a return for the holder on its investment in the virtual currency, such as a right to any type of income (e.g., dividends or interest), or the performance of specific actions by the issuer or related entities aimed at increasing the value of the virtual currency.

In May 2018, the CMVM issued a press release regarding a specific ICO carried out in Portugal in which it states that a token that enables its holders to 'participate in surveys concerning the development of the platform' and 'donate tokens to the [issuer] in order to develop new features' is, in principle, not a security.

The classification of a virtual currency as an atypical security has very important consequences as, for instance:

a the public offerings framework would apply to the ICO (to assess whether an exclusion may apply or, even if that is not the case, whether the issuance of the virtual currency could be exempt from the obligation to publish and file a prospectus);

b specific transparency and fiduciary obligations would apply in the context of the ICO and to the issuer and the members of its corporate bodies;

c some intermediaries providing services to the issuer of such virtual currencies would need to obtain a licence as financial intermediaries (e.g., broker-dealer, custodians);

d exchanges where the virtual currency is listed would need to obtain a licence to trade securities (e.g., regulated markets or multilateral trading facilities); and

e specific restrictions may apply to sales in a secondary market, etc.

III BANKING AND MONEY TRANSMISSION

Portuguese banking, payments and money transfer laws do not specifically refer to virtual currencies. Therefore, whether a specific virtual currency falls under the scope of those laws is a matter of interpretation. In this regard, as previously mentioned, given the myriad different characteristics that virtual currencies may have, a case-by-case assessment is of the utmost importance.

Under Portuguese law there is no legal definition of money. Nonetheless, from an economic standpoint, money is usually said to play three roles in our society: as a medium of exchange (to enable the efficient execution of transactions), as a unit of account (to enable the measurement of the value and costs of goods and services), and as a store of value (to enable the transfer of value over time). From the perspectives of the ECB (in a report from February 2015) and the International Monetary Fund (in a report from January 2016), virtual

currencies do not currently fulfil these three economic roles and, as such, even though some virtual currencies may aim to fulfil some or all three of the economic roles of money referred to above, they cannot be deemed as money at this stage. Furthermore, the BoP clarified that virtual currencies are not legal tender in Portugal in a press release from March 2015 (i.e., it is not compulsory to accept them as a means of payment in transactions). Nonetheless, virtual currencies are considered as an alternative means of payment the same as any other asset (tangible or intangible) that may be legally used as a mean of payment if the parties to a transaction so agree. This is line with the decision of the European Court of Justice that considered Bitcoin a contractual means of payment.[2] However, both the ECB and the BoP stated that virtual currencies are not regulated or supervised by them.

In very specific (and perhaps unlikely – notwithstanding the trend of the stablecoins) cases, depending on the characteristics of a virtual currency, there is a risk of e-money laws being considered applicable. Under Portuguese law, electronic money means electronically (including magnetically) stored monetary value as represented by a claim on the issuer that is issued on receipt of funds (banknotes, coins or scriptural money) for the purpose of making payment transactions, and that is accepted by a natural or legal person other than the electronic money issuer. In principle, virtual currencies would fall outside the scope of this definition as, *inter alia*, they are not a digital representation of the value of any fiat currency, e-money is redeemable at par value with the fiat currency it represents, and e-money is issued by a specific entity with legal personality (which may not always be the case with virtual currencies). Nevertheless, if a virtual currency is issued by a specific entity with legal personality at par value with a specified fiat currency and its value is indexed to the value of that fiat currency, then it may be deemed a form of electronic money if the virtual currency is accepted as a means of payment (i.e., to pay for products or services) by a natural or legal person other than the electronic money issuer. In this case, e-money laws may be applicable and the issuer of that virtual currency may have to obtain an e-money licence, and specific intermediaries may have to be registered with the BoP as e-money agents or intermediaries.

As we describe in further detail in Sections V and VII, exchanges and issuers may be subject to particular banking laws depending on their specific model of operation or the type of funds received in return for the virtual currencies issued, respectively.

IV ANTI-MONEY LAUNDERING

In its report on virtual currencies from June 2014, the Financial Action Task Force (FAFT) concluded that '[t]he legitimate use of virtual currencies offers many benefits such as increased payment efficiency and lower transaction costs. Virtual currencies facilitate international payments and have the potential to provide payment services to populations that do not have access or limited access to regular banking services.' Nonetheless, the FAFT has also highlighted that:

> *other characteristics of virtual currencies, coupled with their global reach, present potential AML/CFT risks, such as: the anonymity provided by the trade in virtual currencies on the internet; the limited identification and verification of participants; the lack of clarity regarding the responsibility for AML/CFT compliance, supervision and enforcement for these transactions that are segmented across several countries; the lack of a central oversight body.*

2 Judgment of the European Court of Justice in case C-264/14, of 22 October 2015.

Virtual currencies or virtual currency operators are not yet specifically referred to in the anti-money laundering and counter-terrorist financing (AML/CFT) framework in force in Portugal. Nonetheless, taking into account the aspects referred to in Sections II, III, V and VI, depending on the characteristics of each case, some virtual currency operators may be subject to the AML/CFT framework currently in force in Portugal.

In general terms, the Portuguese legal framework on AML and CTF is composed of a vast number of pieces of legislation, but it is identical in broad terms to the legal framework in force in other EU Member States given that, to a large extent, it reflects the implementation of EU directives on the subject (notably Directive (EU) 2015/849). Sectoral authorities (such as the BoP and the CMVM) may provide for implementing rules specifically applicable to entities operating in the relevant sector. For instance, Law No. 83/2017, of 18 August (Law 83/2017), provides for the general AML/CFT framework in Portugal, but the BoP has established specific rules that supplement Law 83/2017 and that specifically apply to credit institutions and investment firms (Regulation No. 5/2013, of 18 December, which is currently under review by the BoP).

Money laundering and the financing of terrorism are crimes under the Portuguese Criminal Code and punishable with imprisonment. Both natural and legal persons can be criminally prosecuted for these crimes.

Failing to put adequate procedures and systems in place to prevent money laundering and financing of terrorism and to notify those practices to the authorities may also give rise to administrative offences punishable with a fine of up to €5 million (which may be aggravated, and ancillary sanctions may be applied cumulatively).

General investigatory powers are recognised for police departments, judicial authorities, investigating magistrates and the Public Prosecutor's Office. Furthermore, specific investigatory powers are awarded by Law 83/2017 to the competent authorities responsible for the investigation of money laundering activities and practices, including the Central Bureau of Investigation and Prosecution (CBIP) and the Financial Intelligence Unit (FIU). Further to the investigatory powers set forth in Law 36/94, upon receiving a reasoned order, the CBIP may directly access all financial, tax, administrative, judicial and police information necessary for the fulfilment of its mission regarding AML/CTF. Moreover, both the CIBP and the FIU may request information from any person that they deem to be relevant for the pursuit of their functions and, if necessary, these authorities may summon and question any person for this purpose.

The recently enacted fifth AML Directive[3] addresses specific risks associated with virtual currencies, aiming at bringing more transparency to the virtual currencies sector across the EU. Member States must implement this Directive by 10 January 2020. Portugal has not yet implemented it.

This new Directive provides the first definition of virtual currencies in EU legislation: 'a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically'. Furthermore, 'providers engaged in exchange services between virtual currencies and fiat currencies' and custodian wallet providers (these are defined as 'an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual

3 Directive (EU) 2018/843, of the European Parliament and of the Council, of 30 May 2018.

currencies') come under the scope of the EU AML/CFT framework (notably Directive 2015/849), which means that, among other things, some virtual currency exchanges and custodian wallet providers will have to perform know your customer (KYC) and know your transaction (KYT) analyses regarding their clients (the users of those virtual currency exchanges and wallets) and their respective transactions, and also report suspicious activities.

However, it is worth noting that the fifth AML Directive is only applicable to some virtual currency exchanges: those that accept fiat currency in exchange for virtual currencies and vice versa. Those exchanges that only accept virtual currencies in exchange for virtual currencies fall outside of the scope of this new Directive.

Finally, it is worth noting that those subject to the Portuguese framework on AML/CFT must pay special attention to the AML/CFT risks that may derive from offering products or transactions likely to favour anonymity; developing new products and new commercial practices, including new distribution mechanisms and new payment methods; and using new technologies, or technologies under development, for new products and for existing products. Besides stricter risk management requirements being applicable, there are additional KYC and KYT requirements to be complied with in transactions involving any of these three products or technologies.

V REGULATION OF EXCHANGES

Unlike other jurisdictions (e.g., Japan, the State of New York, Malta), Portugal does not have a specific legal framework applicable to virtual currency exchanges. Therefore, whether a certain virtual currency exchange falls under the scope of any existing legal or regulatory framework is a matter of interpretation. In this regard, given the different business models that virtual currency exchanges may have, a case-by-case assessment is of the utmost importance.

To understand to what extent securities laws and payment services laws are applicable to exchanges, one must consider the following four questions:

a does the virtual currency exchange provide any type of intermediation service (placement, investment advisory, etc.)?;

b does the virtual currency exchange accept fiat currency in exchange for virtual currencies, and vice-versa?;

c are there any virtual currencies listed or to be listed in the virtual currency exchange that classify as securities or e-money?; and

d does the virtual currency exchange offer any type of financial remuneration in connection with the balances that investors hold in such exchange, or does it undertake any obligation to repay the fiat funds deposited?

In basic terms, if the answer is yes to:

i question (a), then there is the risk of the legal and regulatory framework applicable to financial intermediaries being applicable, in particular if the answer to the first part of question (c) is also yes;

ii question (b), then there is the risk of the legal and regulatory framework applicable to payment institutions or e-money institutions being deemed applicable, as the virtual currency exchange may be deemed to be receiving fiat funds from investors to perform payment transactions;

iii question (c), then there is the risk of the legal and regulatory framework applicable to regulated markets or multilateral trading facilities being deemed applicable, if securities, or the legal and regulatory framework applicable to e-money agents or intermediaries; and

iv question (d), then there is the risk of the legal and regulatory framework applicable to credit institutions being deemed applicable, in particular if the answer to question (b) is also yes, as the virtual currency exchange may be deemed to be receiving fiat funds and remunerating them as if they were a deposit, or have some sort of obligation to return such funds, if e-money.

Finally, AML and data protection laws may apply to virtual currency exchanges. Regarding AML, refer to Section IV. Regarding data protection, whenever a virtual currency exchange collects personal information concerning individuals, such virtual currency exchange must comply with the General Data Protection Regulation and all associated legislation.

VI REGULATION OF MINERS

Unlike other jurisdictions (e.g., Belarus, Venezuela, Ukraine), Portugal does not have a specific legal framework applicable to virtual currencies miners. Therefore, whether miners fall within the scope of any existing legal or regulatory framework is a matter of interpretation.

Depending on the specific characteristics of the relevant distributed ledger technology (DLT) in which miners operate (notably regarding consensus protocols) and depending on their specific role, degree and frequency of intervention within such DLT, miners may be deemed service providers (i.e., of transaction processing and validation services) and, as such, will have to comply with the general terms of the law and register with the tax authorities. However, a case-by-case assessment is of the utmost importance.

VII REGULATION OF ISSUERS AND SPONSORS

As further detailed in Section II, classification of a virtual currency as an atypical security entails the application of certain aspects of securities laws to the issuers, the members of its corporate bodies and sponsors in the context of ICOs.

Furthermore, and as further described in Section III, in very specific (and perhaps unlikely – notwithstanding the trend of stablecoins) cases, there is a risk of a virtual currency being deemed a form of electronic money and, as such, this would entail the application of e-money laws. In such cases, the issuer of the virtual currency would have to obtain an e-money licence.

Additionally, if the issuer of the virtual currency accepts funds in the form of fiat currency in return for the virtual currency being issued in the ICO, and if any obligation for the issuer to repay the investors results from the documents and information conveyed by the issuer in connection with the ICO, there is a risk of such activity being considered as the acceptance of deposits from the public, which is an activity that may only be carried out by credit institutions under Portuguese law.

If the issuer of the virtual currency accepts funds in the form of fiat currency in return for the virtual currency being issued in the ICO, but there is no obligation for the issuer to

repay the investors, the risk of it being considered that those funds have been received to perform payment transactions should also be taken into account, in which case a payment services licence would be required.

VIII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

The crime of fraud is set out in Article 217 of the PCC, which states the following:

> *He who, with the intention of obtaining an illegitimate enrichment, for himself or for a third party, by means of error or deceit about facts which he has maliciously provoked, induces someone to acts which cause to him, or cause to another person, damage to his property, shall be punished with imprisonment of up to three years and a fine.*

As per Article 218 of the PCC, the crime of qualified fraud applies to instances where the injury is significantly high.

Criminal fraud, and civil error or civil fraud, must not be confused. Whereas the first may lead to penal liability, the second can only lead to annulment (provided that the applicable requirements are met) or compensation for damages (or both).

In Portugal, the state is the uncontested leader in dispute resolution. In fact, the majority of conflicts are resolved through the legal system, supported by a large network of courts with specific and complex procedural rules.. Nevertheless, with the lack of efficiency of the public system, the importance of arbitration and other dispute resolution methods is increasing significantly.

Law enforcement is the responsibility of police departments, judicial authorities, investigating magistrates, the bureau of investigation and prosecution and the Public Prosecutor's Office. In this regard, the geographical competence of the public prosecutors is determined in accordance with the place where the offence is committed.

A civil claim aimed at obtaining compensation for damages will meet the requirements of civil liability. Hence, compensation may only be claimed upon the verification of damages caused (i.e., with a causal link) by an unlawful act or omission committed with some level of culpability (there are limited exceptions). As compensation corresponds to the degree of damage caused, there is no monetary threshold for such claims.

Pursuant to the Portuguese Civil Code, the right to compensation in the context of non-contractual civil liability has a limitation period of three years as from the date on which the person who suffered the damages became aware of their right to compensation.

As a general rule, claimants must produce evidence of the damage as well as of any facts of the claim that are favourable to their case.

Within the EU, Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters sets out the conditions under which a judgment (concerning civil and commercial matters) issued in a Member State can be enforceable in another. Therefore, pursuant to this Regulation, a judgment issued in a Member State and enforceable in that Member State may be enforceable in Portugal when, upon application by the interested party, it has been declared enforceable. The application of enforceability is filed in the competent court.

IX TAX

Regarding tax matters, there have been some significant developments in the personal income tax (PIT) and value added tax (VAT) treatment of virtual currencies, as described below. In relation to corporate income tax (CIT), since the taxable base is calculated by reference to a taxpayer's profit and loss account drawn up in accordance with the rules set out in the Portuguese General Accounting Rules (GAAP), as adjusted pursuant to the CIT Code, there are main uncertainties related to the accounting treatment of virtual currencies, as there are no specific guidelines in this regard.

From a CIT perspective, income obtained by Portuguese tax-resident entities or by Portuguese permanent establishments of non-resident entities from the sale or exchange of virtual currencies should be subject to CIT. The standard CIT rate is currently of 21 per cent, which may be increased by a municipal surcharge of up to 1.5 per cent (levied on taxable income before the deduction of any carry forward losses). Additionally, taxable income in excess of €1.5 million is subject to a state surcharge, also levied before the deduction of any carry-forward losses. In this respect, taxable income in excess of €1.5 million and up to €7.5 million is subject to a 3 per cent tax rate, taxable income in excess of €7.5 million and up to €35 million is subject to a 5 per cent tax rate, and the excess over €35 million is subject to a 9 per cent tax rate.

From a PIT perspective, income obtained by Portuguese tax-resident individuals from the sale or exchange of virtual currencies is currently not subject to PIT whenever the individuals are acting outside the scope of a business or professional activity. This understanding has already been confirmed by the Portuguese tax authorities through Ruling No. 5717/17 of 27 December 2016. Should a Portuguese tax-resident individual obtain this income within the scope of a business or professional activity (which is deemed to be the case when the sale or exchange of virtual currencies by the individual takes place with regularity), the relevant income should be subject to PIT. In that case, the Portuguese tax-resident individual will be subject to taxation at progressive tax rates ranging between 14.5 and 48 per cent, plus an additional solidarity surcharge of 2.5 per cent due on taxable income between €80,000 and €250,000, and of 5 per cent due on taxable income exceeding €250,000.

From a VAT perspective, transactions to exchange traditional currencies for virtual currencies are deemed to be a supply of services for VAT purposes. Nevertheless, both the VAT Directive and the Portuguese VAT Code provide for a VAT exemption for transactions related to 'currency, bank notes and coins used as legal tender, which, strictly from a tax perspective, should also apply to transactions of virtual currencies. This understanding has already been confirmed by the Portuguese tax authorities through Ruling No. 12904 of 15 February 2018 that held – in line with the judgment of the European Court of Justice in case C-264/14 of 22 October 2015 – that virtual currencies are means of payment that are accepted for that purpose by certain operators and therefore should be exempt from VAT in the same conditions as traditional currencies.

X OTHER ISSUES

Even if no specific legal or regulatory framework is applicable, issuers of virtual currencies will have to comply with the general terms of law (e.g., the principle of good faith) and consumer protection legislation (e.g., the Distance marketing of consumer services Law,[4] the Unfair terms Law,[5] the E-commerce Law,[6] etc.) when offering, marketing and promoting a certain virtual currency to potential investors. In any case, as highlighted in previous sections, this will always depend on the specific characteristics of the relevant virtual currency.

XI LOOKING AHEAD

The government and the Portuguese sector regulatory authorities for the financial sector have shown a great deal of interest in virtual currencies, and have been dedicating their efforts and setting up specialised task forces to understand the risks and opportunities brought about by innovation and the latest technological breakthroughs when applied to, *inter alia*, products, services, processes and business models within the financial sector.

Portugal is witnessing more and more initiatives regarding virtual currencies and ICOs, with new businesses (specialised consultancy firms, specialised training firms, etc.), events (some sponsored by the regulatory authorities themselves) and non-profit organisations (e.g., the Portuguese Association of Blockchain and Cryptocurrencies) emerging in the market. Since 2017, several Portuguese projects have launched ICOs, even though the great majority of them did so in other jurisdictions (e.g., Singapore, Switzerland and Estonia).

As illustrated above, the CMVM and the BoP have been monitoring virtual currencies and ICOs with particular attention. As the Portuguese market matures, we believe that the CMVM and the BoP will take steps to provide further clarity on these subjects, thus mitigating consumer risks and preventing illicit activities without hindering innovation. To this end, cooperation and interaction with virtual currency operators is essential.

4 Decree-Law No. 24/2014.

5 Decree-Law No. 446/85.

6 Decree-Law No. 7/2004.

Chapter 22

RUSSIA

Maxim Pervunin and Tatiana Sangadzhieva[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

Although most activity related to cryptocurrency is provided for in some way by Russian legislation, the draft Law on Digital Financial Assets, which will specifically regulate actions related to cryptocurrency in Russia, is at its third reading and has not yet been passed. Its enactment, which is expected in 2019, has been further slowed by the need for the legislation to comply with Financial Action Task Force (FATF) recommendations. It is expected that any activities not expressly authorised in the law will be unlawful and subject to penalties.

It is also expected that Russian citizens will be prohibited from owning Bitcoin unless it is purchased at foreign exchange and sale points, under foreign law. Trading Bitcoin in Russia will not be permitted. In its current form, the draft law contains no statutory definitions of 'token', 'cryptocurrency' and other terms that featured in previous versions.

II BANKING AND MONEY TRANSMISSION

Russia's Central Bank is opposed to the introduction of cryptocurrency in the country.[2] However, it is contemplating introducing a state cryptocurrency.

Prompt legislative action was prevented by a poor understanding of the very essence of blockchain tools. The policy of the Central Bank is ambiguous and in some places even contradictory. At first, the Central Bank opposed 'money substitutes' and was against introducing digital coins into the monetary system; however, it has since acknowledged the possibility of launching an official cryptocurrency. Business interest in virtual money is explained by the fact that using it helps to reduce transaction costs. The Central Bank intends to study a proposal to create a cryptocurrency linked to the price of gold, which could be used for mutual settlements with other countries.

The Central Bank will regulate all operations related to cryptocurrencies. In March 2019, it sent a draft instruction to the State Duma for discussion in which it proposes to limit the annual amount of cryptocurrency assets available for purchase to unqualified investors.

It is assumed that transactions will be limited to:

a the amount of money transferred as payment;

b the total value of digital assets that are exchanged; and

1 Maxim Pervunin is the managing partner and Tatiana Sangadzhieva is a lawyer at TFH Russia LLC.

2 https://fomag.ru/news/pochemu-nabiullina-protiv-kriptovalyuty-v-denezhnoy-sisteme-a-takzhe-kurs-bitkoina-efiriuma-i-ripple/.

c the cost of digital operational characters transferred in exchange, including cryptocurrencies (this is only about cryptocurrencies that can be issued in Russia within the framework of a future law).

When exchanging digital assets, the transaction amount will be calculated on the basis of their nominal value.

The specific threshold of the Central Bank will be determined separately, but it will probably correspond to the maximum annual amount determined for unqualified investors by the Crowdfunding Bill (600,000 roubles).

Professional securities market participants will not act as intermediaries, but exchange operators (banks, stock exchanges and depositories) will have to track all transactions with the Central Federal Depositary and keep records of their total value.

Banks have begun to pay close attention to income derived from cryptocurrency activities. In May 2019, Sberbank requested this information from one of its clients. The bank sent a letter in which it asked its client to confirm the sources of income from cryptocurrencies and send the address of the cryptographic wallet, the user name, the documents for mining equipment and payment for electricity, an extract from the history of operations of the user of the crypto exchange, and income statements for 2018. It transpired that the recipient of the letter had transferred money received from the exchange of cryptocurrencies to his account at Sberbank and told the bank about it. Representatives of Sberbank confirmed the authenticity of the letter. They clarified that they operate within the framework of the law on combating money laundering and terrorist financing.

III ANTI-MONEY LAUNDERING

FATF measures have been introduced recommending cryptocurrency service providers to follow the same money laundering and terrorist financing procedures that traditional financial services firms are required to. The first FATF check will be carried out in June 2020.

The State Duma has prepared proposals for the regulation of cryptocurrencies, drawn up in accordance with the FATF requirements. The problem is not the cryptocurrencies themselves, but the unlawful purposes for which they are used because digital money is unregulatedreak.

Meanwhile, the Supreme Court[3] introduced the concept of cryptocurrency to the 2015 ruling on money laundering in connection with the FATF recommendations. It clarified that Articles of the Criminal Code[4] on the legalisation of criminal proceeds should be extended to cryptocurrency. The subject of crimes may include 'funds converted from virtual assets (cryptocurrency) acquired as a result of the commission of a crime'.[5]

3 The Supreme Court of the Russian Federation is the supreme judicial body in civil, criminal and administrative cases, in cases regarding the resolution of economic disputes and other cases falling under the jurisdiction of courts, established in accordance with Federal Constitutional Law on the Judicial System.

4 The Criminal Code of the Russian Federation is the main source of criminal law in Russia. New laws providing for criminal liability are subject to inclusion in this Code.

5 https://www.google.ru/amp/s/rg.ru/amp/2019/03/06/verhovnyj-sud-opredelil-nakazanie-za-otmyvanie-deneg-cherez-kriptovaliutu.html.

The Federal Financial Monitoring Service (Rosfinmonitoring)[6] reported that the absence of legislative regulation and state supervision over the issue and circulation of virtual currencies is considered to be among the main vulnerabilities of the Russian economy. In recent years, it has been noted that cryptocurrency has been used for the sale of narcotic drugs and the subsequent laundering of criminal proceeds. According to Rosfinmonitoring (in connection with the commission of crimes), despite the uncertainty of their legal status in Russia, cryptocurrencies are equal to property (in accordance with the purposes of their use) and are identified in monetary terms.

If money laundering occurs through the use of cryptocurrency, then these actions will be covered by Article 174.1 of the Criminal Code. Moreover, law enforcement agencies are already applying this Article in cases where cryptocurrency has been used to launder criminal proceeds.

Digital money is more likely to be used for the unauthorised transfer of funds abroad and to individuals who are engaged in business that is wholly or partly illegal. For these people, in the short term, there are opportunities for cash conversion of cryptocurrency or the use of international exchanges and the shadow internet.

Cryptocurrencies are a relatively unattractive prospect for investment because they do not perform any of the functions of money and are characterised by volatility (according to Rosfinmonitoring's calculations, Bitcoin volatility is 92 per cent). Digital currency cannot maintain its value over time, does not have collateral in the form of a real asset and does not have a guarantee of its relevance and value in the future.

IV REGULATION OF EXCHANGES

The activities of cryptocurrency exchanges that exchange Bitcoin and other popular cryptocurrencies are currently not regulated, except for categorical prohibitions by regulators. Recently, cryptocurrencies have become widespread all over the world and are used for a variety of purposes, from accumulating money and settlements to initial coin offerings (ICOs).

Financial market regulators (the Central Bank and Rosfinmonitoring) repeatedly warned citizens that all operations that use a cryptocurrency are speculative in nature and carry a high risk of losing value.

Draft federal legislation, the Law on Digital Financial Assets and the Law on Attracting Investment through Investment Platforms, requires the establishment of representative offices or subsidiaries in Russian territory for foreign entities to carry out crypto trading, creating legal uncertainty for foreign cryptocurrency exchanges. The largest foreign crypto exchanges have, however, set up representative offices in Russia. Nevertheless the lack of any regulation for accreditation of cryptobirth may be problematic.

V REGULATION OF MINERS

In judicial practice, a stable legal position has been formed that the mining process is an entrepreneurial activity. Accordingly, miners purchasing technical equipment for their activities do not have consumer status in relations with sellers, and from the point of view

6 Rosfinmonitoring is a federal executive body responsible for combating money laundering and terrorist financing, and developing and implementing state policies and regulatory and legal frameworks in this area.

of the customs authorities, these goods are regarded as not intended for personal use. This circumstance significantly affects the amount of customs payments. Generally, the courts do not agree that a buyer of mining equipment is an ordinary consumer, as the very specifics of the goods purchased by him or her and the purposes for which he or she uses that equipment indicate otherwise.

The courts have taken the view that it is well known and does not need to be proved that cryptocurrencies are used in the financial market, have their own independent trading price and are convertible. Cryptocurrencies can be exchanged for currencies such as the US dollar, euro, rouble and other fiat currencies; they are also used as a settlement and payment instrument in accordance with Part 1, Article 61 of the Civil Procedure Code.

Thus, the buyer purposefully extracts (mines) cryptocurrency through the use of computer equipment acquired from the seller to systematically extract profit in the form of convertible and solvent (liquid) cryptocurrency.

In Russian market conditions, energy suppliers have to make concerted efforts to detect miners of cryptocurrency, because many civilians are adept at concealing this activity.

The State Duma plans to introduce administrative responsibility for any actions related to a cryptocurrency that are not provided for by Russian law. According to the Chairman of the State Duma Committee on Financial Markets, Anatoly Aksakov, all actions using cryptocurrency will be considered illegitimate, including mining, organising and issuing, circulation and opening exchange points. It is still possible to own a cryptocurrency, but only if it 'was acquired under foreign law at foreign points of sale and exchange, but not in Russia'.

The penalty for miners and all those who are somehow connected with cryptocurrency will be a fine, the size of which was not established at the time of writing. Russians will still be allowed to own Bitcoins, but only as an exception – there will be no penalty for them only if crypto tokens were acquired under foreign law at foreign exchange and sale points. A similar action carried out in the territory of Russia will inevitably entail administrative responsibility.

VI CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

Cryptocurrencies have a number of characteristics that have not yet been explored or addressed in legislation, which means that wrongdoers still have unprecedented opportunities to commit crimes. The three main factors that aid wrongdoers are the following: the ability to be anonymous when using cryptocurrencies; the decentralised nature of cryptocurrencies; and the lack of a legal regime for regulating cryptocurrency turnover.[7]

Cryptocurrencies have become an instrument for the implementation of cross-border money laundering. However, there are other crimes that are made possible by the use of a cryptocurrency. For example, acts aimed at preventing the enforced collection of arrears, tax evasion or legalisation of criminal proceeds, uncontrolled movement of capital and the lack of guarantees of consumer rights. In general, the factor that connects these crimes is the absence of legal regulation of the use of cryptocurrencies.

In addition, the weak security of cryptocurrency service providers (primarily cryptocurrency exchanges and wallet services) means that they are frequently attacked by hackers and customer funds are lost.

7 FATF/GAFI. Virtual currencies – Key Definitions and Potential AML/CFT Risks. https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

In Russia, the number of crimes committed using information and communication technologies is steadily increasing, from 11,000 in 2013 to 120,000 in 2019. Supervisors take restrictive measures. The activity of exchanging fiat currencies for cryptocurrencies in Russia is viewed as being indicative of illegal entrepreneurship. The most common crimes involving cryptocurrencies are:

a the use of malicious computer programs to generate cryptocurrency;
b distributed denial-of-service attacks (when attackers send artificially generated traffic to the server to disrupt normal traffic);
c legalisation (laundering) of proceeds of crime;
d illicit trafficking in narcotic drugs, weapons and other items prohibited or limited in circulation;
e sex work and trade, and child pornography; and
f cyber fraud.

Prior to regulation expressly addressing the relevant concepts, law enforcement agencies and the courts defined cryptocurrencies differently. Thus, in court decisions, Bitcoin is defined as a peer-to-peer payment system that uses: the same unit of account;[8] an international settlement system with the means for maintaining settlement accounts in the network[9] and the cryptocurrency itself – the money substitute;[10] electronic money;[11] virtual cash;[12] and a virtual means of payment and accumulation (a text sequence consisting of letters of the Latin alphabet and numbers).[13]

The illegal status of cryptocurrency, the absence of exchange rules and the impossibility of accounting are pushing entrepreneurs into foreign jurisdictions. Citizens wishing to generate cryptocurrency turnover are forced to use the services of foreign exchanges, many of which do not work with accounts opened in Russian banks. The withdrawal of fiat funds will require the participation of a foreign bank located in a jurisdiction supported by the exchange.

As mentioned, the lack of regulation means that violations occur frequently. According to the Russian Association of Cryptocurrency and Blockchain, the average size of losses from investments through semi-legal crypto funds is 300,000 roubles; from investments in non-existing mining projects, 2 million roubles; and from fake services as part of ICO campaigns, 500,000 roubles.[14]

8 Decision of the Court of Intellectual Property Rights of 7 September 2016 in Case No. SIP-368/2016 // SPS Consultant Plus.

9 The definition of the Moscow AU on 14 September 2017 in Case No. A40-138925 / 16-95-126; Determination of the Moscow Region AC on 7 September 2017 in Case No. A41-94274 / 15 // SPS Consultant Plus.

10 Decision of the Primorsky District Court of 7 June 2017 in Case No. 2-7811 / 2017 // SPS Consultant Plus.

11 The verdict of the Trans-Baikal Regional Court of 21 February 2017 in Case No. 22-500 / 2017 // ATP 'Consultant Plus'.

12 The verdict of the Bratsk City Court of 3 March 2017 in Case No. 1-50 / 2017 // SPS ConsultantPlus.

13 The decision of the Anapa City Court of 25 February 2016 in Case No. 2-869 / 2016 // SPS ConsultantPlus.

14 Gladysheva T. In Russia, a 'white list' of companies in the field of cryptocurrency and ICO appeared // *Izvestia*, 13 July 2018.

In March 2018, the Ministry of Finance agreed on a draft law on criminal responsibility for the production and circulation of cryptocurrencies, which provides for up to four years' imprisonment. This is to ensure compliance with the requirements of the legislation on anti-money laundering and counter-terrorist financing (AML/CFT). According to the Ministry of Finance, the main risks of money laundering may arise primarily at the stage of withdrawal of cryptoactive assets in fiat money.[15]

VII TAX

With regard to taxation of transactions related to the circulation of cryptocurrencies, the regulatory authorities are not ready to give official explanations prior to the adoption of relevant legislation defining the concepts of mining, cryptocurrency and the legal status of persons conducting operations with cryptocurrency. The only exception is the taxation of personal income. Legal uncertainty can lead to abuse by both the taxpayer and the tax authority. However, by virtue of the law, all ineradicable doubts, contradictions and ambiguities arising from legislation on taxes and fees are interpreted in favour of the taxpayer. The amendments adopted in March 2019 in the first, second and third parts of the Civil Code brought some clarity with regard to which direction the regulation of cryptocurrency operations would go, but the draft laws on digital financial assets and on crowdfunding did not resolve important issues.

The lack of regulation does not mean that transactions involving cryptocurrency do not entail tax consequences. A person is still criminally liable for tax evasion and the general principles of taxation can still be used as a guide. Irrespective of how the legal status of a cryptocurrency is determined in the future, it has always been and will remain virtual. From the point of view of legal regulation, only what happens to the cryptocurrency in the real world matters. It is appropriate to apply the following concept: virtual relationships are only subject to the law when their participants foresaw or should have foreseen that they will have consequences in the real world. Based on a law that has been adopted (but not yet enacted), cryptocurrency, as an object of civil rights, can be categorised as a property right. Tax legislation is based on the fact that taxes and fees must have an economic basis. When establishing taxes, the taxpayer's actual ability to pay tax is taken into account. Clause 1 of Article 54.1[16] of the Tax Code prohibits a taxpayer from reducing the tax base or the amount of tax payable (or both) as a result of distortion of information about the facts of economic life, taxable items to be reflected in tax, or accounting or tax taxpayer reporting. The object of taxation[17] is the sale of goods (work, services), property, profit, income, expenses or another circumstance that has a monetary, quantitative or physical characteristic. Both existing tax legislation and law enforcement practice are based on the assessment of economic activity and its value, and how it is expressed, in the real world. Therefore, as with mining, and the sale and purchase of cryptocurrency, it is the exchange for fiat money or other property (property rights) from the real world that determines its valuation.

15 Pertseva E. Ministry of Internal Affairs took up Bitcoin // *Izvestia*, 23 August 2018.

16 Limits on the Exercise of Rights Relating to the Calculation of the Tax Base and (or) the Amount of a Tax, a Levy or Insurance Contributions.

17 ibid.

In accordance with the Tax Code,[18] the transfer of property rights is subject to value added tax (VAT). The tax base will be defined as the value of these property rights. The moment of determining the tax base will be the date of the exchange of cryptocurrency for fiat money. In most cases, the cryptocurrency can be sold for foreign currency. When determining the tax base, the taxpayer's revenue in foreign currency is recalculated into roubles at the exchange rate of the Central Bank as at the date when the tax base is determined when realising property rights.[19] At the same time, both miners and traders can use the right to a tax deduction on VAT[20] according to which the tax requested from the taxpayer upon the acquisition of property rights is deductible from the budget. This concerns, for example, VAT paid by energy supply organisations or VAT paid when buying cryptocurrency from a VAT-paying resident of Russia. This approach is justified by the nature of the VAT. It is also favoured by the Presidium of the Supreme Court, which noted that, as a general rule, a taxpayer who uses purchased goods (work, services) to conduct VAT-taxable activities is guaranteed the right to deduct the 'input' tax imposed by counterparties, and the exceptions to the rule should be prescribed by law. In this case, the law clearly indicates that this deduction is possible.[21]

When calculating the income tax, the law explicitly states that the taxpayer has the right to reduce its income from the sale of property in the amount of the purchase price of the property and the amount of expenses related to their acquisition and sale.[22] Entrepreneurs and legal entities that are subject to special tax regimes and use simplified accounting systems should bear in mind that their income is also determined by the date of sale of cryptocurrency for fiat money. But those traders who apply the 'income minus expenses' method will not be able to include the cost of buying cryptocurrency in their expenses,[23] as the Tax Code only provides this possibility for goods. With regard to paying taxes to individuals, the Ministry of Finance takes a clearer position and determines the tax base from cryptocurrency purchase and sale operations as the excess of the total income received by the taxpayer in the tax period from the sale of the corresponding cryptocurrency over the total amount of documented expenses for its acquisition. The property deduction of 250,000 roubles, provided for by Subparagraph 1, Paragraph 2, Article 220 of the Tax Code, cannot be applied.

The Ministry of Finance believes that operations with cryptocurrencies should be subject to personal income tax.[24] Accordingly, individuals should independently calculate and pay tax, receiving remuneration from individuals on the basis of civil law contracts. In other words, if one individual sells Bitcoins to another individual, then he or she must independently determine the tax base, report on the income received, and calculate and pay the tax. However, the Ministry of Finance also relies on the provisions of Article 41 of the Tax Code on determining income.

The general consensus is, therefore, that cryptocurrency should be taxed, but it is not yet clear how income in the form of cryptocurrency or from mining cryptocurrency will be tracked.

18 Subsection 1, Clause 1, Article 146.

19 Clause 3, Article 153 of the Tax Code.

20 Clause 3, Article 153 of the Tax Code.

21 Clause 2, Article 171 of the Tax Code.

22 Subparagraph 2.1, Paragraph 1, Article 268 of the Tax Code.

23 Article 346.16 of the Tax Code.

24 Letter dated 13 October 2017, N 03-04-05 / 66994.

VIII LOOKING AHEAD

The lack of dialogue between the government and businesses reduces the possibilities for adopting prudent regulation of new markets. Also, the insufficient use by public authorities of 'soft' tools, such as guidelines on the compliance of new market participants and new technologies with legislation, creates additional risks of inadvertent violation by businesses of existing laws (e.g., not knowing what taxes are applied to mining). This, in turn, leads to an outflow of capital and reduces the competitiveness of the Russian economy.

The general barriers to the development of the digital economy and to business, including the development of blockchain technology and ITO campaigns, should be removed for Russia's digital economy to thrive. It is also necessary to formulate an approach to reduce the risks of the state regarding the violation of tax and business law by businesses, to eliminate the possibility of using virtual currencies to launder money obtained by criminal means and to hide other crimes.

With regard to the regulation of cryptoeconomics, the consolidation of concepts such as 'token' and 'cryptocurrency' in Russia's civil legislation is unlikely and, if it occurred, might adversely affect the formation of a new market owing to the inability to initially envisage all the qualitative characteristics of these objects. In the next few years, as part of the development of the industry, this approach will be developed by the participants together with government authorities. For example, in relation to the definition of the term 'token', the position is being taken that it is a property right within the meaning of Article 128 of the Civil Code and therefore no further changes to the legislation are required. It seems that the concept of 'cryptocurrency' will include other property (within the meaning of Article 128).

Russia should develop approaches to reduce the risk of AML/CFT and diluting the tax base. It seems that it could stimulate the development of the market by directly extending AML/CFT legislation to new market participants without subjecting them to the Federal Law on Banks and Banking Activities and the Federal Law on the National Payment System. It is necessary to develop a guideline that will clarify the procedure for taxation of transactions with cryptocurrency and income from them.

The development of cryptocurrency market regulation and tokens should begin with soft measures aimed at raising market awareness among the participants and the regulators themselves.

Legislative work is under way to legalise cryptocurrency, but until the adoption of amendments to the current legislation, those who use cryptocurrencies do so at their own risk and do not have the right to expect legal protection if their rights are infringed. In particular, they will not be able to recover the money spent on the purchase of cryptocurrency or to bring any property claims against the traders who manage their cryptocurrency assets. The courts often repeat the argument that, as cryptocurrencies are not regulated, all cryptocurrency transactions carried out by the participants in civil transactions are done so at their own risk.

Meanwhile, disputes over the use of these tools periodically arise, which means the courts are forced to adapt existing legislation to protect the interests of bona fide participants in civil transactions.

The draft law of the Ministry of Finance on digital financial assets[25] proposes to consider cryptocurrency as 'a type of digital financial asset created and accounted for in a

25 Draft federal law on digital financial assets // https://www.minfin.ru/en/document/?id_4=121810&page_id=2104&popup=Y&area_id=4.

distributed digital transaction registry by participants of this registry in accordance with the rules for maintaining a digital transaction registry'. From this definition, it is impossible to identify the constitutive signs of a new economic and legal phenomenon (cryptocurrency), which is necessary to regulate cryptocurrency trading in the financial market. It is unclear what purpose the legislators of this bill are pursuing by adopting a technocratic approach to cryptocurrencies. Technologies used to create cryptocurrencies can change significantly owing to the rapid development of science and technology. The use of cryptocurrency as private non-fiat digital money in the global financial market represents a challenge to the global financial system.

Digital assets such as tokens and cryptocurrencies cannot be limited to national legal frameworks.[26] Therefore, it is necessary in the legal sphere to use the terminology that is used globally. In this regard, it seems inappropriate to use 'digital financial asset' as a concept to unite tokens and cryptocurrencies.

There are proposals to make information an object of civil rights. But the concept of information is not the same as the concept of a digital asset used by businesses. Reference to information without an explanation and without defining the limitations of its scope and purpose is too broad for the purposes of applying civil law.

26 Broy, Sh. U., Zaytz T. G. Legislative regulation of the prevention of terrorism and organised crime in the process of using cryptocurrencies and their impact on the economy and society // *Legal Impact on the Economy: Methods, Results, and Prospects: Monograph* / Rep. ed., V. A. Vaipan, M. A. Yegorova. M: Yustitsinform, 2018.

Chapter 23

SINGAPORE

Adrian Ang, Alexander Yap, Anil Shergill and Samuel Kwek[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

While there is a wide variety of cryptocurrencies and digital tokens with differing characteristics, most cryptocurrencies are a cryptographically secured representation of a token holder's rights to receive a benefit or to perform specified functions. However, from a legal perspective, it is critical to distinguish between these digital tokens, as the offering of different types of digital tokens may trigger different regulatory considerations. At last count, there appear to be broadly four categories of digital tokens: digital payment tokens, security tokens, utility tokens and asset-backed tokens.

i Digital payment tokens

On 21 November 2017, the Monetary Authority of Singapore (MAS) launched a second consultation on its proposed payments regulatory framework. Specifically, MAS issued its Consultation Paper on the Proposed Payment Services Bill. The Payment Services Bill (the Bill) was intended to streamline the regulation of payment services under a single piece of legislation, expand the scope of regulated payment activities to include digital payment token services and other innovations, and calibrate regulation according to the risks posed by these activities. The Bill was passed by Parliament on 14 January 2019 and became the Payment Services Act 2019 (the PS Act). The PS Act is expected to come into force once the regulations supporting the PS Act have been consulted on and finalised.

Under the PS Act, a digital payment token is defined to mean 'any digital representation of value that (1) is expressed as a unit (2) is not denominated in any fiat currency and is not pegged by its issuer to any fiat currency (3) is or is intended to be accepted by the public or a section of the public as a medium of exchange, to pay for goods or services, or discharge a debt (4) can be transferred, stored or traded electronically and (5) satisfies any other characteristic that MAS may prescribe'. Bitcoin and Ether are examples of digital payment tokens.

Digital payment tokens are not currently regulated, as they are not considered securities or currency.[2] MAS has now proposed that where someone deals in digital payment tokens, that person could potentially be construed as providing a digital payment token service under the PS Act, triggering licensing requirements.

1 Adrian Ang and Alexander Yap are partners, and Anil Shergill and Samuel Kwek are senior associates, at Allen & Gledhill LLP.

2 https://www.mas.gov.sg/news/media-releases/2014/mas-to-regulate-virtual-currency-intermediaries-for-money-laundering-and-terrorist-financing-risks.

ii Security tokens

On 1 August 2017, MAS released the following statement:[3]

> *the offer or issue of digital tokens in Singapore will be regulated by MAS if the digital tokens constitute products regulated under the Securities and Futures Act [Chapter 289] (SFA) . . . MAS has observed that the function of digital tokens has evolved beyond just being a virtual currency. For example, digital tokens may represent ownership or a security interest over an issuer's assets or property. Such tokens may therefore be considered an offer of shares or units in a collective investment scheme under the SFA. Digital tokens may also represent a debt owed by an issuer and be considered a debenture under the SFA.*

The Securities and Futures Act[4] is the primary piece of legislation that governs securities and investment in Singapore. Where digital tokens are construed as securities under the SFA, such digital tokens would be subject to the various requirements of the SFA. Most commonly, these include licensing requirements for the regulated activity of dealing in capital markets products (the definition of which includes securities) and prospectus registration requirements for offering securities or securities-based derivatives contracts to persons in Singapore.

The term capital markets products includes any securities, units in a collective investment scheme and derivatives contracts. The term securities, in turn, includes shares, units in a business trust or any instrument conferring or representing a legal or beneficial ownership interest in a corporation, partnership or limited liability partnership and debentures (i.e., bonds or notes). The term securities-based derivatives contracts means any derivatives contract of which the underlying thing or any of the underlying things is a security or a securities index, but does not include certain derivatives contracts prescribed by regulations.

There is a risk that a digital token falling within the described instruments above would be a capital markets product, and for the purposes of this chapter will be referred to as a security token. However, it would be prudent to go further and say that if a digital token displays characteristics that the various financial products that form the definition of capital markets products are typically associated with, there is a risk that they may be construed as a security token and trigger licensing requirements for dealing in capital markets products and prospectus registration requirements under the SFA. This is discussed in further detail in Section II.

iii Utility tokens

Utility tokens typically arise in the context of an initial token offering or an initial coin offering (ICO). At a basic level, an issuer offers digital tokens to participants through blockchain and cryptocurrency technology. Participants typically transfer digital payment tokens (such as Bitcoin or Ether) to the issuer in exchange for digital tokens at a predetermined exchange rate. The digital tokens issued are often designed to be usable to pay for the products or services of the issuer (or its related corporation).

3 https://www.mas.gov.sg/news/media-releases/2017/mas-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-singapore.

4 Securities and Futures Act (SFA), Chapter 289 of Singapore.

Conceptually, such an ICO is different from an initial public offering (IPO) in that in an IPO, funds are raised by an issuer through the issuance of its shares to investors. In an ICO, digital tokens are issued to the consumers of the products and services provided by the issuer (or its related corporation). In a sense, the focus of a participant in an ICO may be on the quality of the products and services provided by the issuer (or its related corporation), while for an IPO, the focus of an investor may be on the quality of the products and services provided by the issuer and how that translates to the overall future value of the company (i.e., the share value of the company).

Digital tokens may also have other rights attached to them. In many jurisdictions, there are financial regulatory concerns surrounding ICOs, generally revolving around the proper legal categorisation of the digital tokens issued pursuant to an ICO. The issue is likely to be determined based on whether such digital tokens are effectively capital markets products (or their equivalent in each jurisdiction), and the follow-on applicability of prospectus registration and financial regulatory licensing laws. From a policy perspective, such laws are generally geared towards protecting consumers by ensuring that they are provided with a prescribed level of information on the offering to enable them to better understand their purchase. In addition, such laws seek to ensure that the entity that deals in such capital markets products keeps to a prescribed level of operating standards, both in relation to its internal operations and its dealings with customers and clients. Where digital tokens are taken not to be capital markets products, consumers may end up bereft of the protections afforded by such laws.

Notwithstanding the above, it is by no means clear how a digital token will be categorised in different jurisdictions.

When dealing with utility tokens, a fundamental consideration is often to ensure that the utility tokens are not characterised as capital markets products and do not display such characteristics (i.e., the tokens are not security tokens). As mentioned above, dealing in capital markets products or offering security tokens may trigger both licensing and prospectus requirements, and it is often the case that such requirements run counter to the considerations underpinning an ICO. It is also advisable to ensure that the underlying product or service that the utility token holder is able to access is not in itself regulated.

iv Asset-backed tokens

One of the benefits of blockchain technology is the ability to tokenise virtually any asset. The technology allows ownership of an asset to be shared between multiple persons, and bought and sold across national boundaries with ease. However, the broad scope of the assets that can be the subject of tokenisation also brings about a broad range of legal considerations, depending on the specific asset that is tokenised and the rights attached to each token.

One commonly tokenised asset belongs to the category of precious metals. In effect, what typically transpires is that the issuer of a token (or a related corporation) has a store of precious metal and wishes to provide the general public with the ability to gain exposure to the price of the precious metal. It may be the case that tokenisation of the ownership in the precious metal allows for each token to be priced in such a manner that the average person can afford to purchase ownership in the precious metal (via ownership of the token). This is possible as there is no limit on the number of tokens that can be representative of a specific amount of precious metal. There is also the added advantage of the token holder being able to transact in the tokens online, without having to deal with the physical aspects of the precious metal but with the ability to withdraw the actual precious metal at any time.

Where advising on tokens that represent ownership in precious metals, consideration should be given to whether this triggers any regulatory implications. By way of example, the buying and selling of tokens may be construed as undertaking spot commodity trading under the Commodity Trading Act (CTA).[5] The CTA defines a spot commodity broker as 'a person whether as principal or agent who carries on the business of soliciting or accepting orders, for the purchase or sale of any commodity by way of spot commodity trading, whether or not the business is part of, or is carried on in conjunction with, any other business'. Spot commodity trading is in turn defined as 'the purchase or sale of a commodity at its current market or spot price, where it is intended that such transaction results in the physical delivery of the commodity'.

Another common business model for such category of digital tokens relates to the tokenisation of real estate. One example is where an issuer collects monies (fiat) from purchasers of a token, and with such monies purchases real estate. Each token represents beneficial interests in a trust that holds the real estate (and rights to some form of return on the real estate). There is a manager that manages the real estate with a view to generating a return for the token holders. Depending on the exact scope of the business model, there may be a number of regulatory issues that are triggered under such a scheme. It is possible that such an arrangement may be considered a collective investment scheme under the SFA, and the offering of the tokens may be seen as the regulated activity of dealing in capital markets products under the SFA. Again, depending on the exact business model, it is possible that the manager may be construed to be providing fund management services under the SFA, thus triggering licensing requirements therefor, unless exempt. A unit in a collective investment scheme falls under the definition of a capital markets product under the SFA.

II SECURITIES AND INVESTMENT LAWS

As mentioned in Section I.ii, dealing in or offering security tokens may trigger both licensing and prospectus requirements under the SFA. Apart from such concerns, issuers and distributors of security tokens who advise or promulgate research analyses and reports could be subject to the licensing requirements of the Financial Advisers Act (FAA).[6]

In addition, operators of platforms or exchanges that facilitate secondary trading of these security tokens that are or have characteristics of derivatives contracts, securities or units in collective investment schemes would need to be approved or recognised by MAS as an approved exchange or recognised market operator, respectively, under the SFA.

An important point to note is that the SFA and the FAA have extraterritorial application. Under the SFA, where acts are carried out partly in and partly outside Singapore, they would be treated as being committed wholly in Singapore, and where an act is carried out wholly outside Singapore, it would be treated as being carried on in Singapore if it has a substantial and reasonably foreseeable effect in Singapore.[7] Under the FAA, a person will be deemed to be acting as a financial adviser in Singapore if he or she engages in any activity or conduct

5 Commodity Trading Act, Chapter 48A of Singapore.

6 Financial Advisers Act, Chapter 110 of Singapore.

7 Section 339 of the SFA.

that is intended to or likely to induce the public in Singapore or any section thereof to use any financial advisory service provided by the person, whether or not the activity or conduct is intended to or likely to have that effect outside Singapore.[8]

III BANKING AND MONEY TRANSMISSION

i Banking

Banking is regulated at a national level by MAS (as part of its regulation of conventional banks), and MAS also imposes data and transactional security requirements on the financial institutions it regulates.

Commercial banks are regulated under the Banking Act.[9] They may undertake universal banking. Besides commercial banking, which includes deposit taking, the provision of cheque services and lending, banks may also carry out any other businesses that are regulated or authorised by MAS, including financial advisory services, insurance broking and capital market services.

Merchant banks are approved under the Monetary Authority of Singapore Act[10] and their operations are governed by the Merchant Bank Directives. On 21 May 2019 MAS released a consultation[11] proposing to consolidate the regulation and licensing of merchant banks under the Banking Act. Their Asian Currency Unit operations are also subjected to the Banking Act. Merchant banks operate within the Guidelines for Operation of Merchant Banks. Their typical activities include corporate finance, underwriting of share and bond issues, mergers and acquisitions, portfolio investment management, management consultancy and other fee-based activities. Most merchant banks have, with MAS' approval, established Asian Currency Units to transact in the Asian dollar market.

The specific type of regulations that a digital bank will trigger will generally depend on the types of activities that it undertakes, and which of the categories set out above the digital bank falls within.

It was reported in May 2019 that MAS was considering whether to allow digital-only banking licenses, which would permit financial technology firms to operate digital-only banks without needing a traditional bank at its core.

ii Money transmission

There is a licensing requirement under the Money-changing and Remittance Businesses Act (MRBA)[12] for the carrying on of remittance business. Remittance business is defined in the MRBA to mean 'the business of accepting monies for the purpose of transmitting them to persons resident in another country or a territory outside Singapore'.[13] Section 2(2)(b) of the MRBA provides that a person is deemed to be carrying on remittance business if he or she offers to transmit money on behalf of any person to another person resident in another

8 Section 6(2) of the FAA.

9 Banking Act, Chapter 19 of Singapore.

10 Monetary Authority of Singapore Act, Chapter 186 of Singapore.

11 The consultation can be accessed at: https://www.mas.gov.sg/publications/consultations/2019/consultation-paper-on-regulating-merchant-banks-under-the-banking-act.

12 Money-changing and Remittance Businesses Act, Chapter 187 of Singapore.

13 Section 2(1) of the MRBA.

country. Persons who facilitate the transmission of digital tokens or fiat should consider whether such transmission would trigger licensing requirements for operating a remittance business.

Notwithstanding the current requirements under the MRBA, under the PS Act, the regulatory requirements relating to the transmission of monies will be expanded, as can be seen from the expanded scope of the regulated activity of 'cross-border money transfer service' and the new regulated activity of 'domestic money transfer service'. As such, where proposing to transfer fiat or digital tokens representing fiat, a person should be mindful of the regulatory requirements under the PS Act.

Under the PS Act, money is defined to include currency and e-money but does not include any digital payment token and any excluded digital representation of value. The PS Act clearly distinguishes between e-money and digital payment tokens. A 'digital payment token' is defined to mean 'any digital representation of value that (1) is expressed as a unit (2) is not denominated in any fiat currency and is not pegged by its issuer to any fiat currency (3) is or is intended to be accepted by the public or a section of the public as a medium of exchange, to pay for goods or services, or discharge a debt (4) can be transferred, stored or traded electronically and (5) satisfies any other characteristic that MAS may prescribe'. By contrast, e-money is defined to mean:

> *electronically stored monetary value that (1) is denominated in any currency, or pegged by its issuer to any currency (2) has been paid for in advance to enable the making of payment transactions through the use of a payment account (3) is accepted by a person other than its issuer and (4) represents a claim on its issuer.*

The definition in the PS Act is useful from a conceptual standpoint, as it provides a clean framework to separate digital payment tokens and e-money.

Different regulated activities may be triggered depending on whether e-money or a digital payment token is being handled. Dealing in digital payment tokens could potentially be construed as providing a digital payment token service under the PS Act, thus triggering licensing requirements therefor. Separately, where e-money issuance is undertaken, or someone is construed to be providing account issuance services, providing domestic money transfer services, providing cross-border money transfer services or providing merchant acquisition services in relation to e-money, licensing requirements could be triggered for these activities under the PS Act.

IV ANTI-MONEY LAUNDERING

i General

Financial institutions operating in Singapore are required to put in place robust controls to detect and deter the flow of illicit funds through Singapore's financial system. Such controls include the need for financial institutions to identify and know their customers (including beneficial owners), conduct regular account reviews, and monitor and report any suspicious transaction. The requirements on financial institutions are set out in MAS Notices on the Prevention of Money Laundering and Countering the Financing of Terrorism (the AML/CFT Notices).

Financial institutions are encouraged to refer to guidance papers for good practices for combating money laundering and terrorism financing, and AML/CFT announcements for information on high-risk jurisdictions, as well as other news.

Such AML/CFT requirements are imposed generally on financial institutions operating in Singapore and are typically independent of whether digital tokens are involved in a transaction. Having said that, the presence of digital tokens may mean that financial institutions will need to conduct additional AML/CFT procedures owing to the anonymous nature of digital tokens.

The AML/CFT risk posed by digital tokens is well recognised in Singapore. In his reply to a parliamentary question on banning the trading of Bitcoin or cryptocurrency, Tharman Shanmugaratnam, the Deputy Prime Minister and the Minister in charge of MAS, observed: '[w]hen it comes to money laundering or terrorism financing, Singapore's laws do not make any distinction between transactions effected using fiat currency, virtual currency or other novel ways of transmitting value. Hence, MAS' AML/CFT requirements apply to all activities of financial institutions, whether conducted in fiat or virtual currencies'.[14] In his reply to a parliamentary question on AML/CFT enforcement on virtual currency transactions, he noted: '[t]here is a clear risk of money laundering . . . [c]ryptocurrency transactions are anonymous. Given also the decentralised systems behind cryptocurrency payments, and the speed at which they can be performed, they can be used to conceal the illicit movement of funds.'[15]

ii Future specific AML/CFT laws

The PS Act will broaden the current scope of MAS' regulatory purview by requiring intermediaries that buy, sell or exchange digital payment tokens to specifically address money laundering and terrorism financing risks.[16] On 6 June 2019, MAS issued the Consultation Paper on the Proposed Payment Services Notices on Prevention of Money Laundering and Countering the Financing of Terrorism (the AML Consultation).[17] MAS has stated in the AML Consultation that all transactions under digital payment token services are considered to carry higher inherent money laundering and terrorism financing risks due to the anonymity, speed and cross-border nature of digital payment token transactions. It is proposed that AML/CFT requirements be introduced on licensees under the PS Act who provide digital payment token services that deal in or facilitate the exchange of digital payment tokens for real currencies where:

a dealing in digital payment tokens includes the buying and selling of digital payment tokens – this will typically involve the exchange of digital payment tokens (such as Bitcoin or Ether) for any fiat currency or another digital payment token (such as a Bitcoin for Ether transaction); and

14 Reply to Parliamentary Question on AML/CFT enforcement on virtual currency transactions, available at https://www.mas.gov.sg/news/parliamentary-replies/2018/reply-to-parliamentary-question-on-amlcft-enforcement-on-virtual-currency-transactions.

15 Reply to Parliamentary Question on banning the trading of bitcoin currency or cryptocurrency, available at https://www.mas.gov.sg/news/parliamentary-replies/2018/reply-to-parliamentary-question-on-banning-the-trading-of-bitcoin-currency-or-cryptocurrency.

16 Crypto Tokens: The Good, The Bad, and The Ugly: Speech by Mr Ravi Menon, Managing Director, MAS, at Money20/20, 15 March 2018, available at https://www.mas.gov.sg/news/speeches/2018/crypto-tokens-the-good-the-bad-and-the-ugly.

17 This can be accessed at: https://www.mas.gov.sg/publications/consultations/2019/proposed-payment-services-notices-on-prevention-money-laundering-countering-financing-terrorism.

b facilitating the exchange of digital payment tokens means establishing or operating a digital payment token exchange that allows the buying or selling of any digital payment token in exchange for any fiat currency or another digital payment token (whether of the same or a different type).

MAS also indicated in the AML Consultation that to fully align with the Financial Action Task Force Standards, it intends to amend the PS Act and issue further AML/CFT Notices at a later stage. The consultation on further amendments is expected to take place at the end of 2020.

V REGULATION OF EXCHANGES

The SFA provides that no person shall establish or operate an organised market (including a securities market), or hold him or herself out as operating an organised market, unless such person is an approved exchange or a recognised market operator. Operators of platforms or exchanges that facilitate secondary trading of security tokens that are or have characteristics of derivatives contracts, securities or units in collective investment schemes would need to be approved or recognised by MAS as an approved exchange or recognised market operator, respectively.

Digital payment token exchanges will be regulated under the PS Act as providing a digital payment token service that includes facilitating the exchange of digital payment tokens. This would be the case even where such digital payment tokens are not deemed to be capital markets products (i.e., not security tokens) within the meaning of the SFA but otherwise fall within the definition of digital payment tokens under the PS Act. Digital payment token exchanges will be required to apply for a licence to operate in Singapore.

VI REGULATION OF MINERS

Whether the mining of digital payment tokens will trigger licensing or regulatory requirements will depend on the exact scope of the mining arrangement. It is possible that if a company offers a service where it rents out mining machines, runs and maintains a collective mining pool that the mining machines are connected to, maintains the mining machines, pools returns from the mining operations and distributes such returns to the miners, this could potentially be construed as operating a collective investment scheme, and relevant regulatory implications will need to be considered.

VII REGULATION OF ISSUERS AND SPONSORS

Generally, issuers and sponsors of digital payment tokens (such as Bitcoin and Ether) are not regulated in Singapore, unless the digital payment token exhibits characteristics of capital markets products or is a tokenised asset. Once the PS Act comes into force, issuers and sponsors of digital payment tokens may trigger licensing requirements for providing digital payment token services, depending on the exact service that is being contemplated.

Utility tokens are typically meant to represent a presale of a product or service to be provided by the issuer (or its related corporation), and such utility tokens are issued to the

consumers of such products or services. In this regard, depending on whether the underlying products or services that utility tokens can be exchanged for trigger licensing or regulatory requirements, issuers of utility tokens may accordingly be subject to regulation.

VIII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

It is expected that every jurisdiction (Singapore included) will face issues pertaining to the bringing and the enforcement of actions relating to digital payment token trading. The two biggest issues arise with respect to identification of the counterparty (in a civil action) or perpetrator of the fraud (in a criminal action). If the counterparty or perpetrator can be identified and located, the second issue concerns bringing an action against that person and enforcing a judgment against that person.

Given the cross-border nature of the internet and digital payment token transactions, fraud can be perpetrated from virtually any location relating to persons in any other location: after all, anonymity is one of the greatest hallmarks of digital payment token systems and blockchain technology. This is coupled with the ease of concealing one's identity on the internet. In such situations, the challenges lie in being able to identify and locate, and subsequently bring and enforce legal action against, that person, whether locally or in a foreign jurisdiction. At present, there may be methods of identifying and locating such persons, but it is expected that a concerted effort and a large amount of resources would need to be expended to mount any successful attempt at doing so. In the case of civil proceedings, a claimant is unlikely to have the expertise or resources to be able to do so. In the case of criminal proceedings, it is likely that the scale of the fraud (and possibly other factors) would determine whether expending the amount of resources to identify, locate and bring an action against a perpetrator is justifiable.

IX TAX

There is no capital gains tax or inheritance tax in Singapore. The corporate income tax rate is 17 per cent for companies, while goods and services tax (GST) is currently charged at a rate of 7 per cent. There remains some residual uncertainty as to how taxes will be applied to certain digital token offerings. By way of example, in the context of an initial token offering, it is unclear how corporate tax and GST will be applied to the sale of the utility tokens pursuant to the offering.

X OTHER ISSUES

Based on publicly available reports[18] and discussions with industry players, it is understood that certain fintech companies (e.g., cryptocurrency exchanges) and companies that have conducted offerings of utility tokens have had difficulties in opening or maintaining bank accounts in Singapore. A number of banks in Singapore have either refused to allow such persons to open a bank account or have otherwise closed existing bank accounts. We believe that the reason for this probably comes down to concerns relating to AML/CFT requirements.

18 https://www.bloomberg.com/news/articles/2017-09-26/singapore-cryptocurrency-firms-facing-bank-account-closures.

XI LOOKING AHEAD

As discussed in Section I.i, the PS Act will streamline the regulation of payment services under a single piece of legislation, expand the scope of regulated payment activities to include digital payment token services and other innovations, and calibrate regulation according to the risks posed by these activities.

When the PS Act comes into force, payment firms will only need to hold one licence under a single regulatory framework to conduct any or all of the specified payment activities. Only payment activities where payment firms face customers or merchants, process funds or acquire transactions, and pose relevant regulatory concerns will need to be licensed. The new framework will expand the scope of regulation to include domestic money transfers (e.g., transferring money through payment kiosks), merchant acquisitions (e.g., acquiring transactions through a point-of-sale terminal or online payment gateway), and the purchase and sale of digital payment tokens.

To help ensure that the expanded scope of regulation is not onerous, the PS Act will differentiate regulatory requirements according to the risks that specific payment activities pose rather than apply a uniform set of regulations on all payment service providers. This can be seen from the calibrated approach that MAS has taken in the AML Consultation.

The PS Act will empower MAS to regulate payment services for money laundering and terrorism financing risks, strengthen safeguards for funds belonging to consumers and merchants, set standards on technology risk management, and enhance the interoperability of payment solutions across a wider range of payment activities.

Chapter 24

SPAIN

Pilar Lluesma Rodrigo and Alberto Gil Soriano[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

In Spain, there is no legislation specific to virtual currencies, nor is any draft legislation in the pipeline. There is only one piece of draft legislation, approved by the government in February 2019, which indirectly relates to virtual currencies, although it has not yet been debated in the Spanish parliament. This draft legislation includes measures for the digital transformation of the financial system, including the legal framework for a regulatory sandbox.[2]

That said, in 2018 the Spanish securities regulator (CNMV) and the Bank of Spain issued joint advice on the risks associated with purchasing virtual currencies or investing in products tied to them,[3] and the CNMV has issued two other documents setting out its opinion and position on several matters related to virtual currencies. However, thus far in 2019, only the CNMV has issued an statement to clarify that it has not authorised any prospectus, nor has it exercised any authorisation for or power to verify any transaction in connection with cryptocurrencies.[4]

The Spanish tax authorities have also issued several binding rulings on the tax aspects of activities involving virtual currencies.

II SECURITIES AND INVESTMENT LAWS

i Classification and commercialisation of virtual currencies

The CNMV has unofficially stated that virtual currencies per se should not be considered as securities. However, it has acknowledged that the offering and commercialisation of virtual currencies can have investment law implications as follows.[5]

Direct marketing

Where virtual currencies are acquired through platforms operating on the internet (exchanges) and through cryptocurrency automatic teller machines (ATMs), the CNMV considers that investors do not actually directly own the virtual currencies, and instead only have rights

1 Pilar Lluesma Rodrigo is counsel and Alberto Gil Soriano is a senior associate at Uría Menéndez. The authors would like to thank Alberto Gómez Fraga and Alejandro Virumbrales de Rojas for their collaboration on this chapter.

2 http://www.rdmf.es/wp-content/uploads/2018/07/Anteproyecto-sandbox-fintech.pdf.

3 https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/NotasInformativas/18/presbe2018_07en.pdf.

4 https://www.cnmv.es/portal/verDoc.axd?t={76316281-6a21-42a5-b742-085dca1d9c7f}.

5 See CNMV considerations on cryptocurrencies and ICOs addressed to market professionals, 8 February 2018.

in relation to an unsupervised exchange or intermediary. As a consequence, purchasers are exposed to the risk of an intermediary becoming insolvent or not complying with basic rules on proper record-keeping, diligent custody and recording of assets, and the correct management of conflicts of interest.

Contracts for differences

Entities offering these products should be authorised by the CNMV to provide investment services and meet all reporting obligations and other applicable rules of conduct.

Futures, options and other derivatives

If these types of products have been authorised by a regulated supervisor, their active marketing under a public offering by market professionals to retail investors might require a prospectus approved by the CNMV or another EU authority under the passporting arrangements.

Specific investment funds and other collective investment vehicles that invest in virtual currencies

These types of vehicles and investment funds should be approved or registered by the CNMV. The CNMV[6] has acknowledged that, in accordance with Article 2.1 of Law 22/2014, a closed-ended collective investment scheme can invest directly in virtual currencies, but it has to be registered with the CNMV. In this regard, the CNMV has pointed out that the divestment policies of its participants or partners must meet the following requirements: divestment must take place simultaneously with respect to all investors and participants; and investors and participants must be remunerated according to the articles of association or regulations for each class of shares or participations.

This type of fund cannot be marketed to retail investors.

Acquiring structured bonds where the underlying asset is a virtual currency

The marketing under a public offering regime of exchange-traded products and exchange-traded notes requires the approval of the supervisors of an explanatory prospectus that has also been subject to the relevant EU passporting procedure.

ii Initial coin offerings

The CNMV[7] understands that transactions structured as initial coin offerings (ICOs) in many cases should be treated as issues or public offerings of transferable securities given the broad definition of transferable security under Spanish law.[8]

6 See Questions and Answers for FinTech companies on activities and services that may be within the CNMV's remit, last updated 12 March 2019.

7 See CNMV considerations on cryptocurrencies and ICOs addressed to market professionals, 8 February 2018.

8 Article 2.1. of the Spanish Securities Law: 'Any patrimonial right, regardless of its name, which, because of its legal configuration and system of transfer, can be traded in a generalised and impersonal way on a financial market.'

The CNMV sets out the following factors as being relevant in assessing whether transferable securities are being offered through an ICO:

a tokens that assign rights or expectations of a share in the potential increase in value or profitability of businesses or projects or, in general, that they constitute or assign rights equivalent or similar to those of shares, bonds or other financial instruments governed by Spanish securities law; or

b tokens that entitle access to services or to receive goods or products, that they are offered referring explicitly or implicitly to the expectation that the purchaser or investor will obtain a profit as a result of their increase in value or some form of remuneration associated with the instrument, or reference is made to its liquidity or tradability on equivalent or allegedly similar markets to regulated securities markets.

However, with regard to point (b) above, if it cannot be reasonably established that there is a correlation between the expectations of a profit or an increase of value and the evolution of the underlying business or project, then the token should not be considered a financial instrument.[9]

If ICOs qualify as financial instruments, then the regulation contained in, relating to or arising from the Markets in Financial Instruments Directive II, the Prospectus Directive and the Alternative Investment Fund Managers Directive should apply to them.

Even if an ICO does not qualify as a public offer (because it is either aimed at fewer than 150 investors, or involves a minimum investment of €100,000 or a total amount of less than €5 million), if the placement is made using whatsoever form of advertising (including websites in Spanish offering the tokens), an entity authorised to provide investment services should intervene in relation to its marketing.[10] The CNMV understands that this requirement is fulfilled if the entity authorised to provide investment services intervenes:

a on the occasion of each individual subscription or acquisition of the securities or financial instruments as a placement agent, broker or adviser, subject to the rules applicable in each case; or

b by validating and supervising the offer in general and, in particular, the information provided to investors, and the placement or marketing procedure used (without an authorised entity having to intervene on the occasion of each subscription or acquisition). With regard to the validation of information, the authorised entity must ensure that the information is clear, impartial and not misleading, and that it refers to the characteristics and risks of the securities issued, as well as the company's legal, economic and financial situation, in a sufficiently detailed manner to allow the investor to make a well-informed investment decision. Likewise, the information for investors shall include a warning on the novel nature of the registry technology and on the fact that the custody of the tokens is not carried out by an authorised entity.

To date, the CNMV has not authorised any ICOs, although it has analysed several potential ICO structures. The action of the CNMV in connection with those projects on the issue of tokens, which could be equivalent to transferable securities, has been limited to confirm that in the event of complying with the requirements set out in the Spanish legislation not be

9 See CNMV Criteria in relation to ICO, 20 September 2018.

10 Article 35.3 of the Spanish Securities Law.

considered as a public offer, the transaction would not require the approval of a prospectus; nor would it be subject to verification or prior intervention by the CNMV, although the participation of an investment firm is necessary.

III BANKING AND MONEY TRANSMISSION

The Bank of Spain, the Spanish authority responsible for banking and money transfer matters, has not issued any statement or otherwise set out its position on virtual currencies other than in the aforementioned joint warning issued with the CNMV.

According to the joint warning, and although they acknowledge that virtual currencies are occasionally presented as an alternative to legal tender, the Spanish authorities note that the former differ greatly from the latter in that their acceptance as a means of payment of a debt or other obligations is not mandatory, their circulation is very limited and their value fluctuates widely, meaning that they cannot be considered as a sound store of value or a stable unit of account.

In this regard, the advice of the European Banking Authority on crypto assets of 9 January 2019 provides that a competent authority will consider a token to be electronic money if it: is electronically stored; has monetary value; represents a claim on the issuer; is issued on receipt of funds; is issued for the purpose of making payment transactions; and is accepted by persons other than the issuer.[11]

At present, no virtual currency, including Bitcoin, is recognised by Spanish law as a digital currency, electronic money or as a payment method.

IV ANTI-MONEY LAUNDERING

Without prejudice to the warnings issued by the Bank of Spain and the CNMV on money laundering risks regarding virtual currencies themselves and the activities related to them, there is no specific Spanish money laundering regulation (in force or in draft form) applicable to virtual currencies, and the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences (SEPBLAC), the Spanish money laundering authority, has not expressed its view on this matter.

The implementation of the Fifth Anti-Money Laundering Directive[12] is not expected to be implemented into the Spanish legislation in the short term.

V REGULATION OF EXCHANGES

The regulation to which an exchange is subject under Spanish law depends on whether or not the assets are traded as financial instruments and on the type of activity performed within the exchange.

Although there is no specific regulation on trading platforms for virtual currencies or other crypto assets, the CNMV[13] has indicated that to the extent that the assets traded in an exchange are not considered as financial instruments, at a very minimum they should

11 https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf.

12 Directive (EU) 2018/843 of 30 May 2018.

13 See Questions and Answers for FinTech companies on activities and services that may be within CNMV's remit, last updated 12 March 2019.

be subject to rules related to custody, registration, management of conflicts of interest between clients and transparency on fees (in addition to anti-money laundering regulations). Therefore, the CNMV recommends that these platforms voluntarily apply the principles of securities market regulations relating to the aforementioned matters to ensure the proper functioning of their activities. If they qualify as financial instruments, Spanish securities market legislation applies, which means the corresponding authorisations must be obtained, including, where appropriate, an authorisation as a trading venue (such as a regulated market, a multilateral trading system or an organised trading facility), or as an investment firm or credit institution that operates as a systematic internaliser.

However, the Bank of Spain has not given any guidance as to whether activities performed by an exchange would qualify as payment services or currency exchange services for regulatory purposes where virtual currencies are used solely for payment purposes (not as securities or similar).

To the extent that regulated markets, multilateral trading facilities (MTFs) and organised trading facilities (OTFs) located in Spain require that the instruments traded on or through them be represented in book entries, tokens cannot be traded in Spanish regulated markets, MTFs or OTFs because they cannot be represented in book entries.

VI REGULATION OF MINERS

With the exception of the tax issues explained in Section IX, there is no regulation of miners in Spain, and the Bank of Spain and the CNMV have not expressed their views on this matter.

However, to the extent that miners would not be considered as issuers of financial instruments or electronic money, or as placing financial instruments, no licence or authorisation would be required under Spanish law to mine.

VII REGULATION OF ISSUERS AND SPONSORS

To the extent that virtual currencies could be classed as financial instruments or as electronic money, their issuers must obtain the corresponding authorisations from the CNMV and the Bank of Spain. In terms of virtual currencies as financial instruments, see Section II.ii regarding ICOs. Neither the Bank of Spain nor the current legislation considers a virtual currency as electronic money; therefore, its issuance falls outside the scope of the Spanish legislation on electronic money institutions, although the assessment has to be made on a case-by-case basis.

The concept of sponsor does not exist under Spanish law.

VIII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

In recent years, fraud through improper acts of disposition relating to cryptocurrencies such as Bitcoin has been increasing. As with any other type of asset, there are certain criminal liabilities when dealing with virtual currencies, given that the conduct of a third party (such as a wealth manager) may cause a loss to the investor's equity.

First, it must be kept in mind that equity as a whole is the legal interest protected from the crime of fraud and that cryptocurrencies are a part of this equity because they are considered valuable assets. As a consequence, improper acts of disposition of cryptocurrency

assets are protected under criminal law. The behaviour described is considered punishable when the requirements in Article 248 of the Criminal Code have been met. This Article sets out the ways in which the crime of fraud can be considered to have been committed.

The first of those is in Article 248.1: when the perpetrator, for financial gain and by means of deception, induces an essential error relating to the victim that produces an act of disposition of assets to his or her own detriment or to the detriment of a third party. In addition, there must be a link between the deception of the perpetrator and the act of disposition of the victim (see High Court Judgment 531/2015 of 23 September).

Article 248.1 also provides for another type of fraud in cases in which perpetrators effect a manipulation through a computer or similar device to carry out a non-consensual transfer of an asset to the detriment of the victim or a third party (High Court Judgment 860/2008 of 17 December). This is computer fraud, a type of fraud set out in Article 248.2.a) of the Criminal Code. This Article sets out the same scheme as described above but without the need for deception – which is interpreted narrowly – as it is replaced by manipulation through a computer. Where there must be a deception for there to be traditional fraud, there must be manipulation through a computer or similar device for there to be computer fraud. This implies that this crime can be committed through a range of behaviours, given the breadth of the expression 'manipulation through a computer or similar device'. Thus, for example, the offence would be committed when an individual alters an email address or bank account number or implants files that unlock a user's passwords.

Judgment 326/2019 of June 20 of the Criminal Chamber of the Supreme Court ruled on Spain's first case of fraud regarding cryptocurrencies under Article 248.1 of the Criminal Code. In this case, the Supreme Court upheld the sentence of imprisonment given to a director of a company as the perpetrator of the offence of fraud. According to the judgment, the director signed several high-level trading agreements under which he committed to manage Bitcoins that were delivered to him as a deposit, reinvest the potential dividends and, finally, at maturity, deliver the profits obtained in exchange for a commission. However, it was proven that at the time of signing those agreements, he did not intend to fulfil his obligations as he had not carried out any transactions, and his only intention was to seize the received Bitcoins and simulate the execution of the agreements.

In the judgment, the Supreme Court held that cryptocurrencies are an intangible asset and not physical money, and consequently cannot be considered as money in the legal sense. Thus, although the victim delivered cryptocurrencies (and subsequently lost them because of the fraud), the perpetrator had to pay back the equivalent value in euros of the cryptocurrencies at the time when they were delivered.

The criminal proceedings through which these crimes are prosecuted in Spain do not contain any special provision for when the disposition of assets relates to a type of cryptocurrency instead of a traditional currency. Therefore, the procedure for summary proceedings will apply if the penalty does not exceed nine years in prison.

These proceedings are divided into three phases. The first is the pretrial phase, in which the judge will try to obtain evidence to determine whether the investigated behaviour may be considered criminal and, if so, discover the identity of the perpetrator. The second is the intermediate phase, in which the prosecution and defence will draft their respective reports. The third phase is the oral trial, in which the admitted evidence is assessed.

The main procedural difficulties faced by the Spanish authorities when it comes to prosecuting these crimes are the lack of jurisdiction and competence. The anonymity with

which perpetrators act, the places from which they do so (in most cases this is outside Spain) and the fact that the funds usually go to other countries prevent action being taken against them through the judicial route in Spain.

IX TAX

Virtual currencies perform an economic function (store of value or medium of exchange), which means that their possession and use may have tax implications. In addition, they pose a higher-than-average risk of being used as a means to commit tax fraud given that it is very difficult to determine the true identity of their owners (to the point that they are almost anonymous), and that the transactions are peer-to-peer and may have a cross-border element, and therefore the ability of tax authorities to monitor them is reduced. All this has put them under the spotlight of the Spanish tax authorities, albeit the tax regime and reporting obligations regarding virtual currencies are still at an early stage.

i Income tax and value added tax (dynamic approach)

The tax treatment of virtual currencies and their trading differs within the country, depending on the tax. From an accounting standpoint, the Spanish Accounting Board considers virtual currencies to be an intangible asset or a commercial stock, depending on their use.

To date, the Spanish tax authorities have considered that any operation (except mining) with virtual currencies constitutes a barter transaction for income tax purposes (personal income tax, corporate income tax and non-resident income tax), which means that users of virtual currencies make a capital gain or loss with any delivery of virtual currencies; and tax compliance becomes complicated and burdensome for both the taxpayer and the tax authority.

The Spanish tax authorities set out in binding tax ruling V0808-18 of 22 March that the use of virtual currencies outside of the performance of an economic activity may result in capital gains or losses at the moment in which the transaction takes place (Article 14.1.c) of Law 35/2006 of 28 November on personal income tax (the PIT Law)), with a tax rate of up to 23 per cent for individuals. According to binding tax ruling V1604-18 of 11 June, fees charged by the exchange increase and the decrease the acquisition and sale price, respectively, if they are directly related to the transaction. The first-in, first-out principle applies. The income obtained from mining is considered business income, and the applicable tax rate could be as much as 48 per cent for individuals, depending on the autonomous region where they reside. The corporate income tax rate is 25 per cent, while the non-resident income tax rate is 24 per cent (19 per cent for residents of the European Union and European Economic Area). The Spanish tax authorities also state in binding tax ruling V1149-18 of 8 May that the exit tax regulated in Article 95 *bis* of the PIT Law does not apply to virtual currencies.

As regards value added tax (VAT), the Spanish tax authorities' position, as set out in binding tax ruling V1748-18 of 18 June, is aligned with that of the European Court of Justice, which considered in *Hedqvist*[14] that virtual currencies constitute a currency in the sense of Article 135(1)(e) of the VAT Directive and are a direct means of payment; therefore, services related to those currencies (including mining) are covered by the VAT exemption granted by that Article. Consequently, input VAT will not be deductible.

14 Judgment of 22 October 2015, *Hedqvist*, Case C-264/14.

ii Net wealth tax and reporting obligations (static approach)

Virtual currencies, as an asset, fall under the scope of Law 19/1991 of 6 June on net wealth tax (the NWT Law) and therefore must be declared by filing Form 714 with the Spanish tax authorities by 30 June each year. According to Article 24 of the NWT Law, taxpayers must report their virtual currencies' market value in euros on 31 December. There is no official market value, so taxpayers will have to rely on the most widely used websites (such as www.coindesk.com). The Spanish tax authorities endorsed this conclusion in binding rulings V0590-18 of 1 March and V2289-18 of 3 August, among others. The net wealth tax rate can be up to 2.75 per cent, depending on the autonomous region of residence (there are some regions with a zero per cent rate).

In addition to the net wealth tax, there are three independent obligations to declare all assets held abroad worth more than €50,000 (bank accounts, securities and real estate). Taxpayers must submit Form 720 (informative report of assets and rights held abroad) by 31 March each year. To date, virtual currencies have not been considered to be securities or held in a bank account for tax purposes; therefore, it seems they need not be included in a Form 720 declaration. However, this approach will probably change in the near future. In this regard, the government made public on 19 October 2018 a draft bill on measures to prevent and fight tax evasion (the Draft Bill), including a new obligation to report the amount of virtual currencies held in Spain or abroad (through Form 720), identifying the owner and the beneficial owner; and report all transactions involving virtual currencies (acquisitions, sales, barter transactions or transfers). The legislative proposal was published for public consultation on 23 October 2018.[15]

The Annual Tax and Customs Control Plan for 2018, published in the Spanish Official Gazette of 23 January 2018, pointed out that, in the context of the prevention and suppression of smuggling, drug trafficking and money laundering, the tax authorities 'will detect and prevent the use by organised crime of the deep web to trade in any illicit goods, as well as the use of cryptocurrencies such as Bitcoin or similar as a means of payment'. In addition, the National Anti-fraud Office attempted to identify all entities that operate with virtual currencies, and sent them requests to provide specific information. Thus, the pre-filled tax forms that the Spanish authorities make available to the taxpayers each year include that the taxpayer has carried out transactions with virtual currencies.

The Spanish tax authorities are also assessing the possibility of imposing new reporting obligations, regulating 'human ATMs' (persons carrying out physical transfers of virtual currencies using apps such as Meetup[16]) and establishing a sanctioning regime for non-compliance with these reporting obligations. In fact, the Draft Bill requires: (1) wallet providers to provide information on virtual currencies balances (segregated by virtual currency), owners, authorised persons or beneficiaries of these balances; and (2) exchanges to provide information on the transactions carried out, identifying the parties involved, address, tax identification number, class and number of virtual currencies, and price and date of the transaction. These reporting obligations also apply to issuers of ICOs with tax residence in Spain.

15 http://www.hacienda.gob.es/Documentacion/Publico/NormativaDoctrina/Proyectos/Tributarios/ANTEPROYECTO%20LEY%20ATAD.pdf.

16 www.meetup.com.

However, the dissolution of the Spanish parliament and the calling of a general election in spring 2019 implied the automatic withdrawal of the Draft Bill. It is likely that the new government, formed after the general election and likely to take office in September 2019, will relaunch this initiative.

X LOOKING AHEAD

While no specific legislation has been adopted in Spain on virtual currencies, the need for comprehensive regulation (of, inter alia, tax, consumer protection and regulatory aspects) regarding this matter has been already discussed in both Spanish legislative chambers by all political parties.

On the other hand, the Spanish supervisory bodies (the CNMV, the Bank of Spain and SEPBLAC) understand that, given the transnational nature of virtual currencies and the activities related to them (issuance, deposit, marketing, etc.), their regulation should be addressed at an international level or, at the very least, at an EU level, so that as many regulators and supervisory bodies as possible adopt and share common positions, otherwise uncoordinated regulatory approaches may prove ineffective and create incentives for regulatory arbitrage. The first step is Directive 2018/843 of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, which directly regulates virtual currencies for the first time at an EU level.

Despite the potential risks that virtual currencies pose as a consequence of their lack of regulation, both the Spanish legislator and supervisory bodies are aware of their importance and of the technological developments behind them, and they are therefore pressing for the speedy adoption of regulations and common positions on this matter.

Chapter 25

SWEDEN

Niclas Rockborn[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

Swedish law does not contain any comprehensive regulation governing virtual currencies and virtual currencies are largely unregulated under Swedish law. However, in their capacity of constituting instruments of payment and, potentially, transferable securities (as further elaborated in Sections II and III), some aspects regarding virtual currencies and various activities relating to them are subject to regulation pursuant to more general legal frameworks. There is also, to a limited extent, upcoming specific regulation regarding certain activities relating to virtual currencies that will subject custodian wallet providers and virtual currency exchanges to regulatory registration requirements and requirements to comply with the Swedish Anti-Money Laundering Act (the AML Act) (see Section IV).

The legal status of virtual currencies is, in some aspects, relatively clear. However, in other aspects, it is subject to a high degree of uncertainty, as well as controversy, as to whether virtual currencies fall within the scope of various regulated types of property. As a starting point and a basis for the discussion of the issue of legally classifying and categorising virtual currencies – which is an issue that has bearing on the applicable obligations of persons conducting various types of activities involving virtual currencies – it is possible under Swedish law for intangibles to have the legal status of property without any explicit statute granting such status to a specific category of intangibles.[2] While there is no express statute governing the legal status of virtual currencies under Swedish law, it is sufficient that a virtual currency is recognised as an object under customary practice, as well as by the parties to a legal relationship involving such virtual currency, for it to constitute property. Consequently, it is legally possible to own virtual currencies under Swedish law, and virtual currencies are afforded the same general protection as other types of property under the legal concept of ownership.

The more detailed classification of virtual currencies as financial instruments (more specifically transferable securities) or instruments of payment, or both, is discussed further below.

In recent years, following the increasing popularity of virtual currencies, and in particular consumers' interest in investing and trading in them, both national and international regulatory authorities, including the Swedish Financial Supervisory Authority (SFSA), have issued statements of warning relating to virtual currencies and initial coin offerings (ICOs), noting the lack of applicable regulation in many material aspects. The increasing significance

1 Niclas Rockborn is a partner at Gernandt & Danielsson Advokatbyrå.

2 See, inter alia, Government Bill 2004/05:18, p. 57. Cf. the position under English law following the judgment in *OBG v. Allan*, United Kingdom House of Lords Decision.

of virtual currencies in the eyes of both the European Union and the Swedish regulator is demonstrated not least by the recent amendments to Swedish AML legislation, bringing providers of certain services related to virtual currencies into the scope of the AML Act.

II SECURITIES AND INVESTMENT LAWS

i Classification as a financial instrument

It has not been explicitly settled whether virtual currencies may qualify as financial instruments under Swedish law. The key to making this determination is whether virtual currencies constitute transferable securities, as defined in the Swedish Securities Market Act, which implements the Markets in Financial Instruments Directive (MiFID) and MiFID II.[3] The European Securities Markets Authority (ESMA) has stated that virtual currencies may, depending on how an offering of coins or tokens is structured, constitute transferable securities.[4] In response to a survey undertaken by ESMA in the summer of 2018 regarding the qualification of virtual currencies as financial instruments in the European Union, the SFSA expressed the view that dematerialised instruments can qualify as securities if the instruments can be registered in a manner that has the same legal effect, specifically in regards to rights *in rem*, as possession and presentation of a physical certificate, such as a coupon bond or a bearer bond. Registration based solely on contractual grounds is not sufficient to meet this requirement. The SFSA concluded that it cannot generally be ascertained whether virtual currencies can qualify as securities, attributing this to the lack of precedent on how an acquirer of virtual currencies can obtain rights *in rem* under Swedish law. In addition to noting this uncertainty, the SFSA expressed the view that an instrument must entail rights to its holder or obligations to its issuer, or both, which are legally enforceable. Consequently, whether this requirement is met in relation to any particular virtual currency or ICO must be assessed in each individual case.

A question of a more general nature, which has significant implications for the issue of whether virtual currencies qualify as financial instruments, is the extent, if any, to which national deviations in the interpretation of what constitutes transferable securities are legally permissible under MiFID II. European capital markets law has undergone a shift in character from generally setting forth minimum harmonisation rules, with greater possibilities of national discrepancies and margins of appreciation, to an increased use of directly applicable regulations and full harmonisation directives, leaving no room for national discrepancies. The structure of the legal framework, with the definitions found at the beginning of MiFID II playing an essential role in the application of other legal acts within capital markets law, further questions the room for national deviations in this regard. As the definitions (e.g., of financial instruments and transferable securities) found in MiFID II are used to determine the scope of applicability of several other legal acts, some of which take the form of directly applicable

3 Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments, and Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments, respectively.

4 See ESMA's statement dated 13 November 2017, Reference No. ESMA50-157-828 and ESMA's Advice on Initial Coin Offerings and Crypto-Assets dated 9 January 2019, Reference No. ESMA50-157-1391.

regulations (e.g., the Market Abuse Regulation[5] and the new Prospectus Regulation[6]), allowing national deviations from the definitions may have a considerable impact on the European capital markets regulatory framework in its entirety. As one of the purposes of MiFID II is to harmonise the legal framework of the European Union, and considering the important role that the definitions play for other legal acts, the position most consistent with the EU regulator's intentions concerning the interpretation and implementation of the definitions would be to consider the room for national deviations from the definitions in MiFID II to be extremely limited. Further, allowing deviations would open up the possibility of EU Member States interpreting the definitions to treat essential investor protection law, such as the prospectus rules, as not applicable to make themselves more attractive to new industries, such as the virtual currency industry. This could open up a race to the bottom in terms of investor protection, which is directly contrary to the purposes of European capital markets law. The foregoing supports the view that, when assessing whether virtual currencies may constitute transferable securities, national legislation must be interpreted in such a way that it does not deviate from the definition under EU law. Having noted this, however, it is an undisputable fact that there are varying positions among national regulators with respect to the interpretation of the definitions in MiFID II. In fact, these more or less considerable differences are recognised by ESMA in its survey regarding legal qualification of virtual currencies.

As regards whether virtual currencies constitute financial instruments, mainly by being transferable securities, tokens or coins created and marketed through an ICO and subsequently traded in some form of secondary market appear to be the most relevant units of analysis. The rights associated with a token may vary with every issuance, so this chapter is written using the classification of tokens as currency tokens, utility tokens and investment tokens.[7]

Currency tokens such as Bitcoin and Ethereum are intended to be used as a general means of payment and function in a similar manner to regular currencies. These virtual currencies are unlikely to constitute transferable securities as they generally do not constitute securities. The ownership and possession or the equivalent registration on the blockchain of currency tokens usually does not give any rights towards the issuer or any other physical or legal person, which is a prerequisite of such tokens being considered as securities. In particular, such registration is not legally recognised under Swedish law as granting rights *in rem*, and is based solely on contractual grounds. As a consequence, currency tokens generally fall outside the scope of the definition of securities. In cases where they are classified as securities owing to them granting such rights, and are negotiable on the capital market, they may still fall outside the scope of the definition of transferable securities under MiFID II on the basis of being regarded as instruments of payment.

Utility tokens function mainly as either a means of payment in a specific setting with no use as a general means of payment (e.g., paying for services or goods from a specific vendor) or as granting access to a service or product through ownership of such tokens. The product or service does not always exist at the time of the ICO. In general, these tokens do

5 Regulation (EU) 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse.

6 Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market.

7 Cf. the classification of the Swiss Financial Market Supervisory Authority in the Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs), published 16 February 2018.

not constitute transferable securities in the sense of the definition under MiFID II; they appear not to fit into the purposes and intentions of MiFID II and other capital markets law. In essence, utility tokens function more as a means of purchase of a product or a service, with an added element of uncertainty regarding whether a product or service will be able to be delivered owing to it not being available at the time of the purchase of the tokens. The various problems that may arise in the context of such issuances are mainly dealt with through legislation other than capital markets law, for instance consumer protection law. However, if tokens are being marketed with the expectation of being able to be sold for a profit as the project that the tokens finance develops, there is an increased possibility of the tokens being classified as transferable securities, provided that they are securities and meet the requirements of transferability and being negotiable on the capital market. Further, if the tokens give rights to financial benefits, such as dividends or put options with a financial gain in the event that the underlying project of the issuance is successful, the tokens are likely to be considered transferable securities.

Investment tokens are tokens whose main purpose is being an investment, and generally give financial rights and in some cases participation rights analogous to shares in a company. Investment tokens are likely to be considered transferable securities, provided that they are securities and meet the requirements of transferability and being negotiable on the capital market.

The classification of tokens is not absolute, which means that some tokens may have attributes from different classes. An analysis of the rights of tokens must be done on a case-by-case basis to determine whether they constitute transferable securities.

In conclusion, the legal qualification of virtual currencies as financial instruments under Swedish law is uncertain. The limited available guidance indicates that virtual currencies would generally be expected to fall outside the qualification as financial instruments. However, this ultimately depends on the structuring of and the rights associated with the virtual currency. In the case of ICOs, if coins or tokens have an investment component, for instance a right to dividends or payouts depending on the success of the issuer, they may be deemed transferable securities, provided that they meet the requirements of transferability and are negotiable on the capital market according to MiFID II. Additionally, derivative instruments related to virtual currencies may constitute financial instruments, for example where they relate to price differences for virtual currencies.

ii Prospectus obligations

If tokens are considered to be transferable securities, they may be subject to the new Prospectus Regulation and Swedish law and regulations that implement the European prospectus regime. If transferable securities are offered to the public or are being listed on a regulated market, a prospectus must be prepared unless an exemption is applicable.[8] It is customary as part of the ICO process to publish a white paper, which usually describes the project and related topics in brief. At the time of writing, the content of these white papers does not, in general, meet the Swedish prospectus requirements.

The new Prospectus Regulation entered fully into force on 21 July 2019. One of its main purposes is to reduce the administrative burden under the prospectus regime, especially

8 Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market.

for smaller companies. The Regulation is guided by the principle of proportionality, where the information required to be disclosed should be proportional to the size of the issuer and the burden the disclosure requirement places on it. As part of this, and to make it easier for smaller companies to raise capital throughout the European Union, a growth prospectus is introduced that is less burdensome, imposing less extensive requirements than a regular prospectus. Further, the threshold of capital to be raised before triggering the prospectus obligation will be increased, and there will also be room for even higher national thresholds. However, Sweden has decided to maintain its threshold at €2.5 million, which was the applicable threshold during the old prospectus regime.

The changes may have an effect on ICOs where tokens are considered to be transferable securities. First, ICOs by smaller organisations may fall under less burdensome prospectus requirements. Secondly, and on a more speculative note, the less burdensome prospectus rules may have an impact on the interpretation of whether ICOs fall within the Regulation at all, as the commonly presented argument – that it would be contrary to the intentions of the legislation to include virtual currency issuers in the prospectus regime owing to considerations regarding their size and the burden the current regime places on issuers – may no longer hold the same weight where there are less burdensome requirements specifically adapted to smaller issuers.

III BANKING AND MONEY TRANSMISSION

i Banking activities

Transmitting transactions using virtual currencies do not constitute regulated banking activities pursuant to the Swedish Banking Act, as payments using virtual currencies are not made through a general payment system. Whether institutions transmitting transactions using virtual currencies could potentially fall within the scope of the banking legislation in the future if payment systems using virtual currencies have grown to such an extent that they constitute general payment systems has not been established definitively. It is, however, notable that the Swedish legislator has discussed whether institutions transmitting payments using e-money could be subject to the banking legislation if the extent of such payments grew in commonality to such an extent as to be considered to be made in a general payment system.[9]

ii Payment services

Virtual currencies do not constitute funds as defined in the Swedish Payment Services Act implementing the Payment Services Directive (PSD) and PSD II.[10] Accordingly, services provided relating to virtual currencies do not currently constitute payment services regulated under the Payment Services Act.

9 Government Bill 2002/03:139, p. 195.

10 Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market and Directive (EU) 2015/2466 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, respectively.

iii Classification matters

Virtual currencies may constitute instruments of payment under Swedish law. Virtual currencies may constitute instruments of payment under Swedish law. Although the concept is relevant, as the classification of a virtual currency as an instrument of payment has certain legal repercussions, there is no legal definition of instruments of payment under Swedish law. However, the traditional view expressed in legal literature is that any instrument that is intended to be used to make payment, is not subject to transfer restrictions, and is of some value to the recipient may constitute an instrument of payment from a general law of obligations perspective.[11] The SFSA has also issued a general statement adopting this view of virtual currencies, that is, that they constitute instruments of payment.[12] However, the SFSA's statement cannot be interpreted as a statement that all virtual currencies meet the requirements to qualify as instruments of payment; it is submitted that the general definition of instruments of payment cannot be applied when determining which virtual currencies should be regarded as instruments of payment. Applying such a broad definition would, to be consistent in relation to instruments other than virtual currencies, have unreasonable consequences, as it governs the scope of entities subject to the anti-money laundering obligations described in Section IV. Therefore, a more nuanced assessment of individual virtual currencies should be made. Relevant factors in making the assessment may be similar to those used to identify whether a virtual currency is within the scope of MiFID II's definition of transferable securities: for example, whether the virtual currency is primarily intended to be used as a general means of payment, and the extent to which it is connected to a specific issuer (by way of rights to goods or services or by way of a possible increase in value, depending on the issuer's success). Currency tokens would be more likely to qualify as instruments of payment, owing to their intended purpose of functioning as such, while investment tokens and utility tokens would be less likely to qualify as instruments of payment. There is however, ultimately no guidance from the authorities or in Swedish legal literature that offers any indication as to how the assessment should be made.

Virtual currencies are not recognised as legal tender in the sense that there is any legal obligation to accept them as payment.[13]

IV ANTI-MONEY LAUNDERING

The Swedish Currency Exchange Act sets forth requirements that certain types of financial institutions comply with anti-money laundering provisions, despite not being obliged entities as relevant to determine the direct scope of applicability of the AML Act.

The Currency Exchange Act has recently been amended (effective as of 1 January 2020) to implement the EU's Fifth Anti-Money Laundering Directive (the Fifth AML Directive),[14]

11 Elgebrant, Emil, *Kryptovalutor: Särskild rättsverkan vid innehav av bitcoins och andra liknande betalningsmedel*, Wolters Kluwer Sverige AB, Stockholm, 2016, s. 40. See also Lindskog, Stefan, *Betalning*, Nordstedts Juridik AB, Stockholm, 2014, s. 70.

12 https://www.fi.se/sv/bank/sok-tillstand/valutavaxlare-och-annan-finansiell-verksamhet.

13 Chapter 5 Section 2 of the Swedish Central Bank Act (1988:1385).

14 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

which entered into force in July 2018. The change extends the scope of the Currency Exchange Act to include custodian wallet providers and providers of virtual currency exchange services. For the purposes of the Act:

a custodian wallet providers are providers of services to safeguard private cryptographic keys on behalf of their customers, and to hold, store and transfer virtual currencies; and

b providers of virtual currency exchange services are service providers who offer exchange services between virtual currencies and (1) Swedish or foreign fiat currency, (2) e-money (as defined in the Swedish E-money Act) or (3) other virtual currencies.

Crucially, the concept of a virtual currency for the purposes of the Currency Exchange Act is the same as in the Fifth AML Directive, namely a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and that can be transferred, stored and traded electronically. This definition will ordinarily include currency tokens and, to a lesser extent, investment tokens. However, utility tokens will generally not fall within the definition, as it has been stated in recitals to the Fifth AML Directive that the concept of virtual currencies is distinct from, for example, in-game currencies that can be used exclusively within a specific game environment.

Notably, the inclusion of providers of exchange services between virtual currencies goes beyond the requirements in the Fifth AML Directive, whereby Sweden has elected to impose a 'gold-plated' regime, imposing requirements beyond the minimum requirements under the common EU standard.

The Currency Exchange Act does not apply to a number of institutions that are subject to supervision pursuant to other legislation, such as credit institutions, investment firms, payment institutions and insurance companies.

An institution that falls under the scope of the Currency Exchange Act is required to apply for and obtain registration with the SFSA prior to commencing its regulated activities. To become registered, an institution applying for registration must show that there are grounds to assume that the operations will be conducted in a manner compliant with the applicable anti-money laundering legislation, and must also pass an ownership assessment procedure. The ownership assessment procedure prescribed by the Currency Exchange Act constitutes an assessment of whether any individual applying for registration under the Act has materially failed to adhere to his or her professional obligations or has been convicted of a severe criminal offence. In the case of legal entities applying for registration, this assessment shall be made in relation to all individuals in the entity's managing body and all holders of a qualifying holding in the entity. A qualifying holding is defined as a direct or indirect holding representing 10 per cent or more of the shares or votes in the legal entity, or both, or, in other cases, a holding that makes it possible to exercise significant influence over the management of the legal entity.

Virtual currency providers within the scope of the Currency Exchange Act must consequently comply with the rules of the AML Act, which include requirements to prepare a risk assessment, conduct customer due diligence, and monitor and report suspicious transactions.

V REGULATION OF EXCHANGES

Depending on the nature of an exchange, different legal regimes may be applicable. As described in Section IV, providers of exchange services between virtual currencies, between virtual and fiat currencies or between virtual currencies and e-money are subject to registration requirements and compliance with Swedish AML legislation. If an exchange is dealing with virtual currencies that are considered to be financial instruments, the requirements for operating such markets may be applicable and will require authorisation by the SFSA.[15] At the time of writing and as far as we are aware, no such operations are being conducted by any Swedish entity on a regulated or unregulated basis, although there have been initiatives in the market that have not succeeded in reaching the operational stage. As a consequence, it is difficult to assess how and to what extent the current legal regime regulating traditional exchanges should be adapted to an exchange of blockchain-based financial instruments. However, this difficulty should not per se be taken as an indication that the traditional exchange rules would not be applicable to an operator of a virtual currency exchange.

VI REGULATION OF MINERS

Virtual currency mining activities as such are not regulated under Swedish law. There are no licensing, registration or authorisation requirements specifically applicable to virtual currency mining activities. The SFSA has acknowledged virtual currency mining as a well-established form of activity within the fintech industry in Sweden.[16]

There are no restrictions under Swedish law prohibiting, limiting or otherwise stipulating any mandatory provisions specifically applicable to the sale of virtual currency mining machines in Sweden. Provided that such machines are not sold to consumers, the parties to any sale of virtual currency mining machines are at liberty to set out the terms applicable to such transaction at their own discretion.

Certain computer and software products are subject to authorisation requirements when exported from Sweden, pursuant to the Dual-Use Items Regulation,[17] which is directly applicable in all EU Member States. Virtual currency mining machines will generally not fall within the categories of computers and software subject to the Dual-Use Items Regulation. However, as the scope of the Regulation is, in part, purely capacity-based, it cannot be categorically ruled out that certain virtual currency mining machines may fall within the scope of the Regulation (e.g., machines exceeding a certain processing power or being specifically designed to be operable at extreme temperatures), and thus authorisation would be required to export these products from Sweden.

15 Chapter 2 Section 1 and Chapter 12 Section 1 of the Securities Market Act.

16 See the SFSA's report, 'The Authority's role in relation to innovations', of 1 December 2017: www.fi.se/contentassets/d3cd30fe473d4a7995f0c38209ddb7f1/myndighetens-roll-kring-innovationer.pdf.

17 Council Regulation (EC) No. 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items. The scope of the Dual-Use Items Regulation is set out in Commission Delegated Regulation (EU) 2017/2268 of 26 September 2017 amending Council Regulation (EC) No. 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfers, brokering and transit of dual-use items.

VII REGULATION OF ISSUERS AND SPONSORS

A public offering of coins or tokens of a virtual currency may constitute an alternative investment fund as defined in the Swedish Alternative Investment Fund Managers Act (the AIFM Act) to the extent that such an offering is used to raise capital from a number of investors with a view to investing such capital in accordance with a defined investment policy.[18] Similarly, as in relation to the definition of financial instruments discussed in Section II, offerings of virtual currencies will typically not constitute alternative investment funds, but owing to the broad range and varying nature of virtual currencies, it cannot be categorically ruled out that an offering thereof could constitute an alternative investment fund, in which case a number of obligations under the AIFM Act would apply.

VIII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

Swedish legislation criminalising, inter alia, fraud, embezzlement and money laundering is relatively modern in the sense that it criminalises such actions regardless of whether they relate to traditional money or virtual currencies. For example, neither fraud nor embezzlement require the transfer of any money. Rather, the relevant criterion is whether the action entails a profit or gain for the perpetrator and a loss for the victim, which can be the case even where the property embezzled or to which the fraud relates is a virtual currency. In a similar vein, money laundering is criminalised where the conducted action relates to money or any other property that is derived from criminal activities. Accordingly, the broad scope of the provisions covers actions taken to hide the criminal source of virtual currencies to the same extent as traditional money, as virtual currencies constitute property under Swedish law.

The Swedish legislator has acknowledged the increasing need to address crimes relating to virtual currencies and has, in addition to actively participating in the EU initiatives regarding the Fifth AML Directive (addressed in Section IV) and the Directive on combating fraud and the counterfeiting of non-cash means,[19] implemented an enhanced and strengthened coordination unit against money laundering and terrorism financing within the Swedish Police Authority.

IX LOOKING AHEAD

Riksbanken, the Swedish Central Bank, is currently assessing the possibility of establishing, and backing, an e-currency: the e-krona. Being backed by Riksbanken means that the e-krona would differ from typical cryptocurrencies. Notwithstanding this, Riksbanken stated in a September 2017 report that the e-krona may, depending on which technical solution is ultimately decided upon, constitute a virtual currency (subject, further, to how such a term is defined).[20]

Riksbanken notes in its report that the current regulatory framework will need to be adjusted to enable the establishment of the e-krona. It is therefore expected, if the initiative

18 Cf. ESMA's statement Reference No. ESMA50-157-828.

19 Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment.

20 See the Swedish Central Bank's report, Riksbanken e-kronaprojekt: Rapport 1, dated September 2017: www.riksbank.se/globalassets/media/rapporter/e-krona/2017/rapport_ekrona_uppdaterad_170920_sve.pdf.

materialises, that there will be relatively significant changes to the current legal status and Swedish regulation of e-currencies and virtual currencies. At the time of writing, the initiative to establish the e-currency is at a very early developmental stage, with the latest publicly announced step in the initiative being that Riksbanken will cooperate with a technical service provider during 2020 to develop the technical platform and payment methods in relation to the e-krona. It is expected that it will be several years before any specific legislative action is taken in relation to the launch of the e-currency, if the initiative is launched at all.

Chapter 26

SWITZERLAND

Olivier Favre, Tarek Houdrouge and Fabio Elsener[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

i Market size

Switzerland is the home of the crypto valley in Zug, near Zurich, and has an active community of enterprises working in the crypto space. While it is difficult to attribute a rank to Switzerland in the fast-moving global crypto community, Switzerland has taken the role of a pioneer in this area and is one of the most important jurisdictions for initial coin offerings (ICOs) and securities token offerings (STOs).[2] The recent choice of Switzerland as place of incorporation for the Libra Association is testament to the attraction of Switzerland as a home for innovative ventures in the blockchain business.

ii Legal framework

Switzerland has a favourable and attractive legal framework regarding crypto assets, although it does not have a separate legal framework for them. For cryptocurrencies, it already provides a regulatory framework that allows the issuance and trading of such assets, provided that anti-money laundering rules are complied with.

Switzerland is in the process of further improving the regulatory framework for asset tokens. The Federal Council started a consultation on 22 March 2019 proposing various amendments to Swiss laws to take into account the potential offered by the distributed ledger technology (the DLT Bill) that would introduce DLT rights as the digital alternative to certificated securities. DLT rights should be exclusively transferable through the blockchain. According to the DLT Bill, Switzerland would also introduce a new type licence category for trading venues, where DLT rights could be traded. The Federal Council proposes these improvements to the legal framework for distributed ledger and blockchain applications as amendments to current Swiss laws, without creating a separate regulatory regime for such technology. For further information, see Section X.

The Swiss Financial Market Supervisory Authority (FINMA) has repeatedly stated that it will not distinguish between different technologies used for the same activity: that is, it will apply the principle of 'same business, same rules' to any kind of new technology. FINMA

1 Olivier Favre and Tarek Houdrouge are partners and Fabio Elsener is a senior associate at Schellenberg Wittmer Ltd.

2 See https://ico.tokens-economy.com/statistics/ for a comparison of the ICO and STO activities per country.

adheres to this principle at present when applying Swiss financial market laws to crypto assets and blockchain-based applications and this will also apply going forward with the proposed new legislation on DLT rights.

iii Regulatory classification of tokens

On 16 February 2018, FINMA published guidance on how to apply Swiss financial markets laws in its guidelines regarding the regulatory framework for ICOs (the ICO Guidelines).[3] In the ICO Guidelines, FINMA clarifies how to classify cryptocurrencies and other coins or tokens (collectively with cryptocurrencies, tokens) or other assets registered on distributed ledgers under Swiss law.

According to the ICO Guidelines, FINMA distinguishes the following categories of tokens:

a payment tokens or cryptocurrencies, which are intended only as means of payment and that do not give rise to any claims against the issuer;

b utility tokens, which provide rights to access or use a digital application or service, provided that such application or service is already operational at the time of the token sale; and

c asset tokens, which represent an asset, for instance a debt or equity claim against the issuer or a third party, or a right in an underlying asset.

FINMA has further clarified that tokens may also take a hybrid form including elements of more than one of these categories. These hybrid tokens must comply cumulatively with the regulatory requirements applicable to each relevant token category. FINMA acknowledges that a token's classification may change over time. For the purpose of assessing the regulatory implications of an ICO, the moment of the token issuance is relevant. However, the initial classification may change post-ICO. In the event of any secondary market trading activity with tokens, their classification in the moment of the relevant trading activity must be taken into account.

Payment tokens do not qualify as legal tender or other means of payment under Swiss law. However, the Swiss Federal Council has clarified that payment tokens may be used as private means of payment if the parties to a transaction agree on the use of payment tokens as the applicable means of payment for such a transaction. In addition, the issuance of payment tokens requires compliance with the Swiss anti-money laundering rules (see Section V).

iv Enquiries to FINMA

Notwithstanding the guidance provided by FINMA, given that this field is new and the structures of token offerings are always evolving, regarding the application of the ICO Guidelines in real-life projects, it is normal practice to seek a confirmation from FINMA to the effect of obtaining a no-action comfort from the regulator.

FINMA offers the possibility to file such no-action enquiries in order to confirm the regulatory interpretation.

3 FINMA, Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs) (available at https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en).

II SECURITIES AND INVESTMENT LAWS

i Relevance for asset tokens and certain types of utility tokens

Swiss securities laws are relevant for the issuance of asset tokens or any hybrid form of tokens involving the functionality of asset tokens (e.g., a utility token regarding the use of a platform that is not fully developed).

However, payment tokens and utility tokens that do not represent any claims against an issuer or a third party are not subject to Swiss securities laws, as they do not represent any rights.[4] Such payment tokens and utility tokens should be classified as intangible digital assets sui generis for the time being.[5]

ii Issuance of tokens representing rights against an issuer or a third party

To the extent that asset tokens or utility tokens representing any claims against an issuer or third parties are governed by Swiss law, according to the view expressed by FINMA as well as according to the prevailing view in the Swiss market, these tokens should qualify as uncertificated securities according to Article 973c CO.[6] The creation of these uncertificated securities requires a decision from the competent corporate body as well as the registration of the first holders of the uncertificated securities in a register held by the issuer. This register is not subject to any form requirements, and therefore it is possible to qualify the distributed ledger as such a register.

If the token sale involves a financial institution pursuant to Article 4(2) of the Swiss Federal Intermediated Securities Act (FISA) acting as custodian for intermediated securities, the tokens can be issued as intermediated securities.[7] The advantage of creating intermediated securities would be that the entitlements in the tokens could be transferred by book-entry in the custody accounts of the custodians involved according to the rules of the FISA. However, given that token sales are usually structured in a way that does not involve a securities custodian, we will not cover the further requirements to be taken into account for the issuance of tokens in the form of intermediated securities.

iii Transfer requirements for tokens

Under Swiss law, payment tokens and utility tokens that do not represent any claims against an issuer or third parties can be validly created and transferred in accordance with the terms of the respective distributed ledger. A transfer can therefore be validly made by executing a transaction between two wallets.

---

4 Swiss LegalTech Association, Regulatory Task Force Report, 27 April 2018, p. 25 (available at http://www.swisslegaltech.ch/wp-content/uploads/2018/05/SLTA-Regulatory-Task-Force-Report-2.pdf).

5 Cf. Federal Council report, Legal framework for distributed ledger technology and blockchain in Switzerland (footnote 3) pp. 54 and 66; Federal Council, Report on virtual currencies, 25 June 2014, 7 (available at http://www.news.admin.ch/NSBSubscriber/message/attachments/35361.pdf). A clarification of the legal qualification of cryptocurrencies has been announced (cf. Federal Department of Finance, press release, 5 July 2017, available at https://www.efd.admin.ch/efd/en/home/dokumentation/nsb-news_list.msgid-67436.html).

6 Swiss LegalTech Association, Regulatory Task Force Report (fn 4), p. 26; ICO Guidelines, p. 4; see also Eggen, 'Was ist ein token?', AJP 2018, p. 558 et seqq., p. 563 et seq.; Blockchain Taskforce, position paper on the legal classification of ICOs, April 2018, p. 8 et seq. (available at https://blockchaintaskforce.ch/wp-content/uploads/2018/06/Blockchain-Taskforce-White-Paper-Annex1.pdf).

7 Swiss LegalTech Association, Regulatory Task Force Report (footnote 7), p. 26 et seq.

However, asset tokens and utility tokens representing enforceable rights against an issuer or a third party require, in addition to a valid transfer on the relevant distributed ledger, that the rights represented in such tokens are validly created and transferred to the transferee. Depending on the types of rights represented in the tokens, this could be a written form requirement for the transfer of such rights under Swiss law. Regarding the transfer of tokens representing uncertificated securities (see Section II.ii), the rules of assignments pursuant to the CO must currently be complied with, which require a declaration of assignment in writing by the assignor. To the extent that the tokens were registered with a financial institution acting as securities custodian, such securities could be issued as intermediated securities under the FISA, and it would be sufficient to transfer the securities by way of book entry between the custodians involved in the transaction without a transfer by way of an assignment. However, on the basis that no custodians are involved, the written form requirements for a transfer of uncertificated securities must be complied with for a valid transfer.

Under Swiss law, a written form requires that the parties must either provide a wet-ink signature, which can be delivered through a scan, or a certified electronic signature according to Article 14(2bis) CO. We are not aware of any distributed ledger that would currently support such certified electronic signatures; therefore, a written form requirement can, to date, not be substituted by a transaction of tokens on a distributed ledger.

As the transfer of uncertificated securities is subject to a written form requirement, to validly transfer the rights attached to asset tokens and utility tokens representing exercisable rights against an issuer or a third party under Swiss law, a work-around is needed. One solution is the use of terms and conditions of the tokens specifying that the transfer of such tokens to a new token holder shall be construed as a transfer of the contractual relationship in which the new token holder assumes the entire contractual position from the old token holder. Such transfers may be made in the form of a three-party agreement between the issuer, the old and the new token holder. For the purpose of this transfer, it could be argued that all participants of a distributed ledger, including the old and new token holder and the issuer, implicitly agree by participating in the distributed ledger to such a method of transferring tokens. However, it would be prudent to provide, at least, that the issuer must keep a record of the current token holders and acknowledges any transfer to a transferee before any transferee may exercise any rights resulting from the tokens.

With regard to the DLT Bill, the Federal Council proposed the introduction of DLT rights as a new type of right that may be created with a registration on a distributed ledger and that could be transferred according to the terms of the respective distributed ledger without having to meet further requirements of Swiss law. Asset tokens or utility tokens could be issued as DLT rights (see Section X).

iv Classification of tokens as securities

According to Article 2(b) of the Financial Market Infrastructure Act of 19 June 2015 (FMIA), securities are certificated or uncertificated securities, derivatives or intermediated securities, which are standardised and suitable for mass trading. According to Article 2(1) of the Financial Market Infrastructure Ordinance of 25 November 2015, standardised and suitable for mass training means, in this context, that the instruments are offered for sale publicly in the same structure and denomination, or that they are placed with 20 or more clients under identical conditions.

FINMA has clarified in the ICO Guidelines that it will apply these rules in connection with tokens constituting uncertificated securities (see Section II.i) as follows:[8]

a Payment tokens do not qualify as securities given that they are designed to be used as means of payment according to FINMA. Payment tokens cannot fall under the definition of securities as they do not represent any rights that are exercisable against the issuer or third parties.

b Utility tokens can qualify as securities if the platform where they can be used is not operationally ready at the time of the token sale, or if the tokens represent rights that may be enforced against the issuer or a third party. These utility tokens are deemed to have an investment purpose. FINMA further clarified that a case-by-case analysis is needed to clarify whether or not a utility token can be used for its intended purpose. In particular, it specifies that proof of concepts or beta versions of platforms or applications on which the utility tokens cannot (yet) be used would not suffice to fall outside of the definition of securities for the purposes of the FMIA. However, on the basis that the qualification of tokens may change over time, it is possible that utility tokens qualifying as securities will fall outside of this definition once the platform where the tokens shall be used becomes fully functional for its intended purpose.

c Asset tokens qualify as securities provided that they have been offered publicly or to 20 or more persons for sale.

FINMA has stated that any enforceable rights of investors to receive or acquire tokens in the future resulting from a presale, for instance under a simple agreement for future tokens, qualify as securities if the rights have been offered publicly or on identical terms to more than 20 persons. On the other hand, the rights issued in the context of a presale do not constitute securities if the terms used in the presale are not standardised or different terms are used with each investor: for example, by varying the amount of rights, the pricing or any lock-up provision.

v Prospectus requirement

Regardless of the classification of tokens as securities, in respect of any tokens constituting a digital representation of rights that are exercisable against an issuer, the question arises of whether the tokens are subject to a prospectus requirement under the CO. This would, for instance, apply if the rights forming part of the tokens are classified as equity or debt instruments.

This prospectus requirement will be replaced by a new prospectus regime that aims to align the Swiss disclosure requirements to a certain extent with those applicable in the EU. The new prospectus rules will apply in an uniform manner to all public offerings of securities pursuant to the Swiss Financial Services Act (FinSA). They are scheduled to enter into force in January 2020.

In addition, as regards financial instruments offered to retail investors, the FinSA will introduce an obligation to prepare a key investor document as an additional disclosure document in a similar way as currently applicable in the EU pursuant to the Packaged Retail

8 Cf. Section 3.1 of the ICO Guidelines.

and Insurance-based Investment Products Regulation. This new obligation will also apply to certain types of tokens qualifying as financial instruments (e.g., asset tokens with the economics of a structured product or a derivative).

vi Regulatory implications of classification of tokens as securities

If tokens qualify as securities, they are subject to the regulatory framework of the Stock Exchanges and Securities Trading Act of 24 March 1995 (SESTA) and the implementing Stock Exchanges and Securities Trading Ordinance of 2 December 1996. According to this regulatory framework, a licence as a securities dealer is required for any brokerage activities on behalf of clients (other than institutional clients) regarding such tokens, any market-making activities in respect towards such tokens, underwriting such tokens and – provided that the tokens qualify as derivatives – issuing these tokens.[9] A licence requirement is in each case triggered if these activities are executed on a professional basis. With the entry into force of the Financial Institutions Act (FinIA) as of 1 January 2020, the licence category of securities dealers will be replaced by the licence category of securities houses. However, in terms of the substance of the regulation, the current regulatory requirements will not change.

The qualification of tokens as securities has implications on the licence requirements under the FMIA for any secondary trading platform where such tokens can be traded.

III LAWS ON COLLECTIVE INVESTMENTS

As regards any investments in tokens through collective investment schemes or funds or in regard to the issuance of tokens representing units in collective investment schemes, the rules of the Swiss Collective Investment Schemes Act of 23 June 2006 (CISA) and its implementing ordinances must be taken into account. For the purposes of the CISA, a collective investment scheme is a pool of assets raised from investors for the purpose of being invested collectively managed on behalf of the investors. The regulation of the CISA applies irrespective of the legal structure that has been chosen for the collective investment scheme or fund.

As a result, the issuance of tokens, as well as any business activity in relation to tokens (regardless of their classification) by which assets accepted from clients for investment purposes are pooled (i.e., there is no segregation of the investments for each investors), or where the clients' assets are managed by a third party on behalf of those clients, could be subject to the requirements of the CISA and – as of 1 January 2020 – the FinIA, and must be analysed from the perspective of the Swiss regulation of collective investment schemes.

Commercial undertakings generally do not fall within the scope of the CISA. However, it is only possible to draw the line between a commercial undertaking and a collective investment scheme on a case-by-case basis.

IV BANKING REGULATION

According to the Swiss Banking Act of 8 November 1934 (SBA), a banking licence requirement is triggered if a company conducting primarily a financial activity accepts deposits from the public (i.e., from more than 20 persons) or publicly advertises this activity.

9 Cf. Article 3 Stock Exchanges and Securities Trading Ordinance.

According to the Swiss Banking Ordinance of 30 April 2014 (SBO), entering into any liabilities would generally qualify as a deposit-taking activity, unless one of the exceptions defined in Article 5(2) and (3) SBO applies.

In the context of token sales, the most relevant exemptions are the following:

a to the extent that the liabilities are debt securities issued as standardised products suitable for mass trading and are documented with an offering prospectus including the information required under the CO, the liabilities do not qualify as deposits; and

b to the extent that the liabilities arise from client funds held on settlement accounts with securities dealers, asset managers or similar financial intermediaries, provided that such funds are used to settle client transactions, no interest is paid on the funds and – except for accounts with securities dealers – the settlement occurs within 60 days at the latest.

Further, Swiss law provides for a sandbox exemption pursuant to Article 6(2) SBO. According to this exemption, the acceptance of deposits from the public (i.e., from more than 20 persons) up to a maximum amount of 1 million Swiss francs is permitted without a banking licence, provided that no interest income is generated with the deposited amounts and the investor has been informed before accepting the deposit that the accepting person or entity is not subject to prudential supervision by FINMA, and that the investments are not protected by any deposit protection scheme.

Moreover, entities accepting deposits from the public up to a maximum of 100 million Swiss francs, provided that these deposits are not reinvested and they are not interest-bearing, may request a banking licence 'light'. Compared to a full banking licence, certain carve-outs apply regarding organisation, risk management, compliance, the qualifications of the regulatory auditor and the capitalisation requirements. The banking licence light has been available since 1 January 2019. It may be an interesting option for entities active in the crypto space that intend to take deposits from the public in an amount below the cap of 100 million Swiss francs.

When providing storage services regarding tokens, the following question arises: under what circumstances does the activity require a banking licence or a banking licence light? This would be relevant when the storage provider can dispose of the private keys of its clients. In this event, a banking licence may be needed where the crypto assets are held in a way that does not allow a client to set aside the crypto assets in the insolvency of the custodian.

With regard to brokerage services provided in respect of tokens, this activity could be subject to a banking licence if the service provider accepts fiat currencies or tokens on own accounts respectively public keys in connection with such services. In this event, the service provider would need to rely on the settlement account exemption mentioned above. However, this exception is not available to cryptocurrency traders that execute an activity comparable to foreign exchange traders (i.e., that expose their clients to similar bankruptcy risks as foreign exchange traders do).

V ANTI-MONEY LAUNDERING

i Applicable rules

Under Swiss law, anti-money laundering (AML) regulation consists of the Swiss Anti-Money Laundering Act of 10 October 1997 (AMLA) and the Anti-Money Laundering Ordinance of 11 November 2015 (AMLO). The AMLA applies, inter alia, to financial intermediaries. Besides entities subject to prudential supervision, in brief, anyone accepting, holding or

depositing assets belonging to other persons or assisting in the investment of such assets on a professional basis qualifies as a financial intermediary according to Article 2(3) AMLA. Further, the AMLA contains a non-exhaustive list of activities that are considered financial intermediation. In the context of ICOs and tokens, the issuance of means of payment that cannot be used exclusively with the issuer,[10] providing services related to payment transactions in the form of money and asset transmission services,[11] and money exchange services,[12] are relevant financial intermediation activities.

A financial intermediary in the sense of the AMLA must be affiliated with an authorised AML self-regulatory organisation (SRO). Further, a financial intermediary has to comply with the obligations defined in the AMLA, including, without limitation, identification and know your customer (KYC) obligations relating to the contracting party and its beneficial owner, and has to file reports to the Money Laundering Reporting Office in cases of suspected money laundering or terrorism financing.

ii ICOs

Depending on the classification of the tokens to be issued within an ICO, the issuance can qualify as financial intermediation activity. FINMA provides clarity in its ICO Guidelines on this matter, as outlined below.

a The issuance of payment tokens is classified as an issuance of means of payment and therefore constitutes a financial intermediation activity pursuant to the AMLA.

b The issuance of utility tokens that comprise some form of payment function on the designated application or platform, for example the ability to use the utility tokens to pay for services used on such platform, usually qualifies as issuance of means of payment and therefore constitutes a financial intermediation activity pursuant to the AMLA. However, the issuance of utility tokens does not qualify as financial intermediation if a utility token does not have any form of payment function or if the payment function is exceptionally considered as an ancillary function of the utility tokens.[13] To benefit from such an exception, it is required that such utility tokens' main purpose is to provide access rights to a non-financial application, that the entity providing the payment functionality is also the entity operating the non-financial application and that the access to the non-financial application could not be granted without including the ancillary payment functionality embedded in the utility token. However, note that FINMA applies this exception very restrictively, and in practice, any utility token with some sort of payment function is considered as a financial intermediation within the scope of the AMLA.

c The issuance of asset tokens does not qualify as financial intermediation activity pursuant to the AMLA, provided that the asset tokens are classified as securities, and provided further that they are not issued by a bank, securities dealer or certain other prudentially supervised entities. However, in practice, issuers of asset tokens are often

10 Cf. FINMA Circular 2011/01, Financial intermediation according to AMLA, n 64.

11 Cf. Article 4(2) AMLO.

12 Cf. Article 5(1)(a) AMLO.

13 ICO Guidelines, Section 3.6; FINMA Circular 2011/01, Financial intermediation according to AMLA, n 13 et seq.

required to conduct some KYC and identification processes on a voluntary basis owing to the compliance requirements of the banks to which the proceeds of the ICO will be transferred.[14]

The issuance of rights to acquire tokens in the future within a pre-ICO does not constitute a financial intermediation activity, provided that the issuer is not a bank, securities dealer or certain other prudentially supervised entities. However, the subsequent issue of tokens that qualifies as issuance of a means of payment under the AMLA (i.e., payment tokens and, subject to the mentioned exceptions, utility tokens) to pre-ICO investors qualifies as financial intermediation. In consequence, the obligations arising from the AMLA are triggered in the moment of issuance.

FINMA specifies in connection with ICOs that fall within the scope of the AMLA that the obligations arising under the AMLA (e.g., KYC) can be outsourced to financial intermediaries in Switzerland that are affiliated with an SRO or under FINMA supervision, provided that any funds from the ICO are accepted via such financial intermediary: that is, any tokens or fiat currencies paid by investors have to be transferred to the public keys or accounts of the outsourcing partner before being transferred on to the relevant issuer.

iii Exchange and intermediation services

Exchanging fiat currencies against tokens or vice versa or exchanging two different tokens constitutes a financial intermediation activity subject to the AMLA.

If a service provider offers the exchange services directly (i.e., acts as an exchanging counterparty to its clients), this activity qualifies as money exchange under the AMLO. For these services, a de minimis threshold of 5,000 Swiss francs applies, and transactions below this threshold are exempted from KYC or identification obligations under the AMLA.[15]

If a service provider offers exchange services with the involvement of a third party (e.g., an exchange platform for tokens), or if the service provider intermediates services relating to the transfer or exchange of tokens or fiat currencies and is involved in the payment process, such services qualify as money and asset transmitting services pursuant to Article 4(2) AMLO and the service provider qualifies as a financial intermediary under the AMLA.

iv Storage services

A storage services provider qualifies as a financial intermediary if it has the power to dispose of the private keys of the stored tokens (custodian wallets). Further, this activity could trigger a banking licence requirement (see Section IV).

14 Cf. Swiss Bankers Association, SBA guidelines on opening corporate accounts for blockchain companies, September 2018 (available at https://www.swissbanking.org/library/richtlinien/leitfaden-der-sbvg-zur-eroeffnung-von-firmenkonti-fuer-blockchain-unternehmen/?set_language=en).

15 Cf. Article 51(1)(a) FINMA Anti-Money Laundering Ordinance for entities that are subject to FINMA supervision or the relevant regulations of the SROs.

VI REGULATION OF EXCHANGES

i Tokens qualifying as securities

Exchanges for securities are regulated under the FMIA, which distinguishes between a stock exchange, a multilateral trading facility (MTF) and an organised trading facility (OTF). Stock exchanges and MTFs are trading venues allowing for the multilateral trading of securities, where trades are entered into on the basis of non-discretionary rules. Stock exchanges, as opposed to MTFs, further require a listing of securities, that is, a formal application process in order to be admitted on the stock exchange. Stock exchanges and MTFs qualify as financial infrastructures and require a FINMA licence according to Article 4 FMIA.

An OTF is a trading facility providing either for a multilateral trading of securities according to discretionary rules or of other financial instruments according to discretionary or non-discretionary rules, or for bilateral trading between the participants and the operator of the OTF. According to Article 43 FMIA, OTFs can only be operated by supervised banks, securities dealers, stock exchanges or MTFs that are authorised by FINMA to operate an OTF. Note that the term other financial instruments comprises in particular derivative instruments that do not qualify as securities.

A trading venue for asset tokens and utility tokens that qualify as securities would need to be licensed as a stock exchange or MTF or, if the trading activity qualifies as the operation of an OTF, the operator would require a licence as a bank or securities dealer with an approval from FINMA to operate an OTF.

ii Other tokens

In regards to the regulation of exchanges for payment tokens and utility tokens that do not qualify as securities, there are no licence requirements under Swiss law to operate such business in addition to ensuring compliance with Swiss AML requirements (see Section V). However, as the operation of such exchanges usually implies the acceptance of fiat currencies or such tokens on accounts or public keys of the exchange operator, a banking licence requirement could be triggered as an acceptance constituting an acceptance of deposits from the public (see Section IV).

Similar to the provision of brokerage services, an exchange may benefit from the exemption for settlement accounts if the clients' funds accepted on own accounts or public keys are used solely for the execution of trades on the exchange, are not interest-bearing and are transferred on within 60 days. Further, this exemption would only be applicable if the clients were not exposed to an increased bankruptcy risk similar to clients of a foreign exchange trader (see Section IV).

Further, an exchange can benefit from the sandbox exception pursuant to Article 6(2) SBO if fiat currencies and tokens with a value of less than 1 million Swiss francs are accepted from the exchange participants and if the participants are informed of the absence of any prudential supervision over the exchange operator and any protection from a deposit protection scheme.

In any event, the operation of an exchange for tokens constitutes a money and asset transmitting service pursuant to Article 4(2) AMLO. Therefore, an exchange operator qualifies as a financial intermediary that is, in particular, subject to the affiliation obligation with an SRO or a licence requirement by FINMA as a financial intermediary.

VII REGULATION OF MINERS

i Role of mining in virtual currency

In an unrestricted decentralised network (such as the Ethereum or Bitcoin blockchain), the mining of the native tokens of the relevant distributed ledger, usually a payment token, plays an essential role in the record-keeping of transactions on the distributed ledger as there is no central authority monitoring transactions. To secure financial transactions and ensure that there is no fraud, the miners (or crypto miners) must verify transactions and add them to the distributed ledger.

The work of the miners is open to the entire ecosystem of the distributed ledger: everybody can potentially participate on this network and mine tokens. For each block of transactions, miners use mathematical protocols to verify transactions and validate them before sharing the result across the entire network. This process creates virtual currency as the miners are awarded with new virtual currency for their mining activity.

ii Regulatory framework

There is currently no specific legislation addressing the regulatory status of miners in Switzerland. Mining of tokens (self-issuance of tokens) does not trigger a licence requirement under Swiss law provided that the miner does not perform any activity falling within the scope of the regulated activities described in Sections II to VI.

The self-issuance of tokens qualifying as securities is generally not subject to a licence requirement as a securities dealer under the SESTA. This conclusion also holds true in the unlikely event that the tokens would qualify as derivatives provided that there is no offer of these derivatives to the public on a professional basis.

iii FINMA scrutiny and enforcement proceedings in connection with mining

FINMA generally has a favourable approach towards blockchain technology, but it monitors cautiously all market participants to ensure that the Swiss blockchain network remains free of fraud, in particular in the context of ICOs. It regularly highlights the risks involved for investors, and is committed to take actions against ICO business models violating or circumventing regulatory laws.

The most recent example is the launch in July 2018 of enforcement proceedings by FINMA against a Swiss mining company owing to evidence of beach of regulatory laws. More precisely, the result of the proceedings led by the FINMA concluded that the company unlawfully received public deposits on a commercial basis in the context of an ICO.[16] At the time of writing, this mining company is in liquidation.

As the regulatory status of activities in connection with the mining of tokens may raise some issues, a no-action letter from FINMA, for example with regards to specific activities of a miner, is always advisable to obtain legal certainty that the contemplated activity complies with all regulatory laws (see Section II.iv).

16 https://www.finma.ch/en/news/2019/03/20190327---mm---envion/.

VIII REGULATION OF ISSUERS AND SPONSORS

i Issuers

In regards to the legal form for issuers of tokens, two types of forms are generally used: a foundation and a joint-stock corporation.

A foundation offers the complete independence and control of the board of the foundation as there are no shareholders. However, its assets must be used in line with the purpose of the foundation as stated in the deed of foundation. Therefore, the distribution of profits is limited to that purpose and it is not possible to distribute profits to the founders. In addition, every foundation is further subject to governmental supervision. Note that certain tax exemptions are available for foundations or stock corporations with public or non-profit purposes alike. However, the conditions for obtaining such exemptions are very restrictive and are usually not met by entities pursuing an ICO.

In the context of an ICO, to the extent that there is, at least partially, a commercial purpose, and the issuer is not pursuing a non-for-profit purpose, the legal form of the Swiss foundation is most of the time not suitable. Its rigid structure does not allow for the flexibility that is generally needed, in particular as the founders have no ownership or any other control over the foundation's assets or funds and have no legal means to influence the foundation's conduct of business. Instead, a joint-stock corporation is the more suitable type of corporate form for issuers of ICOs.

An issuer of an ICO incorporated as a joint-stock corporation must have – unless it is incorporated with a contribution in kind – a paid-in capital of 50,000 Swiss francs (with a minimum share capital of 100,000 Swiss francs) deposited with a Swiss bank. However, following the incorporation, there is no restriction as to the place where the account is held. The issuer may also have an account with a foreign bank.

The issuer must comply with the regulatory requirements, to the extent applicable to the issuer, as set out in Sections II to VI.

Depending on the classification of the tokens issued, an issuer of tokens may be subject to the AMLA if it carries out financial intermediation activities (see Section V.ii). In the context of ICOs and tokens, the issuance of means of payment that cannot be used exclusively with the issuer, the provision of services related to payment transactions in the form of money and asset transmitting services or money exchange services are, for example, financial intermediation activities (see Section V).

ii Sponsors

As long as there is no activity performed falling into the scope of the regulated activities described in Sections II to VI, the sponsorship of tokens – including the marketing, publicity and promoting of tokens – is currently not subject to licence requirements in Switzerland.

However, this is subject to the following:

a licence requirement under the SBA or the SESTA (or, from 1 January 2020, with the FinIA): if the sponsored company has a foreign regulatory status as a bank or securities dealer because it has the relevant regulatory status under the foreign legislation, it carries out activities qualified as banking or securities dealing under Swiss legislation or it uses the terms bank or securities dealer in its company name, any marketing activities in or from Switzerland for such foreign bank or broker-dealer – provided that such

activities are performed by individuals engaged in Switzerland, on a professional and permanent basis – may bring the foreign bank or broker-dealer within the scope of a FINMA branch office or representative office licensing requirement; or

b prospectus requirement: the public offering of tokens, if they qualify as equity or debt instruments, may be subject to the prospectus requirement in accordance with the CO or, from 1 January 2020, with the FinSA.

IX TAX

The tax consequences of an ICO or token sale basically depend on whether the sold tokens qualify as debt or equity instruments. It is becoming apparent that the token categories developed by FINMA in its ICO Guidelines will also be relevant for tax purposes. Hence, the taxation of tokens depends primarily on whether they qualify as payment tokens, utility tokens or asset tokens. In this context, from a tax point of view, no hybrid tokens will probably exist. Furthermore, there is currently no relevant case law, no uniform tax practice and no unanimous doctrine, which is why the following explanations are to be taken with caution. So far, some tax authorities have published leaflets on the tax treatment of tokens. However, these generally only concern the income and wealth tax treatment at the investor level (if the investor is liable to tax in Switzerland), but not the tax treatment at the company or issuer level. Therefore, it is generally advisable to consult a Swiss tax adviser before an ICO or token sale. In many cases it will be also advisable to obtain an advance tax ruling from the competent tax authority to mitigate any adverse tax consequences.

A token sale can have tax consequences, as outlined below.[17]

i Corporate income tax

The corporate income tax (CIT) treatment of tokens depends on their legal nature. Proceeds from the sale of equity-based asset tokens should qualify as CIT-neutral capital contributions. Proceeds from the sale of debt-based asset tokens can be compared with taking out a loan that is not subject to CIT. In contrast, profits generated by the sale of utility tokens qualify as taxable income basically subject to CIT. However, in most cases the issuer will be obliged to use these proceeds for a specific product development. This obligation is likely to justify the recognition of a provision in the amount of the proceeds collected, which will reduce the taxable income accordingly. Thus, the token sale has no direct CIT consequences. The provision must be reversed in the course of product development. This reversal leads to taxable income, which is offset against the current expenses for product development. If the product development is not carried out by the issuer itself, but is outsourced to a third party, the tax authorities expect a minimum profit of cost plus 5 to 10 per cent to be left with the issuer, which implies that more provisions have to be released than actually necessary. Any profit of the issuer is subject to CIT at the federal, cantonal and municipal levels. Depending on the registered office of the issuer, the combined effective income tax rates currently range

17 The tax consequences described in this section are limited to those for issuers in connection with token sales. Any tax consequences for investors or employees (e.g., due to the allocation of tokens) are not addressed for space reasons. In addition, we have focused on the taxation of utility tokens and asset tokens.

between 12 and 24 per cent.[18] Finally, it should be noted that it will generally not be possible for the issuer to obtain an exemption from CIT, since an exclusively non-profit purpose is hardly ever pursued with a token sale.

ii Capital tax

Capital tax is only levied at the cantonal and municipal levels, and not at the federal level. It is based on the corporation's taxable equity. Proceeds from the sale of debt-based asset tokens are therefore not subject to capital tax, whereas proceeds from the sale of equity-based asset tokens are subject to capital tax. Gains from the sale of utility tokens are also subject to capital tax because such gains are ultimately recognised in the company's equity. The ordinary capital tax rates currently vary between 0.001 and 0.525 per cent, depending on the registered office of the issuer. Some cantons offset CIT against capital tax (i.e., capital tax is not levied in the amount of CIT).

iii Issuance stamp tax

Equity contributions to Swiss corporations are basically subject to issuance stamp tax of 1 per cent on the fair market value of the contribution. Accordingly, issuance stamp tax must be considered in particular for equity-based asset tokens. In contrast, it should not be possible to levy the issuance stamp tax on other tokens as there is typically no equity contribution.

iv Securities transfer tax

Securities transfer tax is levied on the transfer of taxable securities if a Swiss securities dealer in the sense of the Swiss Stamp Duty Act is involved in the transaction as a contracting party or as intermediary. Securities transfer tax amounts to 0.15 per cent on securities issued by a Swiss resident. Taxable securities include, but are not limited to, shares and bonds. The tokens will generally not qualify as shares but may qualify as bonds for securities transfer tax purposes. This applies in particular to debt-based asset tokens. However, primary market transactions, such as issuance and redemption, are not subject to securities transfer tax. Therefore, securities transfer tax is to be considered in particular at a later sale of the tokens by the investors.

v Withholding tax

The sale of equity-based asset tokens is not subject to withholding tax (WHT). However, any distributions made to the holders of those equity-based asset tokens are subject to WHT of 35 per cent. In the case of distributions on utility tokens in the form of a profit or revenue share, a case-by-case examination must be made as to whether WHT may have to be levied on these distributions as well. Distributions on debt-based asset tokens may also be subject to WHT if the asset token qualifies as a bond for WHT purposes.

18 On 19 May 2019, the Swiss public voted for the adoption of the Federal Act on Tax Reform and Financing of the AHV (TRAF). The main goal of the TRAF is to abolish the tax privileges applying to holding companies, domicile and mixed companies on cantonal level, and to principal companies and Swiss Finance Branch-structures on federal level. The cantons will have to adapt their legislation by 1 January 2020. At the same time, most cantons intend to take further complementary measures, which are, in particular, reductions in their corporate income tax rates. Hence, according to the current planning status, from 1 January 2020 the maximum CIT rates will be around 19 per cent.

vi Value added tax

Revenues from the sale of goods and services within Switzerland and Liechtenstein are generally subject to value added tax (VAT) at the standard rate of 7.7 per cent. The sale of pure payment tokens is considered an exchange of payment means and not a sale of goods and services. Accordingly, such a sale is not subject to VAT. The sale of asset tokens is also exempt from VAT. In contrast, the sale of utility tokens is regarded as a taxable service, which is why VAT of 7.7 per cent must be levied on the utility tokens sold to Swiss and Liechtenstein investors. The sale of utility tokens to foreign investors, on the other hand, is not subject to VAT, as this regularly qualifies as a non-taxable export of services.

X LOOKING AHEAD

As mentioned in Section I, if adopted as currently proposed, the DLT Bill will introduce DLT rights as a new type of asset representing rights registered on distributed ledgers that may be exercised against the issuer or third parties (e.g., asset tokens or utility tokens). The DLT rights are designed to be the digital equivalent of certificated securities, provided that the right is linked to a DLT registration – as opposed to a certificate – in a way that it may not be exercised or transferred outside such distributed ledger. Any rights that could be issued as certificated securities may be issued as DLT rights, for example (1) fungible contractual claims (e.g., debt claims), (2) non-fungible contractual claims (e.g., rights arising from a licence agreement), (3) membership rights that can be issued as certificated securities (e.g., rights of shareholders of joint-stock corporations) and (4) rights in rem that can be issued as certificated securities (e.g., mortgage certificates). However, DLT rights could not constitute: cryptocurrencies and other tokens that do not represent any rights against the issuer or a third person; or property rights in movable assets or real estate.

According to the DLT Bill, DLT rights would be issued by:

a entering into an agreement regarding the registration of the DLT rights on the distributed ledger between the issuer and the first holder of the DLT rights (the Registration Agreement), which can also be incorporated within the general terms and conditions of a DLT right; and

b a registration of the DLT rights on the distributed ledger. Pursuant to the terms of the Registration Agreement, the DLT rights may only be exercised and transferred via the distributed ledger.

For these purposes, the distributed ledger must meet the following requirements:

a the terms of the DLT rights, the terms of operation of the distributed ledger and the terms governing the registration must be recorded on the distributed ledger or must be accessible through the distributed ledger;

b it operates according to the terms agreed in the Registration Agreement by applying state-of-the-art processes regarding security and integrity of the data recorded on the distributed ledger; and

c the parties have to be able to consult the entries in the distributed ledger relating to the DLT rights and the information pursuant to point (a), above.

DLT rights can only be transferred by a transfer of the relevant tokens on the distributed ledger, namely by sending the tokens from the public key of the transferor to the public key of the transferee. The transfer would occur as soon as the tokens are registered on the public key of the transferee according to the rules of the distributed ledger.

Furthermore, the DLT Bill would amend:

a Swiss bank insolvency rules, in a way that allows clients of banks to set aside cryptocurrencies and DLT rights held on public keys by the bank for the client in the insolvency of the bank, provided that the cryptocurrencies or DLT rights are held on a segregated basis; and

b the rules of the Swiss Debt Collection and Bankruptcy Act applicable to insolvency proceedings, generally to the effect that cryptocurrencies and DLT rights held by a custodian that is not regulated as a bank on public keys for a client can be set aside in insolvency proceedings applicable to the custodian, provided that the cryptocurrencies or DLT rights are held on a segregated basis.

These proposals will effectively remedy the hurdle of a written form for the transfer of asset and utility tokens representing rights against the issuer or a third party (see Section II.iii). The proposed segregation right in relation to tokens will improve the protection of investors in case of bankruptcy of a service provider (e.g., custodian wallet providers).

As currently proposed, the DLT Bill would also introduce a new licence category for trading platforms, where DLT rights can be traded. The current types of licences for securities trading (i.e., stock exchanges and MTFs) are not suitable to trade DLT rights. They are only accessible by regulated participants and not by retail clients directly. Furthermore, they require the involvement of separate central counterparties and central securities depositories for the purpose of clearing and settlement of transactions. This would not allow post-trading activities, which are integrated into the trading platform. The proposed licence category for a trading venue for DLT rights would provide the regulatory framework for trading venues, where asset tokens may be traded on a non-discretionary basis.

It should be noted that the proposals made in the DLT Bill are subject to further changes in the legislative process. Although an implementation date of the proposals is not yet known, we expect expeditious implementation.

Finally, further legislative developments will have to be monitored in the future as the supervisory authorities are paying more attention to the compliance of token issuances with securities and financial markets laws generally.[19]

19 For a recent example in Switzerland, reference is made to the FINMA enforcement proceedings regarding the Envion ICO (see https://www.finma.ch/en/news/2019/03/20190327---mm---envion).

Chapter 27

UNITED ARAB EMIRATES

Silke Noa Elrifai and Christopher Gunson[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

The United Arab Emirates (UAE) has a developing legal system that has rapidly modernised in recent years. The overall legal system is a civil law system influenced by shariah (Islamic law), of which the major legal codes include the Civil Transactions Law, the Commercial Transactions Law, the Penal Code and the Commercial Companies Code. In addition to UAE federal law, each of the seven emirates of the UAE (Dubai, Abu Dhabi, Sharjah, Ajman, Umm Al Quwain, Ras Al Khaimah and Fujairah) have their own laws and regulations in areas where there is no federal law. In the field of financial and capital markets, the UAE Central Bank and the Securities and Commodities Authority (SCA) are, however, the federal regulators.

Each emirate also has its own free zones, which have limited independence from the emirate and federal law that applies to foreign investment restrictions and customs. There are, however, two financial free zones established pursuant to the UAE Constitution and federal law that are entirely separate jurisdictions in the sense that they have a regime of civil and commercial laws separate from the remainder of the UAE. The two free zones are the Dubai International Financial Centre (DIFC), where the regulator is the Dubai Financial Services Authority (DFSA), and the Abu Dhabi Global Market (ADGM), where the regulator is the Financial Services Regulatory Authority (FSRA). The DIFC applies a common law system modelled on English common law, while the ADGM applies English common law itself. UAE federal criminal laws do, however, apply in the DIFC and the ADGM (e.g., the federal anti-money laundering laws). Where necessary, the onshore UAE, the DIFC and the ADGM are dealt with separately in this chapter.

Although distributed ledger technology is presented as a government priority, the regulation of virtual currencies in the UAE remains limited, apart from in the ADGM, which has recently issued extensive regulation and consequently attracted significant interest by industry players. Although virtual currencies are not prohibited, the SCA and the DFSA have issued circulars to caution investors on virtual currencies, without, however, taking a firm regulatory position.

1 Silke Noa Elrifai is of counsel and Christopher Gunson is a partner at Amereller.

II SECURITIES AND INVESTMENT LAWS

i Onshore UAE

In the onshore UAE, the UAE Central Bank and the SCA share responsibility for the regulatory oversight of the UAE's financial and capital markets. This includes the non-financial free zones, such as the Dubai Multi Commodities Centre (DMCC) and the Dubai Silicon Oasis (DSO).

Although the SCA announced on 9 September 2018 that it would issue a regulation to govern ICOs and determine the status of coins and tokens in mainland UAE, at the time of writing, neither the Central Bank nor the SCA have issued or amended any securities, financial, investment or commodities laws to take account of the rise of virtual currencies. This may be considered surprising giving the large-scale overhaul of the UAE's banking laws and its Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) Framework in 2018 and 2019, as well as the enthusiasm professed for distributed ledger technology and blockchain in the country.

However, even without regulatory action, depending on the technology underlying or rights attaching to a coin or token, UAE securities, investment or financial laws may potentially apply to coins and tokens. Persons or entities issuing or dealing in or with tokens should exercise caution, particularly following the SCA's warning in a circular of 3 February 2018: while the primary focus of the circular was cautionary and mainly focused on initial coin offerings, it is noteworthy that the SCA requested all issuers, intermediaries facilitating initial coin offerings and trading platforms to ensure that they comply with all applicable laws.[2]

Securities and related investments are primarily governed by Federal Law No. 4 of 2000 Concerning the Emirates Securities and Commodities Authority and Market (the Securities Law),[3] and regulations issued thereunder and relating thereto.[4] The Securities Law established the SCA as a second federal regulator and includes basic rules on the offering of securities.[5] Under the Securities Law, any securities or commodities market or exchange must be in the corporate form of a local public institution or public corporation and must be licensed by the SCA.[6] This requirement was relaxed in 2014, permitting the listing of securities in private

2 SCA, Public Warning Statement on Initial Coin Offerings (ICO) (3 February 2018), available at https://www.sca.gov.ae/English/Opendata/pages/warning/4.aspx (last accessed 25 June 2019).

3 Federal Law No. 4 of 2000 Concerning the Emirates Securities and Commodities Authority and Market (Securities Law) available in Arabic at http://www.dubaided.ae/English/DataCenter/BusinessRegulations/pages/federallaw4of2000.aspx (last accessed 25 June 2019).

4 See, for example, Council of Ministers' Decision No. 12 of 2000 concerning the Regulations as to the Listing of Securities and Commodities; Council of Ministers Decision No. 3/R of 2000 concerning the Regulations as to Disclosure and Transparency; UAE Central Bank Board of Directors' Resolution No. 164/8/94 regarding the Regulation for Investment Companies and Banking, Financial and Investment Consultation Establishment or Companies; Federal Law No. 2 of 2015 concerning Commercial Companies; Administrative Decision No. 3/RT of 2017 regulating venture capital funds; SCA Board of Directors Decision No. 1 of 2014 concerning the Regulation of Investment Management; SCA Board of Directors Decision No. 27 of 2014 on the Regulation of Securities Brokerage; and SCA Board of Directors Decision No. 18 of 2015 Amending Certain Articles of the Regulation as to Disclosure and Transparency, Administrative Decision No. (39/R.T) of 2017 concerning the Investment Policy of Open-ended Public Mutual Funds, Decision No. 18 of 2018 Concerning the Regulations as to Licensing Credit Rating Agencies.

5 Article 2, Securities Law.

6 Article 20, Securities Law.

joint-stock companies on regulated exchanges.[7] The licensing requirement also applies to brokers. The Securities Law and (most) regulations issued thereunder define securities as 'shares, bonds and notes . . . and any other domestic or non-domestic financial instruments accepted by the Authority'.[8] The definition leaves room for the Authority (the SCA) to subsume virtual currencies or tokens within its definition. The Law defines commodities as '[a]gricultural produce and natural resources extracted from under the ground and the seas after being processed and prepared for commercial use', which would not appear to cover virtual currencies. However, later regulation defines commodities to include 'and any other commodities traded in contracts'.[9]

Highly relevant to trading platforms of virtual currencies, the activity of market making requires a licence from the SCA. Market making is defined as 'the activity which mainly depends on providing continuous prices for the purchase and sale of certain securities to increase the liquidity of such securities'.[10] Where coins or tokens are considered securities, the provision of trading bots to ensure liquidity of the token may therefore potentially amount to a regulated activity in onshore UAE.

ii DIFC

The DFSA, the DIFC's competent regulator, has stated that it currently does not regulate digital coins or tokens and considers them to be high risk. [11] It also currently does not license any firms in the DIFC to carry out activities related to virtual currency investments.

The core laws regulating licensable businesses in the DIFC and administered by the DFSA are:

a the Regulatory Law 2004;
b the Markets Law 2012;
c the Law Regulating Islamic Financial Business 2004;
d the Collective Investment Law 2010; and
e the Investment Trust Law 2006.[12]

The DFSA has issued a Rulebook that contains subsidiary legislation made under the Regulatory Law 2004 by the board of directors of the DFSA.[13]

7 SCA Board of Directors Decision No. 10 of 2014 Concerning the Regulation of Listing and Trading of Shares of Private Joint Stock.

8 Article 1 (Definitions), Securities Law.

9 See, for example, SCA Board Decision No. (157/R) of 2005 Concerning The Regulations As To Listing And Trading Of Commodities And Commodities Contracts available at https://www.sca.gov.ae/mservices/api/regulations/GetRegulationByIdAsPdf/105 (last accessed 25 June 2019).

10 SCA Board Decision 46 of 2012 concerning the regulations as to Market Makers.

11 DFSA, DFSA Issues General Investor Statement on Cryptocurrencies (13 September 2017), available at https://www.dfsa.ae/MediaRelease/News/DFSA-Issues-General-Investor-Statement (last accessed 24 June 2019).

12 DFSA administrative laws available at http://dfsa.complinet.com/en/display/display.html?rbid=1547&record_id=7475 (last accessed 25 June 2019).

13 DFSA rules available at http://dfsa.complinet.com/en/display/display.html?rbid=1547&record_id=1840 (last accessed 25 June 2019).

The DIFC prohibits people from performing financial services, including dealing in and advising on investments such as securities and derivatives, unless authorised to do so.[14] An activity constitutes a financial service under the Regulatory Law 2004, subject to various exemptions, if it amounts to:

a accepting deposits;
b providing credit;
c providing money services;
d dealing in investments as principal;
e dealing in investments as an agent;
f arranging deals in investments;
g managing assets;
h advising on financial products;
i managing a collective investment fund;
j providing custody;
k arranging custody;
l effecting contracts of insurance;
m carrying out contracts of insurance;
n operating an exchange;
o operating a clearing house;
p insurance intermediation;
q insurance management;
r managing a profit-sharing investment account;
s operating an alternative trading system;
t providing trust services;
u providing fund administration;
v acting as the trustee of a fund;
w operating a representative office;
x operating a credit rating agency;
y arranging credit and advising on credit; and
z operating a crowdfunding platform.[15]

The DIFC also prohibits financial promotions, which covers any communication 'which invites or induces a Person to (a) enter into, or offer to enter into, an agreement in relation to the provision of a financial service; or (b) exercise any rights conferred by a financial product or acquire, dispose of, underwrite or convert a financial product'.[16]

While there is extensive room for virtual currency transactions to fall within financial services or promotions, the statement of the DIFC indicates that at this point in time it does not consider the issuance of or dealing in digital tokens to fall within its wide regulatory framework.

14 Article 41, DIFC Law No. 1 of 2004 (Regulatory Law).

15 DFSA General Rules, Rule 2.2.1 available at http://dfsa.complinet.com/net_file_store/new_rulebooks/d/f/DFSA1547_1843_VER420.pdf (last accessed 9 June 2019).

16 Article 41A, Regulatory Law.

iii ADGM

The competent regulator in the ADGM is the FSRA. In summer 2018, the FSRA issued a far-reaching framework regulating the operation of cryptoasset businesses, which was updated in May 2019.[17]

The FSRA considers coins and tokens 'digital assets'.[18] As further expanded on in Section VII, the FSRA classifies those digital assets as digital securities, cryptoassets (e.g., Bitcoin, Ether), fiat tokens (i.e., digital tokens that are fully backed by fiat), derivatives and funds (i.e., derivatives over any digital assets and collective investment funds investing in digital assets) and other digital tokens (e.g., utility tokens).[19] Only the latter remain unregulated. Where the FSRA classifies digital assets as digital securities or derivatives or funds, dealing in them and their issuance must fully comply with the provisions applying to securities, derivatives and funds as set forth in the Financial Services and Market Act (as amended) (FSMR) and ancillary rules issued by the FSRA. Where the digital asset is a cryptoasset, those operating a cryptoasset business, including cryptoasset exchanges, wallet providers or other intermediaries are required to hold a financial service provider licence to operate a cryptoasset business under the FSMR. Where fiat tokens are involved, activities may constitute money services under the FSMR.

III BANKING AND MONEY TRANSMISSION

The Central Bank is the UAE's banking, credit and monetary regulator, and:

a provides general regulation of banking-related matters;
b oversees the issuance of currency;
c supervises banking and other licensable financial activities;
d advises the government on financial issues;
e maintains foreign exchange reserves; and
f acts as a bank for the government and other banks in the UAE.

In September 2018, the UAE government overhauled its financial service and banking laws through the issuance of Federal Law No. 14 of 2018 concerning the Central Bank and Organisation of Financial Institutions and Activities (the Financial Services Law).[20] The Financial Services Law replaced Federal Law No. 10 of 1980 concerning the Central Bank,

17 See 73B of Schedule 1, Financial Services and Markets (Amendment No 2) Regulations 2018 available at http://adgm.complinet.com/net_file_store/new_rulebooks/f/i/Financial_Services_and_Markets_Amendment_No_2_Regulations_25_June_2018.pdf (last accessed 25 June 2019).

18 Guidance – Regulation of Crypto Asset Activities in ADGM available at https://www.adgm.com/-/media/project/adgm/legal-framework/documents/guidance-and-policy/guidance-for-applicants/fsra-guidance/guidance-regulation-of-crypto-asset-activities-in-adgm_v20_20190514.pdf (last accessed 25 June 2019), Para. 10.

19 Guidance – Regulation of Crypto Asset Activities in ADGM available at https://www.adgm.com/-/media/project/adgm/legal-framework/documents/guidance-and-policy/guidance-for-applicants/fsra-guidance/guidance-regulation-of-crypto-asset-activities-in-adgm_v20_20190514.pdf (last accessed 25 June 2019), Para. 10.

20 Federal Law No. (14) of 2018 Regarding the Central Bank and Organisation of Financial Institutions and Activities available at https://www.mof.gov.ae/en/lawsAndPolitics/govLaws/Documents/Decretal%20Federal%20Law%20No.%20%2814%29%20of%202018%20Regarding%20the%20Central%20Bank.pdf (last accessed 26 June 2019).

the Monetary System and the Organisation of Banking as the main legal framework for banking in the UAE.[21] The law regulates financial services within and from the UAE as well as the proceedings of the Central Bank. Despite its recent issuance, the Financial Service Law does not refer to cryptocurrencies or tokens.

However, in January 2017, the Central Bank issued the regulatory framework for stored values and electronic payment systems (the Stored Value Regulation) to regulate different types of electronic payments and stored value.[22] The Stored Value Regulation applies in the UAE but does not apply in the DIFC and the ADGM. The Regulation defines virtual currencies as 'any type of digital unit used as a medium of exchange, a unit of account, or a form of stored value'.[23] The definition goes on to stipulate that virtual currencies are not covered by the Stored Value Regulation, but confusingly also suggests that their usage (and any transactions with them) is prohibited.[24] In February 2017, the Central Bank Governor reportedly clarified that it is not prohibiting virtual currency transactions, and that they do not fall under the Stored Value Regulations.[25]

In the past, local banks in the UAE have adopted inconsistent and changeable restrictions on remitting funds to or receiving funds from cryptocurrency exchanges, typically without prior notice. The basis for such restrictions is typically the know your customer (KYC) and AML obligations applicable to banks (as further considered in Section IV). In May 2018, BitOasis, a virtual currency exchange serving UAE customers, suspended fiat-to-crypto transactions on its trading platform because of issues with its bank.[26] In June 2018, the company was able reinstate that feature.[27] As is the case elsewhere in the world, UAE banks have hesitated opening bank accounts for blockchain companies, although the position has improved recently.

IV ANTI-MONEY LAUNDERING

The UAE has enacted numerous laws at the federal level to prevent and punish money laundering and the financing of terrorism. In the course of 2018 and 2019, and just in time for the Financial Action Task Force (FATF) evaluation of the UAE's AML/CFT regime as part of FATF's 2nd mutual evaluations of member states in the MENA Region, the UAE tightened its AML regime considerably. The updates enshrine the risk-based approach to AML/CFT in the UAE in line with international standards. The main piece of legislation is Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism And

21 Federal Law No. 10 of 1980 concerning the Central Bank, the Monetary System and Organization of Banking available at https://www.centralbank.ae/pdf/OffGazetteB.pdf (last accessed 5 August 2018).

22 UAE Central Bank, Regulatory Framework for Stored Values and Electronic Payment Systems (1 January 2017).

23 ibid., A.1.

24 ibid., D.7.3.

25 *Gulf News*, 'UAE Central Bank clarifies virtual currency ban', available at https://gulfnews.com/business/sectors/banking/uae-central-bank-clarifies-virtual-currency-ban-1.1971802 (last accessed 9 June 2019).

26 *Gulf News*, 'BitOasis confirms suspension of dirham transactions from June 4', (20 May 2018) available at https://gulfnews.com/business/sectors/technology/bitoasis-confirms-suspension-of-dirham-transactions-from-june-4-1.2224349 (last accessed 9 June 2019).

27 *Arabian News*, 'Dubai crypto exchange BitOasis reinstates AED deposits and withdrawals' (4 June 2018), available at https://www.arabianbusiness.com/banking-finance/398141-dubai-crypto-exchange-bitoasis-reinstates-aed-deposits-withdrawals (last accessed 9 June 2019).

Financing of Illegal Organisations (the New AML Law)[28] together with Cabinet Resolution No. (10) of 2019 Concerning the Executive Regulation[29] of Federal Law No. 20 of 2018 (the AML Executive Regulation).[30] The New AML Law and the AML Executive Regulation apply in all emirates, including the DIFC and ADGM. The New AML Law repealed the older Federal Law No. 4 of 2002 concerning Combating Money Laundering and Terrorism Financing Crimes. The overhaul of the UAE's AML/CFT regime went hand in hand with the issuance of the Central Bank Law complementing the New AML Law.

The New AML Law defines the crimes of money laundering and terrorist financing and details the sanctions for such activities. Additionally, Law No. 7 of 2014 on Combating Terrorism Offences (the CTO Law), which was not repealed by the New AML Law, addresses the combating of terrorism crimes.[31]

The main money laundering offence is defined in Article 2 of the New AML Law. The offence renders a person a perpetrator of money laundering who:

a conducts any transaction aiming to conceal the funds' illegal source;

b conceals the true nature, origin, location, way of disposition or ownership of rights with respect to the proceeds of a transaction;

c acquires, possesses or uses the proceeds upon receipt; or

d assists the perpetrator of the office to escape punishment.

Crucially, it is not required to prove the illicit source of the funds to convict a person for money laundering. It is, however, only money laundering if the person is fully aware that such funds are derived from a felony or a misdemeanour.

For the purposes of virtual currencies, funds refer to any assets whatsoever including assets in digital or electronic form.[32] Virtual currencies do fall within the scope of the UAE's AML/CFT regime.

Sanctions for money laundering include prison sentences of up to 10 years, monetary fines for individuals of between 100,000 dirhams and 5 million dirhams. Where a representative of a legal person commits any of the New AML Law's money laundering offences, monetary

28 Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations (New AML Law) available at https://www.mof.gov.ae/en/lawsAndPolitics/govLaws/Documents/EN%20Final%20AML%20Law-%20Reviewed%20MS%2021-11-2018.pdf (last accessed 25 June 2019).

29 Cabinet Resolution No. (10) of 2019 Concerning the Executive Regulation of the Federal Law No. 20 of 2018 concerning Anti-Money Laundering and Combating Terrorism Financing available at https://www.mof.gov.ae/en/lawsAndPolitics/CabinetResolutions/Documents/Cabinet%20Decision%20No%20%20(10)%20of%202019%20CONCERNING%20THE%20IMPLEMENTING%20REGULATION%20%20%20.pdf (last accessed 26 June 2019); see also SCA Board Chairman's Decision No. (21/Chairman) of 2019 procedures of Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations.

30 The SCA Board Chairman's Decision No. (21/Chairman) of 2019 Procedures of Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations available at https://www.sca.gov.ae/english/regulations/pages/default2.aspx (last accessed 26 June 2019).

31 Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations available at https://www.mof.gov.ae/en/lawsAndPolitics/govLaws/Documents/EN%20Final%20AML%20Law-%20Reviewed%20MS%2021-11-2018.pdf (last accessed 27 June 2019).

32 Article 1, Federal Law 9 of 2014.

fines range from 500,000 dirhams to 50 million dirhams.[33] Where the entity is convicted of terrorist financing, it is dissolved. In all cases, tainted funds are to be forfeited or, where this is not possible, equivalent funds seized.[34] Forfeiture also applies to virtual currencies. Again, while cryptocurrencies are not specifically mentioned in the legislation, any virtual funds will be considered assets the court may confiscate if those funds are tainted by money laundering. Other offences include intentionally failing to report a suspicious activity or to provide additional information upon request, deliberately concealing information[35] and tipping off.[36] Failing reporting duties because of gross negligence also attracts prison sentences or fines, or both.[37] Breaches by obliged entities may attract penalties ranging from warnings, revocation of licences, fines to arrest of responsible personnel.[38]

The New AML Law broadly applies to financial institutions, and in contrast to previous regulation, now also explicitly designates non-financial businesses and professions and non-profit organisations as obliged entities.[39] The term 'financial institutions' includes anyone who does any of the following on behalf of a customer:

a receives deposits and other funds that can be paid by the public;
b provides private banking services, credit facilities, cash brokerage services, currency exchange and money transfer services, stored value services, electronic payments for retail and digital cash, and virtual banking services;
c conducts financial transactions in securities, finance and financial leasing;
d issues and manages means of payment, guarantees or obligations;
e trades, invests, operates or manages funds, option or future contracts, and exchange rates;
f conducts interest rate transactions, other derivatives or negotiable financial instruments;
g participates in issuing securities and providing related financial services;
h manages fund portfolios;
i manages saving funds;
j prepares or markets financial activities;
k conducts insurance transactions; or
l conducts any other activity or financial transaction determined by a supervisory authority.[40]

Designated non-financial businesses and professions include brokers when they conclude operations for the benefit of customers concerning a real estate transaction, dealers in precious metals or stones in any related transactions of 55,000 dirhams or more, lawyers, notaries and accountants when preparing, conducting or executing financial transactions for clients in respect of certain transactions, and providers of corporate and trust services or anyone so determined by a supervisory authority.[41] Non-Profit organisations include 'any organised group, of a continuing nature set for a temporary or permanent time period,

33 Article 23, New AML Law.
34 Article 26, New AML Law.
35 Article 30, New AML Law.
36 Article 25, New AML Law.
37 Article 24, New AML Law.
38 Article 14, New AML Law.
39 Article 30, New AML Law.
40 Article 1, New AML Law read together with Articles 1 and 2, AML Executive Regulation.
41 Article 1, New AML Law together with Articles 1 and 3, AML Executive Regulation.

comprising natural or legal persons as well as not-for-profit legal arrangements for the purpose of collecting, receiving or disbursing funds for charitable, religious, cultural, educational, social, communal or any other charitable activities'.

The definitions are wide and non-exhaustive. The definition for activities rendering an entity a financial institution includes the provision of 'digital cash', without any further explanation as to whether this definition includes any or all forms of crypto or whether only fiat-like tokens such as stablecoins, particularly those pegged to a fiat currency[42] are caught by the definition. However, the definition of assets taken together with the scope of obliged entities is wide enough to cover establishments dealing in or with virtual currencies, including blockchain ventures structured as foundations.

The New ALM Law and its Executive Regulation also expands the powers of institutions, units and committees charged with supervision and enforcement of the UAE's AML/CTF regime.[43] These include, among others, the Central Bank, which operates the Financial Intelligence Unit and is to receive suspicious activities report filings from obliged entities, the DMCC Authority within its free zone, the DFSA in the DIFC and the FSRA in the ADGM.[44]

In June 2019, the UAE government announced that regulated entities, including financial institutions, would be required to use 'goAML', a UN-developed software platform, to file any suspicion activity report of money laundering to the Central Bank's Financial Intelligence Unit.[45] The initiative underscores the UAE's commitment to meet international best standards in AML and CTF and digitise its economy.

i DIFC

The AML Law, the CTO Law and their implementing regulations apply in the DIFC by virtue of Article 3 of the Regulatory Law. Violations of the mainland UAE AML/CTF regime may also be punished in the DIFC.[46] Additionally, the DIFC has its own AML/CFT regime contained in Chapter II of Part IV of the DIFC Regulatory Law and the Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (the AML Rules) of the DFSA Rulebook. Until the issuance of the New AML Law in mainland UAE, the DIFC regime went beyond UAE requirements. After some amendments in October 2018, they are now largely in line and ensure compliance with the FATF's 2012 recommendations.[47]

The AML Rules apply a risk-based approach to authorised firms (other than credit rating agencies), authorised market institutions, designated non-financial businesses or professions, and auditors. If a blockchain or virtual currency business were licensed by the DFSA, it would be obliged to comply with its AML Module, which includes extensive customer due diligence and continuing AML monitoring. Decentralised cryptocurrency exchanges may have difficulty complying.

42 As for example the Gemini Dollar, Tether and True USD.

43 See Cabinet Resolution No. 38 of 2014 concerning the Executive Regulation of Federal Law No. 4 of 2002 Concerning Anti-Money Laundering and Combating Terrorism Financing.

44 See, for example, Section 7(6), Financial Services and Markets Regulations 2015, ADGM FSMR.

45 Khaleej Times, 'UAE financial firms to register on new platform or face penalties', available at https://www.khaleejtimes.com/news/crime-and-courts/uae-first-to-launch-un-developed-anti-money-laundering-platform (last accessed 26 June 2019).

46 See Article 71(1) of the Regulatory Law.

47 DFSA, The DFSA Rulebook Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module, available at http://dfsa.complinet.com/net_file_store/new_rulebooks/d/f/DFSA1547_20015_VER130.pdf.

ii ADGM

The mainland UAE AML/CTF regime also applies in the ADGM. Like the DIFC, the FSRA maintains a AML Rulebook, which complements the federal regulations and puts detailed requirements on regulated entities, including for risk-based KYC and AML controls.[48] The FSRA overhauled the ADGM's framework in 2018 and 2019 to bring it in line with the New AML Law and implementing regulations.[49] The Rulebook applies to all FSRA-regulated entities, including those regulated under the 2018 amendments to the FSMA relating to cryptoassets businesses.[50]

V REGULATION OF EXCHANGES

i Onshore UAE

At the time of writing, the SCA has not issued any regulations specifically addressing cryptocurrency exchanges and no cryptocurrency exchange fully operated out of the UAE. BitOasis, which was marketed as the 'first cryptocurrency exchange in the Middle East', was originally incorporated as an entity in the DSO, a Dubai free zone. BitOasis thereafter transferred to an entity incorporated in the British Virgin Islands and is now understood to seek licensing in the ABGM as a cryptoasset exchange.[51]

In December 2017, the DMCC announced that it added proprietary trading in crypto commodities as a licensable regulated activity.[52] The DMCC has stated that it considers virtual currencies a commodity, and therefore considers activity concerning them to be within the free zone's jurisdictional and regulatory scope. This licence is restricted to buying and selling of crypto commodities on a licensee's own account. Importantly, it does not allow the holder of the licence to act as a cryptocurrency exchange. However, the licence appears to be suitable for the operation of trading bots that ensure liquidity on a trading platform. We are aware that at least one licence application to that effect has been granted. To receive a licence, an applicant must have a minimum issued share capital of 50,000 dirhams, present a business plan and reply to a questionnaire. In 2018, the DMCC issued a licence to Regal RA DMCC (Regal), a precious metal trader incorporated in the DMCC.[53] Regal provides physical (cold) storage of virtual currencies it considers commodities on behalf of clients in its headquarters' vault.[54]

48 FSRA, Anti-Money Laundering and Sanctions Rules and Guidance (AML), available at http://adgm.complinet.com/net_file_store/new_rulebooks/a/m/AML_VER03.150419.pdf (last accessed 26 June 2019).

49 ibid.

50 FSRA, Guidance – Regulation of Crypto Asset Activities in ADGM (25 June 2018), available at https://www.iosco.org/library/ico-statements/Abu%20Dhabi%20-%20FSRA%20-%20Guidance%20-%20Regulation%20of%20Crypto%20Asset%20Activities%20in%20ADGM.pdf (last accessed 25 June 2019), p. 8; see also Chapter 17.1.2 of the FSRA Conduct of Business Rulebook.

51 The company operating BitOasis is operated by BO Technologies Ltd, information available at https://bitoasis.net/en/front/privacy-policy (last accessed 25 June 2019).

52 https://www.dmcc.ae/blog/dmcc-services-updates-december-2017.

53 *Arabian Business*, Dubai's first licensed Bitcoin trader: 'It's a commodity not a currency' (13 February 2018), available at https://www.arabianbusiness.com/banking-finance/389854-dubais-first-licensed-bitcoin-trader-its-commodity-not-currency (last accessed 27 June 2019).

54 https://regalassets.ae/cryptocommodities/ (last accessed 27 June 2019).

ii DIFC

Although the DIFC is home to NASDAQ DUBAI, one of the largest stock exchanges in the Middle East, and Dubai Mercantile Exchange, a major energy futures and commodities exchange, the DFSA has thus far not issued regulations specifically addressing cryptocurrency exchanges. Nor has it issued any full licences to businesses operating to that effect. Operating an exchange, a multilateral trading facility or an alternative trading platform are, among other things, licensable activities in the DIFC, and are regulated. However, given the DFSA announcement that it does not currently regulate tokens or coins, operating a virtual currency platform does not appear to fall within any such definition. The DFSA's regulatory sandbox, which issues 'innovation testing licences', has been reported to have issued a licence to TokenMarket Capital Limited to operate as a Category 4 adviser for issuers of or investors in security token offers in or from the DIFC. The company aims to establish a DFSA-licensed and regulated authorised market institution to operate a tokenised securities exchange in or from the DIFC.[55] The development indicates that the DIFC may in due time adapt its regulatory regime to account for crypto businesses including exchanges.

iii ADGM

In contrast to the onshore UAE and the DIFC, a business must be licensed as a financial service provider to operate a cryptocurrency exchange in the ADGM if the exchange's activities fall within the ambit of operating a cryptoasset business under the regulations and guidance issued by the FSRA in June 2018[56] and updated in May 2019.[57]

The Financial Services and Markets (Amendment) Regulation 2018 defines a regulated cryptoasset business to include operating a cryptoasset exchange trading, converting or exchanging fiat currency or other value into accepted cryptoassets, accepted cryptoassets into fiat currency or other value, or one accepted cryptoasset into another accepted cryptoasset.

The ADGM thus regulates both fiat-to-crypto and crypto-to-crypto exchanges. Importantly, however, the transmission of cryptoassets is specifically excluded from the ambit of cryptoasset business.[58] Accordingly, depending on the structure of an exchange, some decentralised non-custodial exchanges appear to fall outside the definition.

The Regulation allows cryptoasset exchanges to trade in what is termed accepted cryptoassets only. The FSRA decides which virtual currencies are accepted cryptoassets. No public register is maintained, because the determination as to what constitutes an accepted

55 https://livecryptonews.info/the-impact-of-regulatory-licences-on-blockchain/; see also https://www.dfsa.ae/MediaRelease/News/DFSA-Regulatory-Sandbox-accepts-seven-new-firms-in; https://www.difc.ae/public-register/tokenmarket-capital/ (last accessed 27 June 2019).

56 73B of Schedule 1, Financial Services and Markets (Amendment No. 2) Regulations 2018 available at http://adgm.complinet.com/net_file_store/new_rulebooks/f/i/Financial_Services_and_Markets_Amendment_No_2_Regulations_25_June_2018.pdf (last accessed 25 June 2019).

57 73B of Schedule 1, Financial Services and Markets (Amendment No. 2) Regulations 2018 available at http://adgm.complinet.com/net_file_store/new_rulebooks/f/i/Financial_Services_and_Markets_Amendment_No_2_Regulations_25_June_2018.pdf (last accessed 25 June 2019); Guidance – Regulation of Crypto Asset Activities in ADGM available at https://www.adgm.com/-/media/project/adgm/legal-framework/documents/guidance-and-policy/guidance-for-applicants/fsra-guidance/guidance-regulation-of-crypto-asset-activities-in-adgm_v20_20190514.pdf (last accessed 25 June 2019) (FSRA Crypto Asset Guidance).

58 32C(3) of Schedule 1, Financial Services and Markets (Amendment No. 2) Regulations 2018.

cryptoasset is specific to the applicant.[59] The Regulation envisages a licensed cryptoasset exchange to be regulated like a multilateral trading facility, and is required to have in place the full gamut of oversight processes, such as:

a market surveillance;
b KYC and AML procedures;
c settlement processes;
d transaction recording;
e transparency and public disclosure mechanisms; and
f exchange-like operational systems and controls.[60]

Businesses hoping to operate a cryptoasset exchange out of the ADGM must pay an initial application fee of US$125,000 and an annual supervision fee of US$60,000.[61] This compares to an initial application fee for other cryptoasset businesses of US$20,000 and an annual supervisory fee of US$15,000, which is to reflect the heightened regulatory burden of the FSRA supervising a cryptoasset exchange.[62] Where the cryptoasset exchange also operates other licensable business, the fee is cumulative. Moreover, a trading levy between 0.0006 per cent and 0.0015 per cent is to be paid to the ADGM calculated on a sliding scale dependent on the average daily trading volume.[63] A licensed cryptoasset exchange is required to maintain minimum regulatory capital in fiat at the standard of a recognised investment exchange, which is equivalent to 12 months' operational expenses.[64] It may be higher, where the FSRA determines that the cryptoasset exchange is high-risk.[65]

At the time of writing, it is understood that BitOasis,[66] Arabian Bourse (ABX)[67] and DEX,[68] among others, have been issued with an in-principle approval by the FSRA to operate their centralised cryptoasset exchanges and custodial wallets. Bithumb, the South Korean centralised cryptocurrency exchange, was also reported to be working towards opening

59 258(1) Financial Services and Markets (Amendment No. 2) Regulations 2018. See also, Guidance – Regulation of Crypto Asset Activities in ADGM available at https://www.adgm.com/-/media/project/adgm/legal-framework/documents/guidance-and-policy/guidance-for-applicants/fsra-guidance/guidance-regulation-of-crypto-asset-activities-in-adgm_v20_20190514.pdf (last accessed 25 June 2019), Para. 30.

60 FSRA Crypto Asset Guidance.

61 FEES Rule 3.14.1 and FEES Rule 3.14.2; see also FSRA Crypto Asset Guidance, p. 34.

62 https://www.adgm.com/-/media/project/adgm/media-centre/publications/adgm_crypto_assets_brochure_v7.pdf (last accessed 25 June 2019).

63 https://www.adgm.com/-/media/project/adgm/media-centre/publications/adgm_crypto_assets_brochure_v7.pdf (last accessed 25 June 2019).

64 See also, FSRA Crypto Asset Guidance, Paras. 30 to 33.

65 ibid.

66 Coindesk, 'BitOasis Clears Hurdle in Bid to Launch Regulated Crypto Asset Exchange' (13 May 2019) available at https://www.coindesk.com/bitoasis-clears-hurdle-in-bid-to-launch-regulated-crypto-asset-exchange (last accessed 29 June 2019).

67 *Funds Global Mena*, 'Crypto exchange gets approval in Abu Dhabi' (14 June 2019), available at http://www.fundsglobalmena.com/news/crypto-exchange-gets-approval-in-abu-dhabi (last accessed 27 June 2019).

68 Zawya, 'DEX Secures In Principle Approval For Crypto Asset Exchange From ADGM's Financial Services Regulator' (24 June 2019), available at https://www.zawya.com/mena/en/press-releases/story/DEX_Secures_In_Principle_Approval_For_Crypto_Asset_Exchange_From_ADGMs_Financial_Services_Regulator-ZAWYA20190624093627/ (last accessed 27 June 2019).

a centralised cryptocurrency exchange in the ADGM through a partnership with Abu Dhabi-based N-VELOP.[69] Abu Dhabi-based MidChains[70] is also reported to have applied for a licence.

VI REGULATION OF MINERS

The mining of virtual currencies is not a regulated practice in the UAE, or in any of the free zones within the UAE. The activity of mining is also not covered in any previous legislation that would be applicable.

Even within the ADGM, the FSRA does not consider the mining of cryptocurrencies to be a regulated activity. The amended FSMA specifically excludes 'the development, dissemination or use of software for the purpose of creating or mining a Crypto Asset' from its regulated activities.[71]

VII REGULATION OF ISSUERS AND SPONSORS

i Onshore UAE

On 9 September 2018, the SRA announced that the issuance of a regulation governing ICOs was imminent. However, as at 29 June 2019, no regulations to this effect have been issued. In its warning issued in February 2018, the SCA reiterated that it does not regulate, mandate or recognise any ICO.[72] At the same time, it urged that 'all issuers of digital tokens, intermediaries facilitating or advising on an offer of digital tokens, and platforms facilitating trading in digital tokens should therefore seek independent legal advice to ensure they comply with all applicable laws, and consult SCA where appropriate'.[73]

In the UAE, as in other jurisdictions, ICOs could be deemed to amount to a sale of a security, units in investment funds, commodities or other assets, depending on the underlying technology or rights attaching to the token. Where tokens have features like securities, ICOs can be anticipated to be subject to onshore UAE securities laws and would have to be licensed by the SCA.

ii DIFC

The DFSA has also taken a wait-and-see approach to explicitly regulating the issuance of ICOs and their issuers and sponsors. In September 2017, the DFSA issued a warning to investors and clarified that 'it does not currently regulate these types of product offerings

69 *Cointelegraph*, 'Bithumb Partners With Blockchain VC Firm Nvelop to Launch Exchange in UAE: Report' (12 February 2019), available at https://cointelegraph.com/news/bithumb-partners-with-blockchain-vc-firm-nvelop-to-launch-exchange-in-uae-report (last accessed 26 June 2019).

70 https://midchains.com/ (last accessed 27 June 2019).

71 73C(2) of Schedule 1, Financial Services and Markets (Amendment No. 2) Regulation 2018.

72 SCA, Public Warning Statement on Initial Coin Offerings (ICO) (3 February 2018), available at https://www.sca.gov.ae/English/Opendata/pages/warning/4.aspx (last accessed 25 June 2019).

73 ibid.

or license firms in the Dubai International Financial Centre (DIFC) to undertake such activities'.[74] However, the warning has not prevented the DFSA from accepting at least one company advising in the field of security token offerings into its regulatory sandbox.[75]

iii ADGM

In October 2017, the FSRA issued guidance applicable to those considering an ICO or transacting in virtual currencies.[76] The guidance has been regularly updated (including in June 2018[77]) and most recently in May 2019.[78] The FSRA considers on a case-by-case basis whether an ICO is to be regulated under the FSMR.[79] This would be the case where the FSRA determines that tokens exhibit the characteristics of securities under Section 58(2)(b) of the FSMR. In that case, the FSRA considers tokens to be securities, and an ICO must comply with the FSMR if it is issued to the public in or from the ADGM.[80] Accordingly, where an ICO is issued abroad but offered to the public in the ADGM, a decision by the FSRA needs to be sought, unless buyers located in the ADGM are excluded from participation.

Further, a FSRA decision to consider a token to be a security triggers the prospectus obligations under Section 61 of the FSMR, other obligations under Chapter 4 of the FSMR Markets Rules, as well as AML and KYC requirements. The usual prospectus exemptions may apply where an offer is only made to professional clients (as defined in the FSMR) or fewer than 50 persons in any 12-month period, or where the consideration to be paid by a single person to acquire tokens is at least US$100,000.[81] Classification as a digital security also triggers requirements for market intermediaries or operators, such as virtual currency exchanges, who trade in those tokens, to be regulated as financial services permission holders, recognised investment exchanges or recognised clearing houses.[82] Additionally, the FSRA may consider tokens used by firms to build an investment fund on the blockchain as units in a collective investment fund (as defined in Section 106 of the FSMR) to which the ADGM's fund rules apply.[83] This classification also triggers extensive regulatory requirements.

74 DFSA Issues General Investor Statement on Cryptocurrencies (13 September 2017), available at https://www.dfsa.ae/MediaRelease/News/DFSA-Issues-General-Investor-Statement (last accessed 25 June 2019).

75 Livecryptonews, 'The Impact of Regulatory Licences on Blockchain' (19 June 2019), available at https://livecryptonews.info/the-impact-of-regulatory-licences-on-blockchain (last accessed 27 June 2019).

76 FSRA, Supplementary Guidance – Regulation of Initial Coin/Token Offerings and Virtual Currencies under the Financial Services and Markets Regulations (October 2017), available at http://adgm.complinet.com/net_file_store/new_rulebooks/i/c/ICOs_and_Virtual_Currencies_Guidance_VER01.08102017.pdf.

77 Guidance – Regulation of Initial Coin/Token Offerings and Crypto Assets under the Financial Services and Markets Regulations (June 2018) available at http://adgm.complinet.com/net_file_store/new_rulebooks/i/c/ICOs_and_Virtual_Currencies_Guidance_VER02.24062018.pdf (last accessed 29 June 2019).

78 FSRA, Regulation of Digital Security Offerings and Crypto Assets under the Financial Services and Markets Regulations (May 2019) available at http://adgm.complinet.com/net_file_store/new_rulebooks/g/u/Guidance_ICOs_and_Crypto_Assets_13052019.pdf (last accessed 29 June 2019) [FSRA ICO Guidance].

79 FSRA ICO Guidance, Article 3.3.

80 ibid.

81 FSRA ICO Guidance, Article 3.6.

82 FSRA ICO Guidance, Article 3.7.

83 FSRA ICO Guidance, Article 3.9.

Where the token to be issued is a stablecoin, it may only be issued in the ADGM, where it is one-to-one backed by fiat currency.[84] The FSRA then characterises the token as a fiat token. Its issuer is considered a money services business that must hold a financial services permission for the regulated activity of 'providing money services' pursuant to Schedule 1, Section 52 of the FSMR.[85] Other requirements under the Operating a Crypto Asset Business framework also apply.

Only where the FSMR does not consider digital tokens to be digital securities, fiat tokens or derivatives is an ICO unlikely to constitute a regulated activity under the FSMR.[86]

VIII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

Various UAE authorities have raised concerns about fraud related to cryptocurrency transactions. The SCA has warned UAE residents about and advised them to avoid trading in virtual currencies. The DFSA has advised potential investors to exercise caution and undertake due diligence to understand the risks involved.[87] One reason for the FSRA's decision to regulate cryptoassets was to prevent significant financial crimes and other risks.[88] The Dubai police has also raised the matter.[89]

Reports have surfaced about virtual currency-related frauds in the UAE, mainly in relation to over-the-counter transactions to buy and sell virtual currencies,[90] investment schemes and scam cryptocurrencies[91] and about the embezzlement of cryptocurrencies by an employee of a cryptocurrency exchange.[92] We are also aware of instances where UAE commercial banks have halted cryptocurrency-related transactions pending approval from the Central Bank.

Owing to a lack of legislation on the federal level, there are no specific criminal or civil penalties in place for the misuse of cryptocurrencies in the onshore UAE or the DIFC, and prima facie outside of the scope of standard criminal provisions such as fraud, embezzlement or theft. However, this no longer appears to be the case for money laundering and terrorist financing offences following the overhaul the UAE's AML/CFT regime. In the FSRA, operators of a cryptoasset business may be found guilty of the full gamut of financial crimes and administrative offences and misdemeanours, including market abuse, and making misleading statements and impressions.[93]

84 FSRA Crypto Asset Guidance, Para. 161.

85 ibid.

86 FSRA ICO Guidance, Article 3.10.

87 See footnote 14.

88 FSRA Crypto Asset Guidance, p. 6.

89 CCN, 'Dubai Police Warns Against Crypto Scams, Predicts Electronic Money Will Replace Cash' (18 September 2018), available at https://www.ccn.com/dubai-police-warns-against-crypto-scams-predicts-replacement-of-cash-with-electronic-money/ (last accessed 29 June 2019).

90 *Khaleej Times*, 'Man arrested in UAE for Dh2 million Bitcoin fraud' (13 February 2018), available at https://www.khaleejtimes.com/news/crime/man-arrested-in-uae-for-dh2-million-bitcoin-fraud.

91 *Gulf News*, "Serial' entrepreneur in Dubai accused of being serial scammer' (11 April 2019), available at https://gulfnews.com/uae/serial-entrepreneur-in-dubai-accused-of-being-serial-scammer-1.63241099 (last accessed 26 June 2019).

92 *Khaleej Times*, 'Dubai employee embezzles Dh800,000 in cryptocurrency fraud' (12 March 2018) available at https://www.khaleejtimes.com/news/crime/dubai-employee-embezzles-dh800000-in-cryptocurrency-fraud.

93 Sections 92, 102 and 103, FSMA (as amended).

IX TAX

The UAE established the Federal Tax Authority in 2016, introduced an excise tax on certain goods in October 2017 and introduced a value added tax on all good and services in the UAE, with some limited exemptions, from January 2018.[94] A sale of virtual currencies could be a taxable transaction under the value added tax laws, but the Federal Tax Authority has not issued any regulations on virtual currencies.

There is no corporate or income tax in the UAE. There are also no withholding tax or foreign exchange controls that impact cross-border payments involving virtual currencies.

X LOOKING AHEAD

A major topic in the UAE is the different regulatory positions that will be adopted by the UAE federal regulators (the Central Bank and SCA) and free zone regulators (the DFSA and FSRA). With the usage of cryptocurrencies and tokens becoming more popular in the Middle East, and the aspiration of the UAE to be at the forefront of new business regulations, we anticipate that the UAE will seek to adopt regulatory measures that are perceived as being pro-business. Regulators in the UAE are most likely to follow standards developed by international best practices and are likely to follow the recent FATF guidelines on cryptocurrencies.[95]

The SCA has announced the formation of a fintech team for the purpose of implementing fintech initiatives and updating the SCA with the latest fintech developments.[96] The SCA stated that it would issue ICO regulations in autumn 2018, but as at 25 June 2019 no regulations have been issued. Moreover, the Dubai government has launched the Dubai Blockchain Strategy, under which blockchain technology is being studied and assessed to put all transactions with governmental authorities onto a blockchain by 2020.[97] Using such technology may, in suitable instances, be cost-effective and more efficient for all the parties involved. In 2018, it was announced that the DIFC was exploring ways to transform into a blockchain-powered judiciary.[98] In June 2019, the Dubai Land Department announced that it had signed an memorandum of understanding with Du, one of the state's telecoms operators, to launch blockchain-based real estate services, on a Du-developed blockchain said to be interoperable with both the Hyperledger and Ethereum blockchains.[99] As the government's main goal is a high level of customer satisfaction across the board, it will prioritise exploring this technology, which will trigger the need to develop respective regulations.

94 Federal Decree-Law No. 8 of 2017 on Value Added Tax available at https://www.mof.gov.ae/En/lawsAndPolitics/govLaws/Documents/VAT%20Decree-Law%20No.%20%288%29%20of%202017%20-%20English.pdf.

95 FAFT, 'Guidance For A Risk-Based Approach Virtual Assets And Virtual Asset Service Providers' (21 June 2019), available at http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf (last accessed 29 June 2019).

96 See footnote 3.

97 Smart Dubai, 'Dubai Blockchain Strategy', https://smartdubai.ae/en/Initiatives/Pages/DubaiBlockchainStrategy.aspx (last accessed on 29 June 2019).

98 *Arabian Business*, 'Smart Dubai, DIFC Courts to launch world's first Court of the Blockchain' (30 July 2018), available at https://www.arabianbusiness.com/technology/401774-smart-dubai-difc-courts-to-launch-worlds-first-court-of-the-blockchain (last accessed 29 June 2019).

99 Cointelegraph, 'Dubai Real Estate Department Signs MoU With Telecoms Firm to Implement Blockchain' (10 June 2019), available at https://cointelegraph.com/news/dubai-real-estate-department-signs-mou-with-telecoms-firm-to-implement-blockchain (last accessed 29 June 2019).

Chapter 28

UNITED KINGDOM

Peter Chapman and Laura Douglas[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

At present, some but not all types of virtual currencies are regulated in the United Kingdom (UK). In general, the structure and substantive characteristics of a virtual currency will determine whether or not it falls within the UK regulatory perimeter, and if so, which regulatory framework or frameworks will apply. In its Guidance on Cryptoassets,[2] the UK Financial Conduct Authority (FCA) identifies three broad categories of virtual currencies (or cryptoassets), with the following features:

a Security tokens: virtual currencies with characteristics that mean they provide rights and obligations akin to traditional instruments such as shares, debentures or units in a collective investment scheme, meaning that they do fall within the UK regulatory perimeter.

b E-money tokens: virtual currencies that meet the definition of electronic money (or e-money) under the Electronic Money Regulations 2011 (EMRs). Again, they fall within the UK regulatory perimeter.

c Unregulated tokens: virtual currencies that are neither security tokens nor e-money tokens and therefore fall outside the UK regulatory perimeter. They include virtual currencies that are not issued or backed by any central authority and are intended and designed to be used directly as a means of exchange, which the FCA refers to as exchange tokens but are often called cryptocurrencies. Unregulated tokens also include 'utility tokens', which grant holders access to a current or prospective service or product but exhibit features that would make them akin to securities. Utility tokens may be the same as or similar to reward-based crowdfunding.

In its Guidance, the FCA states that although it recognises these three broad categories of cryptoassets 'they may move between categories during their lifecycle' and assessing whether a particular virtual currency falls within the UK regulatory perimeter 'can only be done on a case-by-case basis, with reference to a number of different factors'. More generally, the Guidance sets out the FCA's views on when virtual currencies fall within the current UK regulatory perimeter. This Guidance is not binding on the courts but may be persuasive in any determination by the courts, for example when enforcing contracts.

---

1 Peter Chapman is a partner and Laura Douglas is a senior associate knowledge lawyer at Clifford Chance LLP. The authors would like to thank Kate Scott and David Harkness for their contributions to Sections VIII and IX of this chapter.

2 Policy Statement PS19/22: Guidance on Cryptoassets published by the FCA on 31 July 2019, available at https://www.fca.org.uk/publications/policy-statements/ps19-22-guidance-cryptoassets.

i Questions to consider when identifying potentially applicable regulatory regimes

There are various ways in which market participants' activities relating to virtual currencies might be regulated in the UK. When analysing whether, and if so how, activities relating to a particular virtual currency may be regulated, it is helpful to consider the following questions:

a Might virtual currencies be transferable securities or other types of regulated financial instruments or investments?

b Might arrangements relating to the issuance of virtual currencies involve the creation of a collective investment scheme?

c Might virtual currencies give rise to deposit-taking, the issuance of electronic money or the provision of payment services?

d Might the issuance of virtual currencies or the operation of an exchange for virtual currencies be regulated as crowdfunding?

e Might the relevant activities concerning virtual currencies fall within the scope of the UK anti-money laundering legal and regulatory regime?

ii Interaction with EU financial services regulation and the impact of Brexit

The UK is currently a Member State of the European Union (EU). Therefore, EU-wide rules regulating the provision of financial services apply to the regulation of virtual currencies in the UK, whether through the direct application of EU regulations or under UK legislation implementing the requirements of EU directives.

For instance, the UK has implemented into national law requirements of:

a the recast Markets in Financial Instruments Directive (MiFID II),[3] which regulates investment services and activities relating to financial instruments;

b the Capital Requirements Directive and Regulation,[4] which regulate the activities of credit institutions, including deposit-taking;

c the revised Electronic Money Directive and the revised Payment Services Directive,[5] which regulate activities relating to the issuance of electronic money and the provision of payment services, respectively; and

d the Fourth EU Anti-Money Laundering Directive,[6] which regulates entities conducting activities giving rise to money laundering risks.

These EU regulatory requirements may be integrated into or sit alongside domestic UK regulatory requirements, such as those under the Financial Services and Markets Act 2000 (FSMA), the EMRs and the Payment Services Regulations 2017 (PSRs).

At the time of writing, the UK is due to leave the EU on 31 October 2019. This follows the outcome of the Brexit referendum vote in June 2016, the service of notice of the UK's

3 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments.

4 Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms and Regulation (EU) No. 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms.

5 Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions.

6 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

intention to leave the EU under Article 50 of the Treaty on European Union on 29 March 2017 and subsequent extensions to the Article 50 notice. However, the government has committed to preserve and onshore most existing EU and EU-derived legislation as it stands immediately before the UK's departure through the European Union (Withdrawal) Act 2018. Therefore, the analysis of whether virtual currencies are regulated in the UK (including under applicable EU-wide regulatory frameworks) should not be affected by Brexit, at least in the short term.

II SECURITIES AND INVESTMENT SERVICES LAWS

The FSMA forms a cornerstone of the UK regulatory regime for financial services. Under Section 19 FSMA, a person must not carry on a regulated activity in the UK or purport to do so unless he or she is authorised or exempt.[7] This is referred to as the general prohibition, breach of which is a criminal offence (see Section VIII.i).

A regulated activity is an activity of a specified kind that is carried on by way of business and relates to an investment of a specified kind.[8] The Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (RAO) sets out the kinds of activities and investments that are specified for this purpose. Therefore, a key question is whether some types of virtual currencies may be specified investments under the RAO, and if so, into which category or categories of specified investments they fall. In general, the answer to this question will depend on the substantive features of the virtual currency under consideration, and so a case-by-case analysis of the relevant fact pattern will be needed. However, we set out in subsection i some broad principles about how different types of virtual currencies are likely to be categorised under the UK regulatory regime. At a high level, the FCA has indicated exchange tokens (i.e., cryptocurrencies) and utility tokens are not regulated types of financial instruments, whereas activities relating to cryptocurrency derivatives and securities tokens are regulated. We also consider in subsection ii whether arrangements relating to the issue of virtual currencies could involve the creation of a collective investment scheme (CIS).

i Categories of virtual currencies and specified investments

Exchange tokens (cryptocurrencies) and cryptocurrency derivatives

The FCA has made various statements indicating that it does not consider exchange tokens (which it has sometimes referred to as cryptocurrencies or digital currencies) to fall within the UK regulatory perimeter for financial services, provided that they do not form part of other regulated products or services.[9] In general, this means that cryptocurrencies are not considered to be specified investments under the FSMA.[10]

However, in April 2018, the FCA indicated that cryptocurrency derivatives may be financial instruments within the scope of MiFID II, even though cryptocurrencies themselves are not regulated financial instruments in the UK.[11] In this statement, the FCA indicated that cryptocurrency derivatives include futures, options and contracts for difference referencing

7 Section 19 FSMA.

8 Section 22 FSMA.

9 See, for example, the FCA Feedback Statement on Distributed Ledger Technology (December 2017), available at https://www. fca.org.uk/publications/feedback-statements/fs17-4-distributed-ledger-technology and the FCA's Guidance on Cryptoassets.

10 See, for example, the FCA's Feedback Statement on Distributed Ledger Technology.

11 See https://www.fca.org.uk/news/statements/cryptocurrency-derivatives.

cryptocurrencies or tokens issued through an ICO. While the FCA statement is not definitive (and a case-by-case factual analysis would be needed), this means that firms would likely need to be authorised under the FSMA to deal in, advise on or arrange transactions in cryptocurrency derivatives, or provide any other regulated services relating to cryptocurrency derivatives in the UK.

In its April 2018 statement, the FCA also indicated that it does not consider cryptocurrencies to be currencies or commodities for regulatory purposes under MiFID II. This is relevant for assessing which regulatory rules would apply to cryptocurrency derivatives, as specific rules apply to certain categories of derivatives, such as commodity derivatives or derivatives where the underlying is a currency or a regulated financial instrument.

Security tokens

In its Guidance on Cryptoassets, the FCA describes security tokens as virtual currencies that constitute specified investments under the RAO, excluding e-money tokens (see Section III.ii for a discussion of e-money tokens). In many cases, security tokens are likely to fall within the definition of 'securities' under the RAO, which are a subset of specified investments under the RAO. Further regulatory requirements also apply to virtual currencies that are transferable securities, such as the UK prospectus regime (see Section VII.i).

The FCA has indicated that at least some types of virtual currencies may be transferable securities, for example where blockchain is used as a distribution infrastructure for traditional securities. In particular, it identifies that traditional shares issued on a public blockchain may be transferable securities, and that some ICO tokens may 'amount to a transferable security more akin to regulated equity-based crowdfunding'.[12]

Meaning of securities

Broadly, the RAO defines securities as including:[13]

a shares;[14]

b bonds, debentures, certificates of deposit, and other instruments creating or acknowledging indebtedness;[15]

c warrants and other instruments giving entitlements to investments in shares, bonds, debentures, certificates of deposit, and other instruments creating or acknowledging indebtedness;[16]

d certificates representing certain securities: that is, certificates or other instruments that confer contractual or property rights in respect of certain types of securities held by another person and the transfer of which may be effected without the consent of that other person;[17]

e units in a CIS;[18]

12 Paragraph 6 of the FCA's written submission to the House of Commons Treasury Committee digital currencies inquiry, published 22 May 2018, available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/treasury-committee/digital-currencies/written/81677.pdf.

13 Article 3(1) RAO.

14 Article 76 RAO.

15 Articles 77, 77A and 78 RAO.

16 Article 79 RAO.

17 Article 80 RAO.

18 Article 81 RAO.

f rights under a stakeholder or personal pension scheme;[19] and
g greenhouse gas and other emission allowances.[20]

The definition of securities also includes rights or interests in these types of investments (with some exceptions, such as in relation to occupational pensions schemes, which are not generally relevant to virtual currencies).[21]

In its Guidance on Cryptoassets, the FCA provides a non-exhaustive list of factors that are indicative of a security token, including any contractual entitlement holders may have to share in profits or exercise control or voting rights in relation to the issuer's activities. Other factors may include the language used in relevant documentation, although the FCA notes that labels are not definitive and it is the substantive analysis that would determine whether or not a virtual currency is a security token.

Persons that carry on specified activities relating to securities tokens by way of business in the UK would therefore need to be authorised and have appropriate permissions under the FSMA. Relevant specified activities include dealing in (i.e., buying, selling, subscribing for or underwriting) securities as principal or as an agent,[22] arranging transactions or making arrangements with a view to transactions in the securities.[23]

Meaning of transferable securities

If the substantive characteristics of a virtual currency mean that it falls within the definition of a security, it is also necessary to consider whether that security is transferable to identify the applicable regulatory requirements.

The definition of transferable securities under the FSMA[24] cross-refers to MiFID II, which in turn defines transferable securities as 'those classes of securities which are negotiable on the capital market, with the exception of instruments of payment'.[25]

The European Commission has published various Q&As on this definition, which indicate that the concept of being negotiable on the capital market is to be interpreted broadly. In particular, the Commission states that '[i]f the securities in question are of a kind that is capable of being traded on a regulated market or MTF, this will be a conclusive indication that they are transferable securities, even if the individual securities in question are not in fact traded' but conversely, '[i]f restrictions on transfer prevent an instrument from being tradable in such contexts, it is not a transferable security'.[26]

The term 'capital market' is not defined for this purpose, but the Commission has indicated that the concept is broad, and is intended to include all contexts where buying

19 Article 82 RAO.
20 Articles 82A and 82B RAO.
21 Article 89 RAO.
22 Articles 14 and 21 RAO.
23 Article 25 RAO.
24 Section 102A(3) FSMA.
25 Article 4(1)(44) MiFID II. For this purpose, the European Commission defines instruments of payment as 'securities which are used only for the purposes of payment and not for investment. For example, this notion usually includes cheques, bills of exchanges, etc.'. See Your Questions on MiFID, http://ec.europa.eu/internal_market/securities/docs/isd/questions/questions_en.pdf.
26 Question 115, Your Questions on MiFID, updated 31 October 2008, available at http://ec.europa.eu/internal_market/securities/docs/isd/questions/questions_en.pdf.

and selling interests in securities meet.[27] This could, therefore, include a cryptocurrency exchange. This means that those types of virtual currencies that are classed as securities are also likely to qualify as transferable securities where they are traded or capable of being traded on cryptocurrency or other exchanges. They would therefore fall within the prospectus regime (discussed in Section VII.i) and other regulatory requirements that apply specifically to transferable securities.

If security tokens are not negotiable on the capital market, for example due to contractual restrictions on transfer, they may nonetheless fall within the UK crowdfunding regime for non-readily realisable securities (see below and Section V.ii).

Non-readily realisable securities

In 2014, the FCA introduced regulatory rules relating to the promotion of non-readily realisable securities. The FCA defines a non-readily realisable security as a security that is not:

a a readily realisable security: this term includes government and public securities, and securities that are listed or regularly traded on certain exchanges – note that this concept is narrower than that of a transferable security;

b a packaged product: this includes units in a regulated CIS as well as certain insurance, pension and other products;

c a non-mainstream pooled investment: this includes units in an unregulated CIS, certain securities issued by a special purpose vehicle, and rights or interests to such investments; or

d certain types of shares or subordinated debt issued by mutual societies or credit unions.[28]

It is possible that some types of virtual currencies may be both transferable securities and non-readily realisable securities.

Utility tokens

Utility tokens are not regulated financial instruments in the UK. The FCA describes utility tokens as 'tokens representing a claim on prospective services or products' and explains that they are 'tokens that do not amount to transferable securities or other regulated products and only allow access to a network or product'.[29] For example, this would include tokens that entitle the holder to access office space or to use certain software.

ii Could arrangements relating to the issue of virtual currencies involve the creation of a CIS?

Other regulatory requirements will apply if arrangements relating to the issue of a virtual currency involves the creation of a CIS. Units in a CIS are specified investments under the RAO, and establishing, operating or winding up a CIS is a regulated activity under the FSMA (subject to the exclusions discussed below in 'Collective investment undertakings and alternative investment funds').[30]

27 http://ec.europa.eu/internal_market/securities/docs/isd/questions/questions_en.pdf.

28 Glossary of the FCA Handbook, available at https://www.handbook.fca.org.uk/handbook/glossary/.

29 Paragraph 6 of the FCA's written submission to the House of Commons Treasury Committee digital currencies inquiry, available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/treasury-committee/digital-currencies/written/81677.pdf.

30 Article 51ZE RAO.

Collective investment schemes

A CIS is defined as 'any arrangements with respect to property of any description, including money, the purpose or effect of which is to enable persons taking part in the arrangements (whether by becoming owners of the property or any part of it or otherwise) to participate in or receive profits or income arising from the acquisition, holding, management or disposal of the property or sums paid out of such profits or income'.[31]

In addition, the participants in a CIS must not have day-to-day control over the management of the property; and the arrangements must provide for the contributions of the participants and the profits or income to be pooled, or for the property to be managed as a whole by or on behalf of the operator of the scheme, or both.[32]

Virtual currency structures that do not involve an investment in underlying assets (such as cryptocurrencies) or that do not provide for participants to participate in or receive profits or income from a pool (such as utility tokens) would not generally fall within the definition of a CIS.

In some cases, it is possible that the issuer of a virtual currency will itself be a CIS albeit that the virtual currency is not a unit, and holders of the virtual currency will not be unitholders, in the CIS. This may arise, for example, where the issuer raises funds from issuing virtual currency and uses the funds raised to acquire assets or make other investments for the benefit of unitholders in the issuance vehicle (but not the holders of the virtual currency).

Collective investment undertakings and alternative investment funds

If a virtual currency is a CIS, it may also be a collective investment undertaking (CIU), an alternative investment fund (AIF), or both.

A CIU an EU-wide concept that is similar but not identical to that of a CIS.[33] The European Securities and Markets Authority (ESMA) has issued guidelines on the characteristics of a CIU, which provide that an undertaking will be a CIU where:

> *(a) the undertaking does not have a general commercial or industrial purpose; (b) the undertaking pools together capital raised from its investors for the purpose of investment with a view to generating a pooled return for those investors; and (c) the unitholders or shareholders of the undertaking – as a collective group – have no day-to-day discretion or control. The fact that one or more but not all of the aforementioned unitholders or shareholders are granted day-to-day discretion or control should not be taken to show that the undertaking is not a collective investment undertaking.*[34]

31 Section 235(1) FSMA.

32 Section 235(2) and (3) FSMA. PERG 9.4 of the Perimeter Guidance module of the FCA Handbook provides further guidance on the definition of a CIS and the Financial Services and Markets Act 2000 (Collective Investment Schemes) Order 2001 identifies certain types of arrangements that do not amount to a CIS.

33 Note that the UK concept of a CIS is generally understood to encompass the EU-wide concept of a CIU, in keeping with the principle that the UK regulatory perimeter is wide enough to encompass relevant EU regulatory concepts and requirements.

34 ESMA Guidelines on key concepts of the AIFMD, August 2013, https://www.esma.europa.eu/sites/default/files/library/2015/11/2013-611_guidelines_on_key_concepts_of_the_aifmd_-_en.pdf.

An AIF is a CIU that raises capital from a number of investors with a view to investing it in accordance with a defined investment policy for the benefit of those investors, and that does not require authorisation under the Undertakings for Collective Investment in Transferable Securities Directive.[35]

In general, a substantive analysis would be required to determine whether a particular virtual currency may be an AIF. If so, the virtual currency would need an authorised or regulated manager (AIFM) that would be responsible for compliance with the UK regulatory requirements applicable to AIFs and AIFMs. Managing an AIF is a regulated activity under the FSMA.[36]

III BANKING AND MONEY TRANSMISSION

In the UK, a number of banking activities should be considered in the context of virtual currencies, including whether any activities performed in connection with virtual currencies might give rise to the acceptance of deposits, the issuance of electronic money or the performance of payment services.

i Accepting deposits

Accepting deposits in the UK is a regulated activity for the purposes of the FSMA if money received by way of deposit is lent to others or any other activity of the person accepting the deposit is financed wholly, or to a material extent, out of the capital of or interest on money received by way of deposit.[37]

For these purposes, a deposit is defined as a sum of money paid on terms:

a under which it will be repaid, with or without interest or premium, and either on demand or at a time or in circumstances agreed by or on behalf of the person making the payment and the person receiving it; and

b that are not referable to the provision of property (other than currency) or services or the giving of security.

Typically, virtual currencies would not give rise to deposit-taking activity, as issuing virtual currencies does not usually involve the deposit of a sum of money to the issuer (assuming there is an issuer); virtual currencies would often be issued on receipt of other cryptocurrencies. Even if the other cryptocurrencies were to be treated as money, they are rarely issued on terms under which they would be repaid to the holder.

ii Electronic money

The issuance of electronic money is also a regulated activity in the UK.[38] It is a criminal offence to issue electronic money without the appropriate authorisation.

35 Directive 2009/65/EC, as amended. It seems unlikely that virtual currencies would be structured so as to comply with the Undertakings for Collective Investment in Transferable Securities (UCITS) regime.

36 Article 51ZC RAO. Note that Article 51ZG RAO provides that the operator of a CIS that is also an AIF will not be carrying on a regulated activity under Article 51ZE RAO, provided that the AIF is managed by a person that is authorised or registered to do so. Article 51ZG RAO also provides a similar exclusion for operators of CIS that are UCITS.

37 Article 5 RAO.

38 Article 63 EMRs and Article 9B RAO for credit institutions, credit unions and municipal banks.

Under the EMRs, electronic money is defined as electronically (including magnetically) stored monetary value as represented by a claim on the electronic money issuer that is issued on receipt of funds for the purpose of making payment transactions; is accepted as a means of payment by persons other than the issuer; and is not otherwise excluded under the EMRs.

A key characteristic for a product to be electronic money is that it must be issued on receipt of funds (i.e., it is a prepaid product whereby a customer pays for the spending power in advance).

In general, cryptocurrencies are unlikely to give rise to the issuance of electronic money as they do not typically give rise to stored monetary value (the value of cryptocurrencies is often highly volatile, determined by market forces, and is not related to any specific currency). Furthermore, most cryptocurrencies do not give holders a contractual right of claim against an issuer of the relevant cryptocurrency, are not issued on receipt of funds and (with some exceptions) are not usually issued for the purpose of making payment transactions.

That said, however, there are some types of virtual currencies that do function much like electronic money. The FCA refers to virtual currencies that meet the definition of electronic money under the EMRs as e-money tokens in its Guidance on Cryptoassets. In particular, stablecoins are specifically designed to maintain value and are often pegged to underlying assets, including currencies such as the US dollar. If a stablecoin is issued on receipt of fiat currency, such as US dollars, and represents a claim on the issuer such that a holder may be entitled to redeem that stablecoin for fiat currency, this may well constitute the issuance of electronic money by the issuer.

However, in its Guidance on Cryptoassets, the FCA notes stablecoins may be structured and stabilised in different ways, which may impact their regulatory characterisation. For example, some types of stablecoins may be crypto-collateralised, asset-backed or algorithmically stabilised. The FCA notes that, depending on how it is structured, a stablecoin 'could be considered a unit in a collective investment scheme, a debt security, e-money or another type of specified investment. It might also fall outside of the FCA's remit. Ultimately, this can only be determined on a case-by-case basis.'

iii Payment services

The provision of payment services in the UK is regulated under the PSRs. It is a criminal offence to provide payment services without the appropriate authorisation or registration.[39]

Payment services comprise the following activities when carried out as a regular occupation or business activity in the UK:[40]

a services enabling cash to be placed on a payment account and all of the operations required for operating a payment account;

b services enabling cash withdrawals from a payment account and all of the operations required for operating a payment account;

c the execution of payment transactions, including transfers of funds on a payment account with a user's payment service provider or with another payment service provider, including:
- execution of direct debits, including one-off direct debits;
- execution of payment transactions through a payment card or a similar device; and
- execution of credit transfers, including standing orders;

39 Regulation 138 PSRs.

40 Part 1, Schedule 1 PSRs.

d the execution of payment transactions where the funds are covered by a credit line for a payment service user, including:
- execution of direct debits, including one-off direct debits;
- execution of payment transactions through a payment card or a similar device; and
- execution of credit transfers, including standing orders;

e issuing payment instruments[41] or acquiring payment transactions;[42]

f money remittance;[43]

g payment initiation services;[44] and

h account information services.[45]

There are, however, a number of exclusions listed in Part 2, Schedule 2 PSRs (activities that do not constitute payment services), including exemptions similar to the limited network exclusion and the electronic communications exclusion described above in relation to the issuance of electronic money.

As the name suggests, the PSRs regulate services rather than products per se. However, as noted in Section II.i, while the FCA has stated that it does not consider cryptocurrencies to generally fall within the UK regulatory perimeter for financial services, they may do so where they do not form part of other regulated products or services. One such example may be where a cryptocurrency is used as an intermediary currency in money remittance, for instance, converting fiat currency into a digital currency and then back into a different fiat currency to transmit to the recipient (e.g., pounds sterling to Bitcoin to US dollar transactions).

As noted above, money remittance is a regulated payment service, and the interposition of a cryptocurrency in the remittance process would not mean that such a service ceases to be characterised as a regulated payment service; rather it will continue to be treated as a regulated payment service. That said, however, the interposition of a cryptocurrency into a money remittance process does not necessarily make the cryptocurrency itself a regulated financial product or mean its exchange for fiat currency would always constitute a regulated payment service. In its draft Guidance on Cryptoassets,[46] the FCA explained that '[t]he PSRs cover each side of the remittance, but do not cover the use of cryptoassets in between

41 A payment service by a payment service provider contracting with a payer to provide a payment instrument to initiate payment orders and to process the payer's payment transactions (Article 2(1) PSRs).

42 A payment service provided by a payment service provider contracting with a payee to accept and process payment transactions that result in a transfer of funds to the payee (Article 2(1) PSRs).

43 A service for the transmission of money (or any representation of monetary value), without any payment accounts being created in the name of the payer or the payee, where funds are received from a payer for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee; or funds are received on behalf of, and made available to, the payee (Article 2(1) PSRs).

44 An online service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider (Article 2(1) PSRs).

45 An online service to provide consolidated information on one or more payment accounts held by the payment service user with another payment service provider, or with more than one payment service provider, and includes such a service whether information is provided in its original form or after processing; or only to the payment service user or to the payment service user and to another person in accordance with the payment service user's instructions (Article 2(1) PSRs).

46 Consultation Paper CP19/3 on Guidance on Cryptoassets published by the FCA on 23 January 2019, available at https://www.fca.org.uk/publication/consultation/cp19-03.pdf.

which act as the vehicle for remittance.' In general, the arrangements and services offered by persons using such cryptocurrencies need to be considered holistically to determine whether, notwithstanding the use of a cryptocurrency, those persons may be engaging in regulated payment services.

IV ANTI-MONEY LAUNDERING

i Money Laundering Regulations 2017

The Money Laundering Regulations 2017 (MLRs)[47] apply to relevant persons, including banks and other financial institutions, when they are carrying on certain regulated activities.[48] The substantive requirements of the MLRs do not apply generally, in respect of other (unregulated) business or activities.[49] Therefore, a factual analysis is required to determine whether the business activities or transactions relating to a particular virtual currency fall within the scope of the MLRs. Under the current MLRs, this will often depend on whether the virtual currency is itself a regulated financial instrument.

On 15 April 2019, HM Treasury published a consultation on the transposition of the EU's Fifth Money Laundering Directive (5MLD),[50] which is scheduled to be implemented by 10 January 2020. 5MLD brings certain specific cryptoasset-related activities within the scope of the EU anti-money laundering (AML) regime and, as anticipated in the final report of the Cryptoasset Taskforce, the UK government proposes to go beyond the requirements of 5MLD relating to virtual currencies in a number of respects (see Section XI).

If the MLRs do apply, relevant persons will need to comply with requirements under the MLRs, including requirements to:

a take appropriate steps to identify and assess the risks of money laundering and terrorist financing to which the business is subject, and establish and maintain policies, controls and procedures to mitigate and manage effectively such risks;[51] and

b carry out customer due diligence to identify customers, verify customers' identities, and assess the purpose and intended nature of a business relationship or transaction.[52]

47 Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. The MLRs implement requirements of the fourth EU Money Laundering Directive (Directive (EU) 2015/849).

48 These activities are listed at Regulation 10 MLRs, in respect of banks and financial institutions. Other relevant persons under the MLRs include auditors, insolvency practitioners, external accountants and tax advisers, independent legal professionals, trust or company service providers, estate agents, high value dealers and casinos, as such terms are defined in the MLRs (Regulation 8). Also see Section XI in relation to the future expansion of the scope of UK anti-money laundering regulation to virtual currency exchanges and wallet providers.

49 The categories of relevant persons under the MLRs are defined by reference to their carrying on of relevant activities.

50 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

51 Regulations 18 and 19 MLRs.

52 Regulations 28 MLRs. Relevant persons must carry out customer due diligence when establishing a new business relationship and in certain other circumstances set out at Regulation 27 MLRs.

The MLRs also include requirements relating to record keeping and identification of beneficial ownership.[53]

The FCA is responsible for overseeing supervision of the UK's AML regime under the MLRs by financial services institutions,[54] and the UK government has indicated that the FCA will also be the supervisor for firms within scope of the regime by virtue of cryptoasset-related activities. Breach of the MLRs may carry both criminal and civil penalties.[55]

ii FCA 'Dear CEO' letter on cryptoassets and financial crime

In June 2018, the FCA issued a Dear CEO letter advising banks on how to handle financial crime risks posed by cryptoassets, which the FCA defines in the letter as 'any publicly available electronic medium of exchange that features a distributed ledger and a decentralised system for exchanging value'.[56] This was the first guidance the FCA has published specifically on how banks should address financial crime risks posed by cryptoassets or cryptocurrencies.

The letter states that enhanced scrutiny may be necessary where banks provide services to cryptoasset exchanges or clients whose source of wealth arises or is derived from cryptoassets, and when arranging, advising or participating in an ICO. The FCA also reminds banks of its 2012 review[57] of bank defences against investor fraud, noting that retail customers may be at heightened risk of falling victim to fraud where they invest in ICOs.

V REGULATION OF EXCHANGES

The regulatory rules (if any) applicable to virtual currency exchanges will depend on the regulatory characterisation of the types of virtual currencies that are traded on the exchange.

i Exchanges for virtual currencies that are specified investments or MiFID financial instruments (or both)

The operator of an exchange on which virtual currencies qualifying as transferable securities or other MiFID financial instruments can be traded may need to be authorised under the FSMA as the operator of a multilateral trading facility (MTF) or an organised trading facility (OTF).[58]

An MTF is 'a multilateral system . . . which brings together multiple third-party buying and selling interests in financial instruments – in the system and in accordance with non-discretionary rules – in a way that results in a contract'.[59]

53 Parts 4 and 5 MLRs.

54 The FCA took on this oversight role from January 2017, under the Oversight of Professional Body Anti-Money Laundering and Counter Terrorist Financing Supervision Regulations 2017.

55 The MLRs create three criminal offences, of contravening a relevant requirement (Regulation 86), prejudicing an investigation (regulation 87) and providing false or misleading information (Regulation 88). Civil sanctions for breach of the MLRs include fines, suspension or removal of authorisation, prohibitions on firms' senior managers and injunctions (regulations 76, 77, 78 and 80).

56 FCA 'Dear CEO' letter on Cryptoassets and Financial Crime, dated 11 June 2018, available at https:// www.fca.org.uk/publication/correspondence/dear-ceo-letter-cryptoassets-financial-crime.pdf.

57 'Banks' defences against investment fraud: Detecting perpetrators and protecting victims', Financial Services Authority, June 2018, available at https://www.fca.org.uk/publication/archive/banks-defences-against-investment-fraud.pdf.

58 Articles 25D and 25DA RAO.

59 Article 3(1) RAO, which cross-refers to the definition at Article 4(22) MiFID II.

The definition of an OTF is similar, but it relates only to trading of non-equity instruments (i.e., bonds, structured finance products, emission allowances and derivatives), and an OTF does not need to have non-discretionary rules setting out how buying and selling interests are to be matched.[60]

Depending on the way in which the exchange or trading platform operates, the operator may also be carrying on other regulated activities under the FSMA, such as dealing in investments as a principal or agent, arranging deals in investments or making arrangements with a view to investments, sending dematerialised instructions, managing investments or safeguarding and administering investments.

ii Operators of crowdfunding platforms

In the UK, some but not all types of crowdfunding or peer-to-peer financing fall within the regulatory perimeter.

Operating a loan-based or investment-based crowdfunding platform is generally regulated under the FSMA, as discussed below. Depending on how the platform operator structures its business, in some cases it may also be managing a CIU, in which case it will be subject to requirements that apply to AIFMs (see Section II.ii, 'Collective investment undertakings and alternative investment funds').

The FCA also regulates payment services relating to other types of crowdfunding, such as donation-based crowdfunding (i.e., where people give money to businesses or organisations they want to support).

Operating a loan-based crowdfunding platform

Operating a loan-based crowdfunding platform has been regulated under the FSMA since 1 April 2014 through the introduction of a new regulated activity of 'operating an electronic system in relation to lending'.[61]

Loan-based crowdfunding platforms allow investors to extend credit directly to consumers or businesses to make a financial return from interest payments and the repayment of capital over time. For this purpose, credit includes a cash loan and any other form of financial accommodation.[62]

Some types of virtual currencies may involve the provision of credit, so an exchange that operates an electronic system enabling it to bring issuers of such virtual currencies and investors together may need to be authorised under the FSMA and have permission to operate an electronic system in relation to lending.

In June 2019, the FCA published new rules for loan- and investment-based crowdfunding platforms, including in relating to platforms' governance, systems and controls, and wind-down plans. The new rules also aim to better protect investors by

60 Article 3(1) RAO, which cross-refers to the definition at Article 4(23) MiFID II.

61 Article 36H RAO.

62 Articles 36H(9) and 60L RAO.

introducing minimum information requirements, an investment limit for retail customers and a requirement for platforms to assess investors' knowledge and experience where they have not received advice. Most of these new requirements apply from 9 December 2019.[63]

Operating an investment-based crowdfunding platform

Operating an investment-based crowdfunding platform where consumers invest in securities issued by newly established businesses is regulated, as the platform operator will be arranging for others to buy those securities.[64]

Therefore, an exchange on which securities tokens can be traded may be subject to FCA rules relating to operating an investment-based crowdfunding platform. As indicated in Section II.i, specific regulatory rules apply to the promotion of non-readily realisable securities.

VI REGULATION OF MINERS

There is no specific UK regulatory regime that would capture the activities of miners.

As virtual currencies that are mined are likely to be cryptocurrencies (or other types of virtual currencies that are not regulated financial instruments in the UK), it therefore seems less likely that the activities of miners would be regulated.

However, in some cases, a more detailed factual analysis may be needed as to whether miners' activities involve them carrying on a regulated activity in the UK by way of business for the purposes of the FSMA or under the PSRs or EMRs (as discussed in Sections II and III).

VII REGULATION OF ISSUERS AND SPONSORS

Regulation will depend on the regulatory or legal characterisation of the virtual currency in question.

i Prospectus regime

A prospectus may be needed in respect of securities tokens or other types of virtual currency that are characterised as transferable securities.

An issuer of transferable securities must publish a prospectus where an offer of those securities is made to the public in the UK (unless an exemption applies). Breach of this requirement is a criminal offence.[65]

63 FCA Policy Statement PS19/14: Loan-based ('peer-to-peer') and investment-based crowdfunding platforms: Feedback to CP18/20 and final rules, published 4 June 2019 and available at https://www.fca.org.uk/publications/policy-statements/ps19-14-loan-based-peer-to-peer-investment-based-crowdfunding-platforms-feedback-final-rules.

64 Arranging is a specified activity under Article 25 RAO.

65 Section 85(1) FSMA. A prospectus is also required where an application is made for securities to be admitted to trading on a regulated market such as the London Stock Exchange (Section 85(2) FSMA). However, this is unlikely to be relevant for virtual currencies.

ii Underwriting or issuing securities as regulated activities

A sponsor may be carrying on the regulated activity of dealing in investments as principal to the extent that it underwrites an issue of securities tokens.[66] In this case, the sponsor would need to be authorised and have relevant permissions under the FSMA.

It is also possible that the issuer of the securities tokens would be dealing in investments as principal (as the concept of selling includes issuing or creating securities).[67] However, in many cases the issuer is unlikely to be carrying on this activity by way of business and so would not be carrying on a regulated activity for the purposes of Section 19 FSMA.[68]

iii Deposits and electronic money

See Section III for a discussion about whether issuing a virtual currency may involve accepting deposits or issuing electronic money.

VIII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

Nefarious activity concerning virtual currencies have been well-publicised, whether ICOs alleged to be Ponzi schemes, in which 'investors' seek the return of their contributions; hacks of virtual currency exchanges; and thefts of private keys or schemes seeking to defraud holders of their virtual currency via fake exchanges or wallets. In that context, virtual currencies give rise to a number of unique civil and criminal enforcement issues under English law, almost all of which are untested by the English courts.

We address below (1) the regulatory risks arising from unauthorised activities in relation to virtual currencies, and (2) certain liability and enforcement issues regarding virtual currencies, which arise in both the criminal and civil contexts. At the core of the latter is the debate around the correct private law characterisation of virtual currencies, and whether they can be characterised as money or property as a matter of English law. Such characterisation issues will need to be analysed for any type of virtual currency before determining whether any cause of action (at common law or in equity) is available.

i Regulatory enforcement with respect to virtual currencies

FCA enforcement issues

To the extent that an activity in relation to a virtual currency is a regulated activity and the firm engaged in those activities is authorised, it will be subject to the FCA's High Level Principles for Businesses and other Rules set out in the FCA Handbook in relation to its conduct of that regulated activity. The High Level Principles include the obligations to conduct business with integrity; to take reasonable steps to implement appropriate systems and controls; to observe proper standards of market conduct; to treat customers fairly; and to manage conflicts of interest appropriately. Breach of the Principles or underlying Rules may result in an enforcement investigation by the FCA resulting in a range of potential

66 Article 14(1) RAO.

67 See the definition of selling at Article 3(1) RAO.

68 Also see FCA guidance at PERG 13.3, Q15A in the Perimeter Guidance sourcebook of the FCA Handbook, available at https://www.handbook.fca.org.uk/handbook/PERG/13/3.html.

disciplinary sanctions, including financial penalty, restriction of business, suspension of authorisation and public censure. Individuals within the firm may also face liability under the applicable individual accountability regimes.

Firms whose activities bring them within scope of the MLRs face separate enforcement risks for breach of the requirements in the MLRs. These are strict liability requirements that may be treated by the FCA as civil or criminal infringements without the need to show any criminal intent. Again, individuals within the firm may also face liability where a breach of the rules by the firm has been committed through their actions or neglect.

Firms and individuals may face civil or criminal liability for market abuse in relation to virtual currencies that fall within the scope of the market abuse regime, regardless of whether the activities in question are regulated activities or within scope of the MLRs. So for example, publishing misleading information relating to a security token may result in liability for market manipulation, regardless of the status of the individual publishing the information. Similarly trading security tokens in an abusive manner, for example to ramp prices, may result in liability for market manipulation regardless of whether the person engaged in the trading is regulated. Market abuse may be treated as a civil offence punishable by a fine, or a criminal offence punishable by a fine or imprisonment, or both.

As noted above, to the extent that an activity in relation to a virtual currency is a regulated activity, failure to be authorised will be in breach of the general prohibition under Section 19 FSMA. Breach of the general prohibition is a criminal offence pursuant to Section 23 FSMA. Further, an officer of the company (including a director, chief executive, manager, secretary and shadow director) will also be guilty of a criminal offence where it was committed with his or her consent or as a result of his or her neglect.[69] The penalty for an offence under Section 23 FSMA is imprisonment for two years or an unlimited fine, or both.

In parallel, the FCA is able to pursue civil remedies to seek injunctive relief against the party engaged in the unauthorised activity (and its officers) restraining the contravention and ordering them to take such steps as the English courts may direct to remedy it.[70]

The FCA also has the power to seek a restitution order if a person has contravened a relevant requirement under the FSMA (or been knowingly concerned in the contravention of such a requirement), and either profits have accrued to that person, or one or more persons have suffered a loss or been otherwise adversely affected (or both).[71] Theoretically, that could amount to ordering an issuer to pay the FCA 'such sum as appears to the Court to be just'. The English courts may then direct the FCA to distribute such sum to primary or secondary purchasers of a virtual currency, as persons who have suffered a loss pursuant to Section 382 FSMA.

While the FCA has issued consumer warnings in relation to virtual currency risks, it has yet to publicly announce any enforcement action concerning virtual currencies or ICOs (unlike regulators in other jurisdictions, notably the Securities and Exchange Commission and the Commodity Futures Trading Commission in the United States).

69 Section 400(1) FSMA.

70 Section 380 FSMA.

71 Section 382 FSMA.

Statutory remedies under the FSMA

An agreement made by an unauthorised person in breach of the general prohibition is unenforceable against the other contracting party.[72] In addition, the contracting party has a statutory right to recover money or property paid or transferred under the agreement (where, if the transfer is a virtual currency, the private law characterisation issues are pertinent) or to be compensated for any resulting loss suffered by his or her, or both.[73] The English courts can, however, exercise their discretion to uphold an otherwise unenforceable agreement, or order money and property paid or transferred to be retained where it is just and equitable to do so.[74]

ii Liability and enforcement issues regarding virtual currencies

Virtual currencies as money

Virtual currencies, unlike fiat currencies, do not embody units of account sanctioned by the state. Thus, the English courts will have to determine whether virtual currencies are money as a matter of statutory construction, or as a matter of private law. The point appears highly arguable, given that virtual currencies have many similar features to money (including their own unique unit of account, and as a store of value that can be transferred).

A related issue is whether it is possible to obtain a judgment in the English courts in a virtual currency. The English courts have previously determined that, as a matter of procedure, they can give judgments in a foreign currency (and not just sterling),[75] and could be urged to give judgment in a virtual currency, perhaps by awarding delivery in specie rather than damages.

Virtual currencies as property

Criminal liability

Virtual currencies would appear to be capable of falling within the definition of property under Section 4(1) of the Theft Act 1968, which covers 'money and all other property, real or personal, including things in action and other intangible property', opening the door to the prosecution of a theft of virtual currency under English law.

Depending on the facts, frauds concerning virtual currencies are capable of prosecution, either as common law conspiracy to defraud or under the Fraud Act 2006 (as fraud by false representation).[76]

Civil liability

Virtual currencies do not fit neatly within the category of either choses in possession or choses in action, and their private law characterisation has yet to be tested by the English courts.

It is more likely that virtual currencies are a species of intangible property. *Armstrong DLW GmbH v. Winnington Networks Ltd*[77] held that the carbon allowances under an EU trading had permanence and stability, were definable, had value, and were identifiable by, and able to be transferred to, third parties, and treated them as intangible property.

72 Section 26 FSMA.

73 Section 26(2) FSMA.

74 The English courts have this discretion under Section 28 FSMA.

75 *Miliangos v. George Frank* [1976] ACC 443.

76 Section 2 Fraud Act 2006.

77 *Armstrong DLW GmbH v. Winnington Networks Ltd.*

In contrast, the Court of Appeal in *Your Response Ltd v. Datastream Business Media*[78] concluded that information in a database is not property (although the physical medium on which it is recorded may be). By analogy, if virtual currencies on blockchain are treated as lines of data or information on a database, common law actions that depend on possession (such as the tort of conversion) will not be available, following *OBG Ltd v. Allan*.[79]

If virtual currencies can be treated as intangible property, restitutionary claims at common law or in equity are available to the lawful holder of title to such virtual currency, provided the virtual currency can be traced and the defendant identified.

In the context of blockchain technology, while the location of a virtual currency can typically be established, the legal person behind the public key may be more difficult to identify. In *CMOC v. Persons Unknown*,[80] the High Court demonstrated its ability to adapt to new technology (and the fraud associated with it), granting a without-notice freezing injunction against persons unknown when a company's email was infiltrated and emails were fraudulently sent in the name of a senior individual, directing payments to be made out of the company's bank accounts. Accordingly, the possibility to seek injunctive relief (which may be particularly useful where virtual currency exchanges are involved) remains open in relation to virtual currencies. The English courts have, in unreported cases, made disclosure orders requiring a defendant to disclose e-wallets under his or her control, in relation to claims for cryptocurrency.[81]

IX TAX

There is no specific UK tax legislation applicable to cryptocurrencies, although HMRC Brief 9 of 2014 sets out the basic principles.

i Basic direct tax position

Unlike sterling, but like other currencies, purchases and sales of virtual currencies will generally need to be translated into sterling to determine the UK tax consequences.

For most individuals and companies, buying a cryptocurrency and then selling it will give rise to profits or losses that may be subject to tax, the profit or loss being calculated by translating the purchase and sale price into sterling at the prevailing exchange rate.

For individuals, generally purchases and sales of cryptocurrencies will be taxed as a capital gains item. For companies, profits and losses on exchange movements between currencies (including between sterling and a cryptocurrency) will be taxed as trading profits and losses or possibly as capital gains and losses under normal corporation tax rules for companies liable to UK corporation tax.

Income received by an individual or company from trading transactions in cryptocurrencies (e.g., from sales by a trader of stock priced in a cryptocurrency) will be taxed as part of normal trading income, translated into sterling at the prevailing rate. Similarly, it is probable that income from currency mining would be taxed as part of other income, although the position on this is not entirely clear.

78 *Your Response Ltd v. Datastream Business Media* [2014] EWCA Civ 291.

79 *OBG v. Allan* [2007] UKHL 21.

80 *CMOC v. Persons Unknown* [2017] EWHC 3599 (Comm).

81 'Identifying and tracing the origins and flows of cryptocurrency', *Journal of International Banking and Financial Law*, Volume 34(3), 2019, pp. 173–174.

ii VAT

Supplies in the course of a trade priced in cryptocurrency will be liable to VAT in the normal way as for supplies in any other currency.

Income received from cryptocurrency mining will generally be outside the scope of VAT on the basis that the activity does not constitute an economic activity for VAT purposes. Income received by miners for other activities (e.g., the provision of verification services) will generally be exempt from VAT as falling within the category of transactions concerning payments, etc.

No VAT is due on the exchange of cryptocurrencies for sterling or other currencies.

X OTHER ISSUES

i Data protection

The EU General Data Protection Regulation (GDPR)[82] introduced significant changes to the UK data privacy rules from May 2018. It has various implications for the storage and processing of personal data[83] associated with transactions in virtual currencies, particularly for cryptocurrencies and other virtual currencies that use distributed ledger or blockchain technology.

A detailed discussion of GDPR goes beyond the scope of this chapter. However, the decentralised and immutable nature of a blockchain means that particular technical or practical solutions may be needed to comply with GDPR requirements in this context, such as the requirement to delete or anonymise personal data when it is no longer needed,[84] and the rights of individuals to require correction, to be forgotten and to object to the processing of their data.[85]

ii Financial promotions

Under Section 21 FSMA, a person must not communicate an invitation or inducement to engage in investment activity in the course of business unless that person is authorised under the FSMA or the content of the communication is approved by an authorised person. This may include promotions relating to virtual currencies. Breach of Section 21 FSMA is a criminal offence.

In its draft Guidance on Cryptoassets, the FCA indicates that it expects market participants to 'apply the financial promotion rules and communicate financial promotions for products and services, whether regulated or unregulated, in a way which is clear, fair and not misleading'. Regulated firms must also make clear in their promotions whether they relate to regulated or unregulated products and activities and must not suggest that their authorisation extends to unregulated products.

82 Regulation (EU) 2016/679, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

83 i.e., information relating to an identified or identifiable natural person, such as a name or national identification number, Article 4(1) GDPR.

84 Article 5(1)(e) GDPR.

85 Articles 16, 17 and 21 GDPR.

iii Application of regulatory rules to unregulated business

Regulated firms should also consider the extent to which regulatory rules and principles apply even in relation to unregulated areas of their business, such as trading in or offering services relating to cryptocurrencies.

For example, in June 2018, the Prudential Regulation Authority (PRA) issued a Dear CEO letter indicating that PRA-regulated firms should have regard to the PRA's Fundamental Rules 3, 5 and 7 in the context of existing or planned exposures to cryptoassets. These rules require firms to act in a prudent manner, to have effective risk strategies and risk management systems, and to deal with the PRA in an open and cooperative way and to disclose to the PRA anything of which it would reasonably expect notice.[86]

In its draft Guidance on Cryptoassets, the FCA also highlighted that its Principles for Business 3, 4 and 11 generally apply to unregulated activities of authorised firms (although for Principle 3 this is limited to unregulated activities that may have a negative impact on the integrity of the UK financial system, or the ability of the firm to meet the suitability threshold condition). These principles require firms to: take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems; maintain adequate financial resources; and deal with the FCA in an open and cooperative way, and disclose to the FCA anything of which it would reasonably expect notice.

Similarly, most staff at firms regulated by both the PRA and FCA are required to comply with the FCA's individual conduct rules, including a requirement to observe proper standards of market conduct.[87] The individual conduct rules apply in respect of both regulated and unregulated activities.[88]

iv Other legal and regulatory considerations

There are myriad other legal and regulatory issues and considerations that are or may be relevant in the context of virtual currencies. These include intellectual property (and whether, for example, a private key is intellectual property), cybersecurity, consumer protection laws (including in relation to unfair terms and distance selling requirements), outsourcing requirements, sanctions and conflicts of laws analysis.

86 Dear CEO letter on Existing or planned exposure to cryptoassets, published 28 June 2018, available at https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2018/existing-or-planned-exposure-to-crypto-assets.pdf. Conversely, following a consultation in November 2017 (CP17/37), the FCA confirmed in its July 2018 policy statement (PS18/18) that it would not extend application of Principle 5 of the FCA's Principles for Businesses, which requires authorised firms to observer proper standards of market conduct, to their unregulated activities. The policy statement is available at https:// www.fca.org.uk/publication/policy/ps18-18.pdf.

87 Rule 5, Individual Conduct Rules, at COCON 2.1.5 R in the Code of Conduct module of the FCA Handbook, available at https://www.handbook.fca.org.uk/handbook/COCON/2/1.html.

88 Rules COCON 1.1.6 R and 1.1.7 R in the Code of Conduct module of the FCA Handbook, available at https://www.handbook.fca.org.uk/handbook/COCON/1/1.html.

XI LOOKING AHEAD

i HM Treasury consultation on the regulatory perimeter

HM Treasury is expected to publish a consultation later in 2019 exploring legislative change to potentially broaden the UK regulatory perimeter to include further types of virtual currencies that are currently unregulated. This was one of the further actions recommended in the final report on the House of Commons Treasury Committee's inquiry into the use of digital currencies and distributed ledger technology in the UK.[89]

In its final report, the Treasury Committee strongly recommended that regulation of cryptoassets should be introduced, covering consumer protection and AML risks at a minimum. The report also called on the government and regulators to evaluate further the risks of cryptoassets and consider whether their growth should be encouraged through a proportionate regulatory response.

ii 5MLD

5MLD will bring cryptocurrency wallet providers and exchange platforms within the scope of the EU AML framework from 10 January 2020.[90]

Among other things, 5MLD will require these entities to have in place policies and procedures to detect, prevent and report money laundering and terrorist financing. It will also introduce registration or licensing requirements for virtual currency exchange platforms and custodian wallet providers that safeguard private cryptographic keys, potentially bringing these entities within the scope of regulation for the first time.

HM Treasury has consulted on its proposed implementation of 5MLD in the UK, which would 'gold-plate' 5MLD requirements in various respects. Whereas 5MLD uses a relatively narrow definition of virtual currencies as those that are not issued or backed by any central authority (broadly corresponding to exchange tokens or cryptocurrencies), HM Treasury has proposed extending the new requirements to security tokens and utility tokens. HM Treasury also proposes extending these requirements to crypto-to-crypto virtual currency exchange platforms, which again do not fall within the scope of 5MLD itself.[91] The FCA is also expected to consult on its approach to 5MLD later in 2019, in its role as supervisor under the regime.

89 The inquiry webpage is available athttps://www.parliament.uk/business/committees/committees-a-z/commons-select/treasury-committee/inquiries1/parliament-2017/digital-currencies-17-19/. Key conclusions and recommendations are available at https://publications.parliament.uk/pa/cm201719/cmselect/cmtreasy/910/91009.htm and the full report is available at https://publications.parliament.uk/pa/cm201719/cmselect/cmtreasy/910/91002.htm.

90 5MLD entered into force on 9 July 2018. It requires EU Member States to implement its provisions in national law by 10 January 2020. The UK government has indicated that it intends to implement the provisions of 5MLD by 10 January 2020, in accordance with this deadline.

91 HM Treasury consultation on transposition of the Fifth Money Laundering Directive, published 15 April 2019, available at https://www.gov.uk/government/consultations/transposition-of-the-fifth-money-laundering-directive.

iii EU Crowdfunding Regulation and ICOs

The EU has proposed introducing a harmonised licensing and passporting regime for both lending-based and investment-based peer-to-peer platforms under the draft Crowdfunding Regulation, which is currently making its way through the EU ordinary legislative process.[92]

During preliminary negotiations, the EU Parliament also considered including provisions to regulate ICOs in the Crowdfunding Regulation. These provisions were not included in the EU Parliament's final draft of the text, which instead calls upon the Commission to publish a separate legislative proposal on the regulation of ICOs. While the Crowdfunding Regulation is not yet finalised, this does indicate the likely direction of legislative travel: that is, seeking to regulate (rather than prohibit) ICOs in the EU and in the UK.[93]

iv FATF Recommendation 15

The Financial Action Task Force (FATF) formally adopted Recommendation 15 in June 2019, which sets requirements for what the FATF considers effective regulation and AML and counter financing of terrorism for virtual asset services providers (VASPs). VASPs are broadly defined to include any natural or legal person who as a business conducts one or more of:

a exchange between virtual assets and fiat currencies;
b exchange between one or more forms of virtual assets;
c transfer of virtual assets;
d safekeeping or administration of virtual assets or instruments enabling control over virtual assets (or both); and
e participation in and provision of financial services related to an issuer's offer or sale of a virtual asset (or both).

It also sets out how the FATF standards apply to activities or operations involving virtual assets. The UK as part of the G20 has already affirmed that it will align with the FATF standards for virtual assets and VASPs. Countries have 12 months to abide by the Recommendation, with a review set for June 2020. It is expected that the 'gold-plated' implementation of 5MLD by the UK will extend to include the requirements under the FATF Recommendations (where not already included).

92 The Commission adopted its proposal for a regulation on European crowdfunding service providers in March 2018, available at https://ec.europa.eu/info/publications/180308-proposal-crowdfunding_en. The European Parliament's Committee on Economic and Monetary Affairs (ECON) sets out draft provisions to regulate ICOs in its draft report on the proposed Crowdfunding Regulation, published on 10 August, available at http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-626.662&format=PDF&language=EN&secondRef=02.

93 The Crowdfunding Regulation will not apply until after October 2019 (i.e., after the UK is due to leave the EU) and so it is not clear whether the UK will introduce similar requirements. However, Ashley Fox MEP, who drafted the EU Parliament's ECON Committee report, is a British MEP. Therefore, it seems plausible that the UK may take an approach to regulating ICOs similar to the proposals in draft report.

Chapter 29

UNITED STATES

Sidley Austin LLP[1]

I INTRODUCTION TO THE LEGAL AND REGULATORY FRAMEWORK

In the United States, multiple regulators may assert overlapping jurisdiction for market participants transacting in virtual currencies or other digital assets. Legal and regulatory regimes to be considered include those overseen at the federal level by the US Securities and Exchange Commission (SEC), the US Commodity Futures Trading Commission (CFTC), the Financial Crimes Enforcement Network (FinCEN), the Office of Foreign Asset Control (OFAC) of the US Treasury Department and federal banking regulators. In addition, US states have legal and regulatory regimes that should be considered when undertaking virtual currency activities, including state money transmitter requirements, the New York 'BitLicense', and state 'blue sky' laws applicable to digital asset securities transactions. Commercial, tax and bankruptcy laws should also be considered in virtual currency transactions.

The SEC regulates digital asset transactions if they are offered or traded as securities or if they are offered through a collective investment fund. The SEC has published reports and guidance related to the offering of, secondary trading in and investing in digital asset securities. The Securities Act of 1933 (the Securities Act) makes it unlawful for any person to make use of the means or instrumentalities of interstate commerce to offer or sell a security unless such security is registered with the SEC or there is an applicable exemption from the registration requirements. A threshold consideration in trading or investing in digital assets is whether the particular digital asset is a security and therefore subject to the federal securities laws. The inquiry into whether a particular digital asset is a security and thus subject to the federal securities laws is based on the facts and circumstances surrounding the offer and sale of each digital asset. Further, registration requirements under the Securities Exchange Act of 1934 (the Exchange Act) extend to market participants involved in the offer or secondary trading of digital asset securities. The SEC's digital asset guidance, settlement orders and enforcement actions help to shed light on how the legal and regulatory framework applies to different digital asset business models.

The CFTC, the primary federal derivatives regulator in the United States, regulates certain transactions in virtual currencies as commodities. The CFTC has jurisdiction over virtual currency derivatives transactions and has brought civil enforcement cases against

1 Michael S Sackheim is senior counsel; Nathan A Howell, Geoffrey F Aronow, James B Biery, James Munsell, Lilya Tessler, Michael A Levy, Pamela J Martinson, David E Teitelbaum, Dominique Gallego, Andrew P Blake, Teresa Wilton Harmon and Alex R Rovira are partners; Daniel Engoren, Christopher Masterson, David A Miller, Verity A Van Tassel Richards and Sean A Smith are associates; and Kenny Terrero is counsel at Sidley Austin LLP. Special thanks to Ivet A Bell and Daniel J Applebaum, associates, for their editorial assistance with this chapter.

virtual currency derivatives trading facilities alleging failures to comply with the CFTC's requirements for regulated derivatives exchanges. The CFTC also has broad authority to bring civil enforcement actions where there is fraud or manipulation with respect to any commodity transaction in interstate commerce, even if the transaction is not a derivatives transaction (i.e., even if it is not a futures contract, swap or option). Because virtual currencies are commodities as the term is defined in the Commodity Exchange Act (CEA), the CFTC maintains that it can police any fraudulent, deceptive or manipulative activity involving virtual currency spot, cash and forward transactions, making the CFTC a key player in the US regulatory regime for virtual currencies.

FinCEN regulates money services transmitters and has issued interpretative guidance for virtual currency exchanges. Some states also require licensing of money transmitters, including those that facilitate the transmission of virtual currencies. The federal banking agencies have closely monitored banking activities involving virtual currencies. In mid-2018, the former Chair of the CFTC testified before Congress that there may be a gap in the oversight of virtual currencies that are not securities, stating that regulatory oversight through state money transmission regulations is not satisfactory and that the US Congress might consider giving the CFTC or another federal agency the authority to write new rules for spot digital asset markets, including new registration requirements. Each of the 50 states in the United States has its own securities and financial services regulator, many of whom are involved in monitoring activities regarding virtual currencies and in some cases have brought enforcement actions where they found fraud or money laundering.

This chapter reviews the web of concurrent and overlapping regulatory jurisdiction and developments in the United States regarding virtual currency and digital assets, including regulatory requirements applicable to intermediaries and trading platforms.

II SECURITIES AND INVESTMENT LAWS

In this Section, we discuss securities and commodities laws and regulations that apply to digital assets. See Section V (Regulation of Miners), Section VI (Regulation of Issuers and Sponsors) and Section VII (Criminal Fraud and Enforcement) for discussions that also implicate securities and commodities laws as they relate to digital assets.

i Digital asset securities

A threshold consideration in trading or investing in digital assets is whether the particular digital asset is a security and therefore subject to the federal securities laws. Section 5 of the Securities Act makes it unlawful for any person to make use of the means or instrumentalities of interstate commerce to offer or sell a security unless such security is registered with the SEC or there is an applicable exemption from the registration requirements.[2] In July 2017, the SEC issued a Report of Investigation (the DAO Report) analysing whether the offer and sale of a digital asset was subject to the federal securities laws.[3] The digital asset in question was a token issued by an entity known as the Decentralized Autonomous Organisation (DAO), an unincorporated organisation. The DAO was created by a German corporation

2 Securities Act § 5 (codified at 15 U.S.C. § 77e (2018)).

3 Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Exchange Act Release No. 81207 (July 25, 2017) (DAO Report), https://www.sec.gov/litigation/investreport/34-81207.pdf.

named Slock.it UG, and by the time the DAO Report was issued, the DAO had offered and sold approximately 1.15 billion DAO tokens in exchange for a total of approximately 12 million Ether, a virtual currency used on the Ethereum blockchain, which had a value, at the time the offering closed, of approximately US$150 million.

The SEC analysed whether the DAO token was an investment contract, and therefore a security, as defined by the Supreme Court of the United States (the Court) in the seminal case, *SEC v. WJ Howey Co*,[4] which involved the offer and sale of interests in an orange grove. The Court defined an investment contract as an investment of money in a collective enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others. In the DAO Report, the SEC approvingly quoted from the Court's observation that this definition embodies a 'flexible rather than a static principle, one that is capable of adaptation to meet the countless and variable schemes devised by those who seek the use of the money of others on the promise of profits'.[5]

The DAO token represented an ownership interest in a collective vehicle whereby monies raised by the token sales would be used to fund various blockchain projects that could provide holders with a return on their investment. DAO token holders could vote on which projects to fund; however, before a project could be voted on, it first had to be reviewed and approved by one of the DAO's curators, which was a group of individuals selected by Slock. These curators performed crucial security functions and maintained ultimate control over which proposals could be submitted to, voted on and funded by the DAO.

Presented with this fact pattern, the SEC concluded that the DAO token was an investment contract. There was (1) an investment of money (in this case, Ether) in (2) a common enterprise (the DAO platform), with the (3) expectation of profits (promotional materials informed investors that the DAO was a for-profit entity whose objective was to fund projects in exchange for a return on investment) (4) derived from the efforts of others (Slock.it and the curators). Although the DAO token holders did have voting rights, the SEC concluded that the voting rights were limited, and that the holders were substantially reliant on the managerial efforts of Slock.it and the curators. As an investment contract, the DAO Report noted that the offer and sale of the DAO token was required to be registered under the Securities Act (unless a valid exemption from registration applied), and that platforms trading DAO tokens that met the definition of an exchange would need to register as such under the Exchange Act.

Following the issuance of the DAO Report, blockchain market participants focused on the two elements of the investment contract test that could potentially lead to a different conclusion than the one reached by the SEC with respect to the DAO token. Under the *Howey* test, the first two elements would likely always be met: an investment of money in a common enterprise. However, the question arises of whether token projects could avoid triggering the second two elements of the *Howey* test – the expectation of profits and being derived from the efforts of others. For example, what if the value of the token was not primarily to provide a return on investment, but rather to enable the holder to do something that he or she could not do without a token, such as purchase a good or service available through the network on which the token was created? Or, what if the holder's expectation of profits did not rely on the efforts of others, but rather the holder had the power to create his or her own return on investment? What if there was no potential for profit or capital appreciation at all?

4 328 U.S. 293 (1946).

5 id., at 299.

In December 2017, the SEC provided further clarity for blockchain participants in a cease-and-desist order issued to Munchee Inc, a California corporation (Munchee).[6] Munchee commenced business operations when it launched an iPhone app in 2015 (Munchee App), which allowed users to review meals and upload pictures. In early 2017, Munchee sought to raise capital through the development and issuance of a digital token (MUN token). The issuance of the MUN token purported to address the issues raised by the SEC in the DAO Report. For example, Munchee characterised the MUN tokens as utility tokens, because there was a real use case for the MUN token in connection with the already existing Munchee App. The SEC's order quickly addressed the first two elements of the *Howey* analysis and focused on the manner of sale of the MUN token. The order stated that 'investors' expectations were primed by Munchee's marketing of the MUN token offering', and listed several examples of how the marketing of the MUN tokens offered investors hope and expectations that their investments would increase in value. Munchee's marketing materials also stated that Munchee would 'ensure that MUN token is available on a number of exchanges in varying jurisdictions', thereby ensuring MUN token holders could buy and sell MUN on secondary markets to realise the purported increases in value. Additionally, the SEC noted that Munchee and its agents marketed the MUN token to people interested in investing in digital assets instead of marketing to restaurant owners and food critics. Directly addressing the utility token argument that developed after the DAO Report, the SEC stated that 'even if MUN tokens had practical use at the time of the offering, it would not preclude the token from being a security. Determining whether a transaction involves a security does not turn on labelling [. . .] but instead requires an assessment of the economic realities underlying the transaction.'

In June 2018, the SEC's Director of the Division of Corporation Finance, William Hinman, made an important speech in which he provided further guidance refining the SEC's approach to analysing when a digital asset is offered as an investment contract and therefore is a security.[7] He framed the question differently by focusing not on the digital asset itself, but rather on the circumstances surrounding the digital asset and the manner in which it is sold. He conceded that the token, or 'whatever the digital information packet is called', is not a security all by itself, just as the interests in the orange grove in *Howey* were not. The token is 'simply code'. Instead, 'the way it is sold – as part of an investment; to non-users; by promoters to develop the enterprise – can be, and, in that context, most often is, a security – because it evidences an investment contract. And regulating these transactions as securities transactions makes sense.' When there is information asymmetry between promoters or founders and investors, then the protections of the Securities Act – namely, disclosure and liability for material misstatements and omissions – are necessary and appropriate.

On the other hand, Hinman noted that '[i]f the network on which the token or coin is to function is sufficiently decentralised – where purchasers would no longer reasonably expect a person or group to carry out essential managerial or entrepreneurial efforts – the assets may not represent an investment contract. Moreover, when the efforts of the third party are no longer a key factor for determining the enterprise's success, material information

6 *In the Matter of Munchee Inc*, Securities Act Release No. 10445, Admin. File No. 3-18304 (Dec. 11, 2017), https://www.sec.gov/litigation/admin/2017/33-10445.pdf.

7 William Hinman, Director, US Sec. and Exch. Comm'n Div. of Corp. Fin., 'Digital Asset Transactions: When Howey Met Gary (Plastic), Remarks at the Yahoo Finance All Markets Summit: Crypto' (June 14, 2018), https://www.sec.gov/news/speech/speech-hinman-061418.

asymmetries recede.' Hinman put both Bitcoin and Ether into this latter category – as digital assets where there is no central third party whose efforts are a key determining factor in the common enterprise, and where it would seem that the disclosure regime of the federal securities laws would provide little value to the holders of Bitcoin and Ether.

In other words, as has always been the case, an investment contract can be made out of virtually any asset, including digital assets, so long as the investor is reasonably expecting profits from the promoter's efforts. As Hinman reiterated, 'the economic substance of [a] transaction determines the analysis, not the label'. Similarly, an investment contract can also be unwound or undone. The management contract for the orange grove can be terminated. With regard to digital assets, it is a novel idea that this transition or change would or could occur as a result of changes to the facts and circumstances associated with the token, without necessarily any action taken or to be taken by the holder. In response to Hinman's speech, many market participants sought clarity as to the precise mix of facts that would distinguish the sale of digital assets from a securities transaction.

In April 2019, the SEC's Strategic Hub for Innovation and Financial Technology (FinHub)[8] released a framework (the Framework) for applying the investment contract analysis set forth in *Howey* and its progeny to digital assets to 'help market participants assess whether the federal securities laws apply to the offer, sale, or release of a particular digital asset'.[9] While the Framework does not create new law, it provides the SEC staff's view as to whether specific facts commonly present in the digital asset context make it more or less likely that specific elements of the *Howey* test are met. In addition, the Framework provides additional factors to consider that may be indicative of whether a digital asset is offered with 'consumptive' intent (as opposed to investment intent) and highlights particular facts that may change over time to be considered in determining whether and when a subsequent offering and sale of a digital asset previously sold as a security may no longer be considered an offering and sale of a security. Specifically with respect to 'virtual currency', the Framework notes that the ability to use the virtual currency immediately to make payments for goods and services without having to convert it to another digital asset or real currency may make it less likely the *Howey* test is met.

On the same day that the Framework was released, the SEC Division of Corporation Finance issued its first no-action letter relating to the offer and sale of a digital asset.[10] In providing relief that the relevant tokens would not be required to register under the Securities Act or the Exchange Act, the Division of Corporation Finance particularly noted that: (1) the issuer would not use funds from the token sale to develop the related application and that the application would be fully developed and operational at the time tokens are sold; (2) the tokens would be immediately usable for their intended functionality (purchasing air charter services) at the time they are sold; (3) the tokens could not be transferred external to the application; and (4) the tokens would always be sold at a fixed price and redeemable for services valued at that price.

8 The SEC launched FinHub in October 2018 as a 'resource for public engagement on the SEC's FinTech-related issues and initiatives', including digital assets. FinHub is staffed by personnel from across the SEC's divisions and offices.

9 'Framework for 'Investment Contract' Analysis of Digital Assets', US Sec. and Exch. Comm'n (Apr. 3, 2019), https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.

10 *TurnKey Jet, Inc.*, SEC No-Action Letter (Apr. 3, 2019), https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm.

ii Certain market participants

In planning to negotiate, effect, clear or settle transactions in virtual currencies that are securities,[11] market participants should evaluate whether their activities may trigger registration and related requirements under the framework of the Exchange Act, which is administered by the SEC. In particular, market participants should be aware of the definitions of broker,[12] dealer,[13] exchange,[14] alternative trading system (ATS),[15] clearing agency[16] and transfer agent.[17] The SEC has increasingly made clear that it intends to regulate virtual currencies to the extent of its existing authority in these areas.

For example, the SEC's Division of Trading and Markets and Division of Enforcement published a joint statement in which they noted that trading venues on which individuals buy tokens that are securities as part of an ICO (or in secondary transactions) may be required to register with the SEC as a national securities exchange or otherwise avail themselves of an exemption from registration, such as by filing as an ATS.[18] The SEC addressed this same point in its July 2017 issuance of the DAO Report.[19] There, it found that certain platforms that facilitated trading of certain DAO tokens that constituted securities appeared to violate Section 5 of the Exchange Act by engaging in activities that met the definition of an exchange (i.e., matching the orders of multiple buyers and sellers for execution using non-discretionary methods) without being registered as such or relying on an available exemption from registration.

Below is a general overview of some of the most common registration types and related requirements under the Exchange Act that may be triggered by transacting in or otherwise facilitating transactions in virtual currencies that are securities.

Broker-dealers

Registration with the SEC is generally required for any entity that meets the statutory definition of a broker or dealer, including with respect to their activities in virtual currencies that are securities. A securities broker includes any person who is engaged in the business of effecting transactions in securities for the accounts of others.[20] Exceptions from the broker definition are also available to a bank,[21] as defined under the Exchange Act, that only engages in certain securities activities (e.g., third-party brokerage arrangements, trust activities, stock purchase plans and sweep accounts).[22] A securities dealer includes any person engaged in the business of buying and selling securities for such person's own account, regardless of whether through a broker or otherwise. However, the definition also includes an exception

11 As described herein, many, but not all, virtual currencies are viewed by US regulators as being securities.

12 15 U.S.C. § 78c(a)(4) (2018).

13 id., § 78c(a)(5).

14 id., § 78c(a)(1).

15 17 C.F.R. § 242.300(a) (2018).

16 15 U.S.C. § 78c(a)(23) (2018).

17 id., § 78c(a)(25).

18 Divs. of Enf't and Trading and Mkts., US Sec. and Exch. Comm'n, 'Statement on Potentially Unlawful Online Platforms for Trading Digital Assets' (Mar. 7, 2018), https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading.

19 DAO Report, footnote 3.

20 15 U.S.C. § 78c(b)(4) (2018).

21 id., § 78c(a)(6).

22 id., § 78c(a)(4)(B).

for persons who are not in the business of dealing in securities. Specifically, the dealer-trader exception states that a person is generally not acting as a dealer where that person trades for his or her own account but not as part of a regular business. The SEC Division of Trading and Markets has also published a significant volume of guidance in the form of no-action letters that further address when a person may be engaged in broker or dealer activities, but SEC staff would not recommend enforcement action by the agency if the person engages in the specified activities without becoming registered. Consideration of that guidance is therefore also relevant to a market participant's own evaluation of whether it is acting as broker or dealer and must register.

Section 15(a)(1) of the Exchange Act generally requires registration of any person who acts as a broker or dealer, as described above, and who uses instrumentalities of interstate commerce[23] 'to effect any transaction in, or to induce or attempt to induce the purchase or sale of, any security (other than an exempted security or commercial paper, bankers acceptances or commercial bills)'.[24] Registration with the SEC requires the submission of Form BD (Uniform Application for Broker-Dealer Registration) through the Central Registration Depository, which is currently the central licensing and registration system operated by the Financial Industry Regulatory Authority, Inc (FINRA). Unless a broker-dealer is a member of a US national securities exchange and generally limits its securities activities to trading on that exchange, it must also become a member of FINRA, which is the national securities association in the United States for broker-dealers that, among other things, has surveillance and enforcement authority over its members. To apply to become a member of FINRA, broker-dealers must complete a detailed new membership application that requires an applicant to provide FINRA with, among other things, detailed written supervisory and compliance procedures. On 6 July 2018, FINRA issued Regulatory Notice 18-20 requesting member firms to notify FINRA if 'it, or its associated persons or affiliates, currently engages, or intends to engage, in any activities related to digital assets, such as cryptocurrencies and other virtual coins and tokens'.[25] The notice also reminds FINRA members of the requirement to submit a Continuing Membership Application pursuant to NASD Rule 1017 and receive approval from FINRA before engaging in a material change in business operations, but does not state that activities related to digital assets would per se be a material change.

Among other considerations regarding acting as a broker-dealer in respect of virtual currencies that are securities, market participants should consider the compatibility of their planned activities with the existing requirements of the SEC's financial responsibility rules.[26] For example, broker-dealers are generally required by SEC Rule 15c3-3(b)(1) to promptly obtain and thereafter maintain control of all fully paid and excess margin securities that are

23 id., § 78c(a)(17).

24 id., § 78o(a)(1). A broker-dealer and its personnel must also, separately and independently, comply with the securities (or 'blue sky') laws, and in particular the broker-dealer and agent and salesperson registration requirement, of each US state and territory (including the District of Columbia) in which the broker-dealer and its personnel conduct securities activities, even if the broker-dealer does not maintain a place of business in such state.

25 Fin. Indus. Regulatory Auth. Inc., Regulatory Notice 18-20, 'FINRA Encourages Firms to Notify FINRA if they Engage in Activities related to Digital Assets' (July 6, 2018).

26 See Lilya Tessler, David M Katz, Steffen Hemmerich & Daniel Engoren, 'Custody of Digital Asset Securities: A Proposal to Address Open Questions for Broker-Dealers Under the SEC's Customer Protection Rule', Blockchain 2019: A Sidley Austin LLP Educational Series (Mar. 18, 2019), https://www.sidley.com/en/insights/publications/2019/03/custody-of-digital-assets-securities.

carried for the account of a customer.[27] The terms fully paid securities[28] and excess margin securities[29] are separately defined in Rule 15c3-3, and broker-dealers frequently satisfy this obligation today through custody of the securities at a clearing agency (e.g., the Depository Trust Company (DTC) or a custodian bank) because those locations are recognised in Rule 15c3-3(c) as being under the control of the broker-dealer. In terms of virtual currencies that are securities, however, the same recognised good control locations may not be practicable depending on the characteristics of the financial instruments and how they are issued and maintained. Accordingly, a broker-dealer should evaluate its planned activities against the SEC's control requirement, including whether it may need to apply to the SEC for the recognition of a new control location pursuant to Rule 15c3-3(c)(7). On 8 July 2019, the SEC's Division of Trading and Markets and FINRA's Office of General Counsel issued a joint statement on broker-dealer custody of digital asset securities that contained regulatory considerations applicable to various market participants, including those related to noncustodial broker-dealer models, the application of SEC Rule 15c3-3 to broker-dealer custody and books and records and financial reporting rules.[30]

Exchanges and ATSs

In general under the Exchange Act, an exchange is defined to mean a system that brings together the orders for securities of multiple buyers and sellers, and uses established, non-discretionary methods (whether by providing a trading facility or by setting rules) under which such orders interact with each other.[31] As noted above, the SEC and its staff have emphasised recently that market participants who facilitate transactions in virtual currencies that are securities may come within the definition of an exchange, and that any such entity or group of persons that performs the functions typically provided by a securities exchange must either register as a national securities exchange, pursue an exemption from the definition of an exchange[32] or become an ATS that is operated by a broker-dealer. Under the regulatory framework administered by the SEC, an ATS is a national securities exchange; however, it is exempt from such registration provided that it complies with the requirements of the SEC's Regulation ATS.[33]

The regulatory burdens associated with registering and operating as a national securities exchange are significantly greater than those associated with an ATS. For example, the registration process for an exchange involves completing and submitting Form 1 to the SEC, which is published for public notice and comment. By contrast, the submission of Form ATS to the SEC is not subject to the same public notice and comment process. Additionally, under Section 6(b)(2) of the Exchange Act,[34] a national securities exchange is generally required

27 17 C.F.R. § 240.15c3-3(b)(1) (2018).

28 id., § 240.15c3-3(a)(3).

29 id., § 240.15c3-3(a)(5).

30 Div. of Trading and Mkts., US Sec. and Exch. Comm'n, Office of Gen. Counsel, Fin. Indus. Regulatory Auth. Inc., 'Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities' (July 8, 2019), https://www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities.

31 15 U.S.C. § 78c(a)(1) (2018); 17 C.F.R. § 240.3b-16(a) (2018).

32 The SEC has authority to exempt an entity from the exchange definition. 15 U.S.C. § 78e (2018); 17 C.F.R. § 240.3b-16(e) (2018).

33 17 C.F.R. § 240.3a1-1(a)(2) (2018).

34 15 U.S.C. § 78f(b)(2) (2018).

to permit any broker-dealer or natural person associated with a broker-dealer to become a member of the exchange. An ATS is not subject to this obligation, and therefore it has more discretion over who it allows to participate. The rules of an exchange also generally cannot be amended without the advance submission of rule changes to the SEC pursuant to Section 19(b)(1) of the Exchange Act, which are published for public notice and comment and may take up to 240 calendar days for the SEC to approve or disapprove.[35] No such rule filing requirement currently applies to an ATS that wishes to changes its operating procedures. Changes to the operating procedures of an ATS are made pursuant to an amendment to Form ATS or Form ATS-N, are not approved by the SEC, and need only be submitted to the SEC 30 days (at most) in advance of implementation of the change.[36] Exchanges are also subject to the requirements of the SEC's Regulation Systems Compliance and Integrity (Regulation SCI),[37] which require detailed policies, procedures and monitoring to ensure the integrity and resiliency of most exchange systems. ATSs are generally not subject to these same requirements, unless they exceed certain volume thresholds in a given security.[38]

Clearing agencies

Market participants who plan to engage in post-trade activities related to transactions in virtual currencies that are securities should closely examine whether their activities may rise to the level of performing clearing agency functions. The term clearing agency under Section 3(a)(23)(A)[39] of the Exchange Act is defined broadly to generally include any person who:

a acts as an intermediary in making payments or deliveries, or both, in connection with transactions in securities;

b provides facilities for the comparison of data regarding the terms of settlement of securities transactions, to reduce the number of settlements of securities transactions or for the allocation of securities settlement responsibilities;

c acts as a custodian of securities in connection with a system for the central handling of securities whereby all securities of a particular class or series of any issuer deposited within the system are treated as fungible and may be transferred, loaned or pledged by bookkeeping entry, without physical delivery of securities certificates; or

d otherwise permits or facilitates the settlement of securities transactions or the hypothecation or lending of securities without physical delivery of certificates.

In practice, this reaches firms that operate as a central counterparty to novate, net and guarantee securities settlement obligations or that operate as a central securities depository (e.g., DTC) to transfer ownership by book entry. However, the SEC has also recognised in guidance that it may capture firms performing other common types of functions in the securities markets. These include, but are not limited to collateral management activities –

35 id., § 78s(b)(1).

36 17 C.F.R. § 242.304(a)(2)(i)(A) (2018).

37 id., § 242.1000 et seq.

38 id., § 242.1000 (defining SCI alternative trading system).

39 15 U.S.C. § 78c(a)(23)(A) (2018).

involving calculating collateral requirements and facilitating the transfer of collateral between counterparties and trade matching services – whereby an intermediary compares trade data to reduce the number of settlements or to allocate settlement responsibilities.[40]

Like the registration and operation of a national securities exchange, the registration and operation of a registered clearing agency involves significant regulatory requirements that include, but are not limited to, the submission of proposed rule changes to the SEC and compliance with Regulation SCI. Accordingly, market participants who believe that their activities may come within the clearing agency definition may wish to consider whether they nonetheless qualify for certain exclusions from the clearing agency definition in Section 3(a)(23)(B) of the Exchange Act,[41] or whether it would be appropriate to pursue an exemption from registration. The SEC has authority to provide conditional or unconditional exemptions from registration pursuant to Section 17A(b)(1) of the Exchange Act.[42]

Transfer agents

Where a market participant provides services to the issuer of a virtual currency that is a security, it should consider the implications of the transfer agent definition. The definition of a transfer agent in Section 3(a)(25) of the Exchange Act[43] includes any person who engages on behalf of a securities issuer in:

a countersigning such securities upon issuance;
b monitoring the issuance of such securities with a view to preventing unauthorised issuance;
c registering the transfer of the issuer's securities of the issuer;
d exchanging or converting the securities; or
e transferring record ownership of the securities by bookkeeping entry without physical issuance of securities certificates.

In turn, Section 17A(c)(1) of the Exchange Act requires that, except as otherwise provided in the Exchange Act, it is unlawful for any transfer agent, unless registered, to use US instrumentalities of interstate commerce 'to perform the function of a transfer agent with respect to any security registered under Section 12 [of the Exchange Act] or which would be required to be registered except for the exemption from registration provided by subsections (g)(2)(B) or (g)(2)(G) of that section'.[44] Therefore, transfer agent registration is not required unless a person acts as a transfer agent in respect of such securities. The SEC also has authority pursuant to Section 17A(c)(1) of the Exchange Act[45] to provide conditional or unconditional exemptions from transfer agent registration.

40 'Clearing Agency Standards for Operation and Governance', 76 Fed. Reg. 14495 (Mar. 16, 2011), https://www.gpo.gov/fdsys/pkg/FR-2011-03-16/pdf/2011-5182.pdf.
41 15 U.S.C. § 78c(a)(23)(B) (2018).
42 id., § 78q-1(b)(1).
43 id., § 78c(a)(25).
44 id., § 78q-1(c)(1).
45 id.

iii Commodities laws

The CFTC is the US federal regulatory agency that administers and enforces the CEA, having jurisdiction over derivatives, that is, futures contracts, options and swaps involving commodities.[46] CEA Section 1a(9) defines a commodity as '[enumerated agricultural products], and all other goods and articles [. . .] and all services, rights, and interests [. . .] in which contracts for future delivery are presently or in the future dealt in'.[47]

Virtual currencies are not fiat currencies; they are not legal tender issued by a sovereign government. In 2017, the CFTC interpreted virtual currency to encompass any digital representation of value that functions as a medium of exchange, and any other digital unit of account used as a form of currency.[48] In December 2017, the CFTC permitted the trading of Bitcoin futures contracts and Bitcoin binary options on two CFTC-regulated futures exchanges, referred to as designated contract markets (DCMs).[49] Therefore, as of December 2017, Bitcoin satisfied the condition in the 'commodity' definition of being the underlying asset for a futures contract. Receptiveness to trading of Bitcoin futures on US DCMs has been mixed. For example, in the first quarter of 2019, CBOE Global Markets Inc announced that it would discontinue the trading of Bitcoin futures,[50] while in June 2019, the CFTC approved LedgerX's application to be a DCM for the trading of physically settled Bitcoin futures by retail investors.[51]

In 2014, the then-current CFTC Chair advised Congress that derivatives contracts based on virtual currencies fall within the CFTC's jurisdiction.[52] Beginning in 2015, the CFTC commenced several administrative enforcement actions involving virtual currencies. In settling an enforcement case with Coinflip, Inc, an unregistered trading facility on which Bitcoin options were traded, the CFTC determined that Bitcoin and all virtual currencies are commodities within the definition of CEA Section 1a(9), that Bitcoin is not a fiat currency, that Bitcoin options are commodity options and therefore are CFTC-regulated swaps, and that the trading facility was therefore required to be registered with the CFTC as either a swap execution facility (SEF) or DCM.[53] The CFTC determined that all virtual currencies fell within the CEA definition of commodity, notwithstanding that no regulated futures contract based on any virtual currency was traded at that time.

In 2016, in another administrative enforcement proceeding, the CFTC entered into a settlement with Bitfinex, which operated an online platform for retail customers exchanging

46 7 U.S.C. § 1 et seq. (2018). The CFTC's regulations are at 17 C.F.R. § 1 et seq. (2018).

47 7 U.S.C. § 1a(9) (2018).

48 'Retail Commodity Transactions Involving Virtual Currency', 82 Fed. Reg. 60,335, 60,338 (Dec. 20, 2017) (Retail Transactions).

49 Commodity Futures Trading Comm'n, 'CFTC Statement on Self-Certification of Bitcoin Products by CME, CFE and Cantor Exchange', CFTC Release No. 7654-17 (Dec. 1, 2017), https://www.cftc.gov/PressRoom/PressReleases/pr7654-17; see also 'Bitcoin Futures Are Here: The Story So Far', Nasdaq (Dec. 11, 2017), https://www.nasdaq.com/article/bitcoin-futures-are-here-the-story-so-far-cm889984.

50 See Alexander Osipovich, 'Cboe Abandons Bitcoin Futures', Wall Street Journal (Mar. 18, 2019), https://www.wsj.com/articles/cboe-abandons-bitcoin-futures-11552914001.

51 Commodity Futures Trading Comm'n, 'CFTC Approves LedgerX LLC as a Designated Contract Market, CFTC Release No. 7945-19 (June 25, 2019), https://www.cftc.gov/PressRoom/PressReleases/7945-19.

52 Timothy Massad, 'Testimony of Chairman Timothy Massad before the U.S. Senate Committee on Agriculture, Nutrition and Forestry' (Dec. 10, 2014), https://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-6.

53 See *In the Matter of: Coinflip, Inc, d/b/a Derivabit, et al.*, CFTC No. 15-29 (Sept. 17, 2015).

and trading various virtual currencies, including Bitcoin, on a margined, leveraged or financed basis, without actually delivering the Bitcoin to the retail customers, but instead holding the Bitcoin in wallets that it owned and controlled, in violation of the CEA's retail commodity transactions provision that is intended to protect individual retail customers from abuse involving unregulated speculative commodities investments.[54] The CFTC again determined that virtual currencies are commodities, and that the transactions were illegal, off-exchange commodity futures contracts because they were transacted with retail investors and did not result in actual delivery. Retail investors are individuals who are not eligible contract participants (e.g., sophisticated investors, specified regulated entities and large entities). Retail commodity transactions are treated under the CEA as futures contracts and must be traded on regulated DCMs. The CFTC required Bitfinex to register with the CFTC as a futures commission merchant because it engaged in soliciting or accepting orders for retail commodity transactions and received funds from retail customers in connection with the transactions.

In 2017, the CFTC published a proposed interpretation on the meaning of the term actual delivery in the context of retail transactions in virtual currencies, in order to determine whether off-exchange transactions involving virtual currencies fall within the CEA's retail commodity transactions prohibition.[55] The CFTC advised that while the test for whether actual delivery has occurred would be determined by facts and circumstances, it will look to whether, no later than within 28 days, the retail customer is able to take possession and control of the entire quantity of the virtual currency purchased, regardless of whether the purchase was leveraged or financed, and use it freely in commerce without the seller or platform retaining any security interest in the virtual currency. The CFTC advised that a book-out or cash settlement, or where the virtual currency is retained in an omnibus wallet where the platform operator retains the private keys, will not constitute actual delivery. The CFTC recognised that a virtual currency trading platform may have relationships with depositories for its customers, but the platform (and any financing provider) may not retain an interest in the virtual currency deposited in the depository.

In March 2018, in the enforcement case *CFTC v. McDonnell and CabbageTech Corp* (*d/b/a Coin Drop Markets*), a federal district court judge confirmed the CFTC's view that all virtual currencies are commodities under the CEA definition, and that spot transactions in virtual currencies are subject to the CFTC's anti-fraud and anti-manipulation enforcement authority.[56] Notwithstanding that only Bitcoin futures contracts are currently traded on CFTC-regulated DCMs, the court found that all virtual currencies are goods that fall within the CEA's definition of commodity, as excerpted above. The court also held that the CEA grants the CFTC enforcement authority over fraud or manipulation not only in derivatives markets, but also over the underlying virtual currencies spot markets pursuant to CFTC Rule 180.1, which prohibits employing a manipulative or fraudulent scheme not only in connection with derivatives transactions but 'in connection with [. . .] a contract of sale of any

54 *In the Matter of: BFXNA Inc d/b/a Bitfinex*, CFTC No. 16-19 (June 2, 2016).

55 Retail Transactions, footnote 48. In February 2018, the CFTC and the United Kingdom's Financial Conduct Authority signed an arrangement to collaborate and support innovative firms through each other's fintech initiatives. 'Cooperation Arrangement', US CFTC-UK FCA (Feb. 18, 2018), https://www.cftc.gov/sites/default/files/idc/groups/public/@internationalaffairs/documents/file/cftc-fca-cooparrgt021918.pdf.

56 *CFTC v. McDonnell and CabbageTech, Corp. d/b/a Coin Drop Markets*, No. 1:18-cv-00361-JBW-RLM, slip op. (E.D.N.Y. Mar. 6, 2018) (mem.); see also *CFTC v. My Big Coin Pay, Inc.*, No. CV 18-10077-RWZ (D. Mass. Sept. 26, 2018) (mem.).

commodity in interstate commerce'. The court also concluded that the CFTC's jurisdiction over virtual currencies is concurrent with the jurisdiction of other federal and state regulators and criminal prosecutors. In August 2018, following a non-jury trial, the case was decided in favour of the CFTC and the court issued a permanent injunction and assessed civil monetary penalties against the defendants.[57]

With respect to virtual currency swap transactions, the CFTC's jurisdictional authority is not based on the underlying asset being a commodity. Therefore, even if a virtual currency is not a commodity, if the transaction is determined to be a swap, the CFTC would have regulatory authority over the swap transaction, which means that the CFTC's swap dealer, reporting, record-keeping and other swaps compliance rules would apply.

The CFTC has also advised that virtual tokens and virtual coin offerings may be commodities or derivatives contracts depending on the particular facts and circumstances.[58] All CFTC registrants must become members of the National Futures Association (NFA), which requires that its members who trade, broker or advise about virtual currency derivatives notify the NFA of this activity and make appropriate risk disclosures to their customers.[59]

III BANKING AND MONEY TRANSMISSION

Below is an overview of the regulation of virtual currency activities by US federal prudential banking regulators (the Board of Governors of the Federal Reserve System (Fed), the Office of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation (FDIC)) and the Consumer Financial Protection Bureau (CFPB), as well as the regulation of virtual currency activities by the US states, specifically as money transmission or a related money services business activity.[60] The US federal prudential banking regulators and the CFPB have not sought to actively regulate the virtual currencies and virtual currency activities of their supervised entities to date.[61] The US states, on the other hand, have adopted a broad spectrum of approaches concerning the application of money transmission and related laws and regulations to virtual currency activities, including requiring in certain circumstances a specialised virtual currency licence or a more general money transmission licence (MTL).

57 *CFTC v. McDonnell and CabbageTech, Corp. d/b/a Coin Drop Markets*, No. 1:18-cv-00361-JBW-RLM (E.D.N.Y. Aug. 23, 2018), https://www.cftc.gov/sites/default/files/2018-08/enfdropmarketsorder082318.pdf.

58 LabCFTC, 'A CFTC Primer on Virtual Currencies', 14 (Oct. 17, 2017), https://www.cftc.gov/sites/default/files/idc/groups/public/documents/file/labcftc_primercurrencies100417.pdf. In May 2019, the CFTC published its enforcement manual, which is applicable to trading and dealing in all commodities (including virtual currencies) and which provides insight into the agency's approach to investigations and enforcement proceedings.

59 See Notice I-18-13, Nat'l Futures Assoc. (Aug. 9, 2018) (NFA Notice), https://www.nfa.futures.org/news/newsNotice.asp?ArticleID=5036.

60 This section does not address securities or commodities laws and regulations, tax laws or commercial law questions, such as the mechanism for taking a security interest in virtual currencies. The money services business registration requirements of FinCEN are discussed in Section IV.

61 The information in this section was accurate as at 30 June 2019. Regulation of virtual currencies on both the federal and state levels is rapidly evolving and subject to change.

i Federal banking regulators

While the CFTC, the SEC[62] and FinCEN[63] have issued guidance or made public pronouncements that begin to define the scope of their jurisdiction concerning virtual currencies, the Fed, OCC, FDIC and CFPB have largely adopted a more limited 'wait and see' approach.

Fed

In a press conference in late 2017, the former Chair of the Fed, Janet Yellen, responded to a question regarding the Fed's policy regarding Bitcoin as follows:

> *It is a highly speculative asset, and the Fed doesn't really play any role – any regulatory role with respect to Bitcoin other than assuring that banking organisations that we do supervise are attentive, that they're appropriately managing any interactions they have with participants in that market and appropriately monitoring anti-money laundering Bank Secrecy Act, you know, responsibilities that they have.*[64]

In short, Chair Yellen confirmed that the Fed does not have any direct role in regulating Bitcoin or, by implication, the class of other virtual currencies with similar features.

Nonetheless, the Fed continues to monitor the use and development of virtual currencies and the role of Fed-regulated financial institutions in virtual currency activities through the Digital Assets Working Group of the Financial Stability Oversight Council (FSOC), which includes the CFTC, the SEC and FinCEN.[65] In its 2018 Annual Report, FSOC stated '[d]igital assets do not presently appear to pose a threat to the stability of the financial system . . . the estimated market capitalization of digital assets is still relatively small . . . for context, [it] is less than 1 percent of the market capitalization of U.S. stocks' and '[d]igital assets have limited use in the real economy of financial transactions'.[66] The report went on to note, however, that the value and use of virtual currencies could grow rapidly and federal agencies will continue to monitor risk to the banking system.[67] Public comments by current Fed governors, including Chairman Powell, are consistent with these positions.[68] As

62 See Section II.

63 See Section IV.

64 Janet Yellen, 'Transcript of Chair Yellen's Press Conference of December 13, 2017', 12 (Dec. 13, 2017), https://www.federalreserve.gov/mediacenter/files/FOMCpresconf20171213.pdf.

65 'Examining the Growing World of Virtual Currencies and the Oversight Conducted by the U.S. Securities and Exchange Commission and the U.S. Commodity Futures Trading Commission: Hearing Before the S. Comm. on Banking, Hous., and Urban Affairs', 115th Cong. 11 (2018) (Testimony of CFTC Chairman J Christopher Giancarlo); Financial Stability Oversight Council Ann. Rep. 89 (2018) (FSOC Annual Report).

66 FSOC Annual Report, footnote 65.

67 id.

68 'Monetary Policy and the State of the Economy: Hearing Before the H. Comm. on Fin. Servs.', 115th Cong. (Testimony of Jerome Powell); Randal Quarles, Vice Chair, Board of Governors of the Fed. Res. Sys., 'Thoughts on Prudent Innovation in the Payment System, Remarks Before the 2017 Financial Stability and FinTech Conference' (Nov. 30, 2017), https://www.federalreserve.gov/newsevents/speech/quarles20171130a.htm; Lael Brainard, Governor, Board of Governors of the Fed. Res. Sys.,

at June 2019, the Fed has not publicly taken a position on the permissibility of bank holding companies and financial holding companies to engage in various activities (either as principal or agent) related to virtual currencies.

OCC

Like the Fed, the OCC has published little guidance regarding the role of national banks in virtual currency ecosystems.[69] However, in 2018, the OCC announced it will make available a special-purpose national bank charter, generally known as a fintech charter, that may be owned by certain types of non-bank financial services companies.[70] A fintech charter permits a company to operate on a national basis under the OCC's supervision and thereby bypass multi-state licensing and supervision, and certain types of state regulation.[71] These features have led to industry speculation whether the charter will be available to enable a more streamlined alternative for certain virtual currency activities than the multistate licensing approach described below.[72] The OCC has stated that applicants and licensees will be held to the same standards as national banks, suggesting that even if the fintech charter is an avenue for certain virtual currency activities, only certain industry participants may be in a position to meet the applicable regulatory requirements.[73]

The fintech charter proposal proved controversial shortly after it was initially proposed, and state regulators continue to oppose the charter, including through a pending legal challenge to the charter.[74] The initial industry reaction to the fintech charter has been tepid with no formal applications being submitted as at 15 May 2019.[75]

'Cryptocurrencies, Digital Currencies, and Distributed Ledger Technologies: What Are We Learning, Remarks Before the Decoding Digital Currency Conference' (May 15, 2018), https://www.federalreserve.gov/newsevents/speech/brainard20180515a.htm.

69 See, e.g., Michelle Price, 'U.S. Regulator Plays Down Bitcoin Fear, Backs FinTech Charter', Reuters (Dec. 20, 2017), https://www.reuters.com/article/us-usa-occ-bitcoin/u-s-regulator-plays-down-bitcoin-fears-backs-fintech-charter-idUSKBN1EE25C.

70 Office of the Comptroller of the Currency, 'Policy Statement on Financial Technology Companies' Eligibility to Apply For National Bank Charters' (2018); Office of the Comptroller of the Currency, 'Comptroller's Licensing Manual Supplement: Considering Charter Applications From Financial Technology Companies' (2018).

71 id.

72 The OCC has not explicitly commented on what types of virtual currency activities, if any, may be conducted under the authority of a fintech charter. The OCC has stated that the charter is available to entities that facilitate payments electronically, and suggested that certain new or innovative activities may qualify as banking activities permitted by the charter; however, the OCC has expressly stated that entities will not qualify if they intend to accept deposits or engage primarily in fiduciary services.

73 Office of the Comptroller of the Currency, footnote 70. The standards applicable to national banks that apply to fintech charter licensees include those concerning capital and liquidity, profitability, corporate governance and management, risk management, community financial inclusion, financial-stress contingency planning, competition, treating customers fairly and regulatory compliance.

74 As at June 2019, there was a pending lawsuit in the United States District Court for the Southern District of New York brought by the New York Department of Financial Services against the OCC challenging its authority to issue a fintech charter. Unlike prior actions brought by the New York Department of Financial Services and the Conference of State Bank Supervisors, this action survived a motion to dismiss for a lack of ripeness, with some indication that the court was sympathetic to the position of the New York Department of Financial Services. *Vullo v. OCC et al.*, 2019 U.S. Dist. Lexis 77151 (S.D.N.Y. May 2, 2019).

75 Rachel Witkowski, 'Fintech Charter Delayed Following Court Ruling: Otting', American Banker (May 15, 2019), https://www.americanbanker.com/news/fintech-charter-delayed-following-court-ruling-occs-otting.

FDIC

Like the other prudential banking regulators, the FDIC is presently merely monitoring the development of virtual currencies and is likely to continue this approach. The FDIC has publicly stated that it is actively studying the potential effects of virtual currencies on the banking system and banks under its jurisdiction through FSOC's Digital Assets Working Group.[76]

CFPB

In light of its consumer protection mandate, the CFPB's focus with respect to virtual currencies has been on ensuring that consumers are adequately informed of the risks of virtual currencies. In this regard, in 2014, the CFPB issued a public warning regarding the risks of transacting and investing in virtual currencies and began accepting consumer complaints regarding virtual currency matters, a potential first step towards regulation or enforcement.[77] However, in 2016, after taking public comments, the CFPB declined to bring virtual currencies within its regulation on prepaid products or to take a position concerning whether virtual currencies are otherwise subject to Regulation E.[78] Moreover, to date there have been no public CFPB enforcement actions regarding virtual currency activities.

ii State money transmission regulators

The states have adopted a broad spectrum of approaches concerning the application of money transmission laws and regulations to virtual currencies. These approaches include: promulgating an entirely separate regulatory regime for the oversight of entities engaged in virtual currency activities (e.g., New York's BitLicense); incorporating or exempting virtual currency activities from state MTL regimes by statutory amendment or regulatory fiat; and declining to adopt a position (e.g., the approach of the California Department of Business Oversight (CDBO)).[79] As these approaches continue to evolve, there is also a potential alternative approach on the horizon, the Uniform Law Commission's proposed Uniform Regulation of Virtual Currency Business Act (the Uniform Act),[80] which, like the New York BitLicense, is a licensing regime specifically designed for entities involved in virtual currency activities. Although the Uniform Act has only been introduced in the legislatures of a handful of states and has yet to be adopted in any state as at June 2019, it may serve as the basis for future legislative activity concerning virtual currency regulation. Similarly, the Conference

76 Fed. Deposit Ins. Corp. Ann. Rep. 27 (2018).

77 Press release, 'Consumer Fin. Protection Bureau, CFPB Warns Consumers About Bitcoin' (Aug. 11, 2014), https://www.consumerfinance.gov/about-us/newsroom/cfpb-warns-consumers-about-bitcoin/.

78 'Prepaid Accounts under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z)', 79 Fed. Reg. 77101 (Dec. 23, 2014), 81 Fed. Reg. 83978 (Nov. 22, 2016).

79 The states also have generally expressed concern regarding consumer protection in virtual currency transactions, publishing bulletins warning consumers of the risks inherent in such transactions. See, e.g., Lorraine Mirabella, 'State Regulators Warn Consumers About Virtual Currency', *The Baltimore Sun* (Apr. 29, 2014), http://www.baltimoresun.com/bal-consuming-state-regulators-warn-consumers-virtual-currency-20140429-story.html; N.C. Office of the Comm'r of Banks, 'Consumer Alert: Virtual Currencies', https://www.nccob.gov/Public/docs/Financial%20Institutions/Money%20Transmitters/OCOB_Virtual_Currency_Alert.pdf.

80 Unif. Reg. of Virtual-Currency Bus. Act (Unif. Law Comm'n 2017) (Uniform Law), https://www.uniformlaws.org/committees/community-home?CommunityKey=e104aaa8-c10f-45a7-a34a-0423c2106778.

of State Bank Supervisors (CSBS) has published a model regulatory framework for states to consider.[81] The following summarises a handful of representative approaches to regulation of virtual currency activities at the state level. However, there are numerous variations on the themes below, as well as significant pending legislative and regulatory activity that promise to make this a dynamic area for the foreseeable future.

New York BitLicense

New York, through rule-making by the New York Department of Financial Services (NYDFS), has been the most aggressive of the states in regulating virtual currencies. Under New York law, a licence referred to as a BitLicense is broadly required to engage in any virtual currency business activity.[82] Given that New York is the epicentre of US financial markets and services, this requirement has led the NYDFS to be a leader in regulating, or seeking to regulate, a wide spectrum of virtual currency businesses operating in the United States. New York regulations define virtual currencies as 'any type of digital unit that is used as a medium of exchange or a form of digitally stored value' and includes both centralised and decentralised currencies.[83] Excluded from the definition of virtual currencies are: prepaid cards that are issued or redeemable in legal tender; digital units that are part of a customer affinity or rewards programme that cannot be converted into legal tender or a virtual currency; and digital units used within gaming platforms that have no real-world value or market outside the gaming platform, and cannot be converted into real-world value or a virtual currency.[84] Virtual currency business activity, the activity that gives rise to the licensing requirement, broadly entails any of the following:

a receiving a virtual currency for transmission or transmitting a virtual currency;
b storing, holding or maintaining custody or control of a virtual currency on behalf of others;
c buying and selling a virtual currency as a customer business;
d performing exchange services; and
e controlling, administering or issuing a virtual currency.[85]

Virtual currency business activities do not include use of a virtual currency by merchants or consumers to purchase goods or services, investment by merchants and consumers or the development and issuance of software.[86]

81 See Conference of State Bank Supervisors, 'State Regulatory Requirements For Virtual Currency Activities CSBS Model Regulatory Framework' (Sept. 15, 2015), https://www.csbs.org/sites/default/files/2017-11/CSBS-Model-Regulatory-Framework%28September%2015%202015%29.pdf. Several states also have published consumer advisories regarding the risks of transacting or investing in virtual currencies, generally using a model form promulgated jointly by the CSBS and the North American Securities Administrators Association. See, e.g., Md. Office of the Comm'r of Fin. Reg., Advisory Notice 14-01, 'Virtual Currencies: Risks for Buying, Selling, Transacting, and Investing' (Apr. 24, 2014), http://www.dllr.state.md.us/finance/advisories/advisoryvirtual.shtml.

82 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.3 (2019).

83 id., § 200.2(p).

84 id., §§ 200.2(p), (j).

85 id., § 200.2(q).

86 id., §§ 200.2(q), 200.3(c).

In addition to the requirement to obtain a licence, licensees under the BitLicense regime are also required to meet certain substantive compliance requirements. Generally, licensees are required to:

a maintain a sufficient amount of capital as determined by the NYDFS;[87]
b maintain sufficient anti-money laundering (AML), customer identification, cybersecurity, consumer complaint and anti-fraud programmes;[88]
c provide certain disclosures and receipts in connection with transactions;[89]
d file certain money laundering reports with the NYDFS if not otherwise filed with FinCEN;[90]
e have a compliance officer and a chief information security officer;[91]
f maintain certain written policies and procedures;[92]
g maintain a sufficient surety bond;[93] and
h meet certain record retention requirements.[94]

Licensees that hold virtual currencies on behalf of others are also required to: hold such funds in trust with a qualified custodian that is approved by the NYDFS; hold virtual currencies of the same type and amount as what is owed to the beneficiaries; and not sell, lend or assign virtual currencies held on behalf of others except at the direction of the beneficiary.[95] Licensees are also subject to supervision of the NYDFS, which includes periodic examinations and the submission of financial and transactional information to the NYDFS.[96]

Notwithstanding this extensive regulation, it should be noted that, depending on the nature of a licensee's activities, the NYDFS may require an entity that has received a BitLicense to also obtain a New York MTL. Moreover, as an alternative to the BitLicense, the NYDFS also has licensed a handful of trust companies to engage in certain virtual currency trading and custody activities. Although applicants for a trust company licence must meet a particularly high standard, there is an advantage to the trust company licence in that many (but not all) states do not require licences for trust companies that are chartered and supervised in another state.

Inclusive legislation

As an alternative to a new and separate regulatory regime, a number of other states have amended their MTL statutes broadly to include the receipt of virtual currencies for transmission or the issuance or the sale of virtual currencies as stored value.[97] Such amendments typically revise the statutory definitions of money or money transmission to

87 id., § 200.8.
88 id., §§ 200.15, 200.16, 200.20.
89 id., § 200.19.
90 id., § 200.15.
91 id., §§ 200.7(b), 200.16(c).
92 id., §§ 200.7, 200.15–200.17.
93 id., § 200.9(a).
94 id., § 200.12.
95 id., §§ 200.7, 200.2(n).
96 id., §§ 200.13, 200.14.
97 These states include, without limitation, Alabama, Connecticut, North Carolina, Oregon, Vermont and Washington. A 50-state survey was not conducted in the development of this section, and other states may also fall under this category or other categories presented in this section.

include the concept of virtual currencies, and add virtual currency as an additional defined term to the statute.[98] It is important to note that several, but not all, state MTL statutes exempt licensed broker-dealers to some degree,[99] and some states also recognise exceptions for agents of the payee[100] or payment processors.[101] Some virtual currency businesses therefore may be able to take advantage of these and other exceptions on state-by-state or activity-by-activity bases, or both.

In regard to the various types of potential virtual currency activities and whether they are subject to regulation in these states, states generally do not cover end users of a virtual currency (e.g., merchants that accept a virtual currency in payment for goods or services, individuals who use a virtual currency to make such payments and investors who purchase a virtual currency for their own portfolios), but transmitting or maintaining control of virtual currencies for others typically is a covered activity under such regimes,[102] which may be interpreted as covering both purchases and sales of virtual currencies on behalf of others.[103]

Licensees under these state MTL regimes are also subject to certain compliance requirements. Based on the plain text of money transmitter statutes and regulations, these requirements are generally not quite as extensive as those required for a New York BitLicense, but state regulators typically have discretion to require additional controls as a condition of licensing. Common examples of the relevant statutory or regulatory requirements include the following:

a holding permissible investments in an amount equivalent to funds received from senders;

b maintaining a sufficient net worth, which is often at a statutorily specified amount rather than an amount that is specific to the licensee;

c maintaining a sufficient surety bond; and

d meeting certain record retention requirements.

In certain states, money transmitters are also required to maintain certain policies and procedures, provide a receipt with each transaction and provide certain disclosures. State money transmitter licensees are also subject to periodic examinations, and must submit financial and transactional information to the supervising agencies.

For licensees that engage in virtual currency activities, compliance with these requirements can pose challenges in states that have not made accommodations for the unique attributes of virtual currencies that decades-old MTL statutes were not designed to address. For example, if a licensee holds a virtual currency for a customer and the state regulator views that holding as an outstanding obligation of the licensee to the customer, state regulations

98 See, e.g., N.C. Gen. Stat. §§ 53-208.42(12)–(13), (20) (2018); Wash. Rev. Code §§ 19.230.010(18), (30) (2018).

99 See, e.g., Wash. Rev. Code § 19.230.020(10) (2018) (exempting securities broker-dealers 'to the extent of its operation as such').

100 See, e.g., Jorge L Perez, Banking Comm'r, Conn. Dep't. of Banking, 'No Action Position on Money Transmission licensure Requirement for Persons Acting as an Agent of a Payee' (Oct. 24, 2017), https://portal.ct.gov/-/media/DOB/consumer_credit_nonhtml/102417MemoAgentofPayeepdf.pdf?la=en.

101 See, e.g., Wash. Rev. Code § 19.230.020(9) (2018).

102 See, e.g., N.C. Gen. Stat. § 53-208.42(13) (2018).

103 See, e.g., Deborah Bortner, Dir., Div. of Consumer Servs., Wash. Dep't of Fin. Insts., 'Uniform Money Services Act Interim Regulatory Guidance' (Dec. 8, 2014), https://dfi.wa.gov/documents/money-transmitters/virtual-currency-interim-guidance.pdf.

will typically require, as indicated above, that the licensee hold certain eligible investments in an amount equal to the outstanding obligation. For traditional licensees, that typically means holding customer funds in insured bank accounts, US Treasury securities or the like. While most states have concluded that it is permissible to hold a 'like-kind' investment of a virtual currency when the licensee has an obligation to deliver a virtual currency to a customer,[104] that is not uniformly the case, leading to significant duplicate collateralisation requirements in Hawaii, for example.[105]

Inclusive regulatory guidance

At least one state has issued regulatory guidance broadly classifying virtual currencies as money and subject to the state's money transmission laws.[106] Other states have taken a more nuanced position, covering some activities related to virtual currencies, but not others. For example, a line of guidance initially promulgated by Texas and adopted by several other states[107] distinguishes between decentralised and centralised virtual currencies. The guidance concludes that decentralised virtual currencies do not qualify as money under the respective state MTL statutes because they are not a currency as defined by the state law: that is, the coin or paper money of the United States or any other country.[108] As decentralised virtual currencies are not money, their transmission therefore is not money transmission.[109]

However, the guidance further notes that transactions involving decentralised virtual currencies that also involve the exchange of legal tender could constitute money transmission if the transactions involved more than two parties.[110] Under this line of guidance, the direct purchase and sale of virtual currencies as principal, the acceptance of virtual currencies for goods or services, the mere custody of virtual currencies and the exchange of one virtual currency for another virtual currency are not money transmission activities.[111] However, the sale of virtual currencies through an exchange for legal tender would be considered money transmission.[112]

104 See, e.g., Wash. Rev. Code § 19.230.200(1)(b) (2018).

105 See, e.g., Neeraj Agrawal, 'Hawaii's Issue With Bitcoin Businesses Has an Obvious and Easy Solution', Coincenter (Mar. 1, 2017), https://coincenter.org/link/hawaii-s-issue-with-bitcoin-businesses-has-an-obvious-and-easy-solution.

106 Such guidance was issued by the Hawaii Department of Commerce and Consumer Affairs. The guidance is relatively short, does not explain the reasoning of the Department and is very broad – it implies that even mining activities require a licence. Press release, Haw. Dep't. of Commerce and Consumer Affairs, 'State Warns Consumers on Potential Bitcoin Issues' (Feb. 26, 2014) (Hawaii Release). Legislation has been introduced in Hawaii to adopt a form of the Uniform Act.

107 See Charles G Cooper, Banking Comm'r, Tex. Dep't of Banking, Supervisory Memorandum – 1037, 'Regulatory Treatment of Virtual Currencies Under the Texas Money Services Act', 3 (Apr. 3, 2014); Kan. Office of the State Bank Comm'r, Guidance Document MT 2014-01, 'Regulatory Treatment of Virtual Currencies Under the Kansas Money Transmitter Act' (June 6, 2014, revised Apr. 1, 2019); Colo. Dep't of Regulatory Agencies, Div. of Banking, 'Interim Regulatory Guidance Cryptocurrency and the Colorado Money Transmitters Act' (Sept. 20, 2018); Ill. Dep't of Fin. and Prof'l Reg., 'Digital Currency Regulation Guidance' (June 13, 2017); Greg Gonzales, Comm'r, Tenn. Dep't of Fin. Insts., 'Regulatory Treatment of Virtual Currencies under the Tennessee Money Transmitter Act' (Dec.16, 2015).

108 See Cooper, footnote 107.

109 id., at 4.

110 id.

111 id., at 3–4.

112 id.

As for centralised virtual currencies issued by a private party, the guidance generally declines to adopt a broad position given the numerous potential variations in structure.[113] Instead, it generally defers making a judgement until the regulator is presented with the specific facts and circumstances at issue.[114] Texas' recently updated guidance has clarified that one particular type of centralised virtual currency, stablecoin, does qualify as money and is regulated if its value is tied to fiat currency and it is redeemable for such currency.[115] Other state regulators have informally indicated they would likely adopt a similar position.

Exemptive legislation

On the opposite end of the spectrum from New York is Wyoming, which has been aggressive in adopting legislation to make the state hospitable to virtual currency activities. Wyoming has broadly exempted from its money transmission laws the buying, selling, issuing or taking custody of virtual currency[116] and has adopted other legislation to facilitate the use of virtual currencies.[117] Another state, New Hampshire, also excludes virtual currency from its money transmission laws, but the relevant state regulator has interpreted the exemption narrowly.[118]

Exemptive regulatory guidance

A handful of other states have taken a broadly exemptive approach as a regulatory matter. For example, Pennsylvania has held through regulatory guidance that virtual currency exchanges do not need a money transmitter licence for facilitating transactions between buyers and sellers of virtual currencies based on the position that maintaining a clearing account for fiat currency at a depository institution does not require licencing because the exchange never directly handles fiat currency.[119]

No position

At present, not every state has taken a position, either through legislation or the actions of a regulator, regarding the application of MTL statutes to virtual currencies. Most notably, the CDBO has indicated that it is reserving judgement regarding the potential application of the California MTL statute to many virtual currency activities and the necessity of obtaining a licence. In response, some virtual currency companies are moving forward with virtual currency activities in California pending a determination by the CDBO that the California MTL statute applies to such activities and that a licence is required.

113 id., at 3.

114 id.

115 id., at 2, 5.

116 Wyo. Stat. Ann. §§ 40-22-103(xxii), 40-22-104(vi) (2019).

117 Wyoming law for purposes of the Uniform Commercial Code recognises digital assets generally as intangible personal property and virtual currency specifically. id., § 34-29-102.

118 N.H. Rev. Stat. Ann. § 399-G:3(VI-a) (2019); The New Hampshire Department of Banking has interpreted the exemption to not be available to parties that engage in the transfer of both fiat currency and virtual currency. N.H. Dep't. of Banking, "Cryptocurrency' Transmitters No Longer Supervised' (Aug. 1, 2017).

119 Penn. Dep't of Banking, 'Money Transmitter Act Guidance for Virtual Currency Businesses' (Jan. 23, 2019).

Uniform Regulation of Virtual-Currency Business Act

As reflected above, states have adopted a broad range of regulatory approaches. As virtual currencies mature and gain wider acceptance, more states may move to adopt a separate regulatory regime for virtual currencies or otherwise update their already enacted regulatory regimes. Indeed, legislation to that effect has been introduced in a number of states. During such a process, states may look to the Uniform Act referenced above for guidance.[120]

The substance of the Uniform Act is heavily influenced by New York's BitLicense licensing regime, state money transmitter licensing regimes and the CSBS Model Regulatory Framework. Under the Uniform Act, a licence is required to 'engage in virtual-currency business activity'.[121] The Uniform Act incorporates the concept of licensing reciprocity between states, so a separate licence may not be required for every state if the proposal is adopted as drafted.[122] The Uniform Act generally defines a virtual currency as a digital unit used as a medium of exchange or stored value, and includes both centralised and decentralised currencies.[123] Similar to the BitLicense regulation, the definition also excludes a customer affinity or rewards programme that cannot be converted into legal tender or a virtual currency, and digital units used within gaming platforms that have no real-world value and cannot be converted into real-world value or a virtual currency.[124] Unlike the BitLicense regulation, but similar to other states that have amended their money transmission statutes, the Uniform Act does not explicitly exclude prepaid cards that are issued or redeemable in legal tender.

The definition of virtual currency business activity – the activity that gives rise to the licensing requirement – includes 'exchanging, transferring, or storing virtual currency or engaging in virtual currency administration'.[125] The definition also explicitly includes issuing, or holding on behalf of others, electronic certificates representing an interest in precious metals .[126] As with the BitLicense regulation and several amended MTL statutes, the Uniform Act also excludes from the definition of virtual currency business activity direct purchases of goods and services using a virtual currency, the direct purchase of a virtual currency as an investment and persons whose activities are limited to the development or issuance of software.[127] The Uniform Act also provides a number of additional exceptions. Among the exceptions, several worth highlighting are those for:

a registered broker-dealers or other securities and commodities intermediaries under the Uniform Commercial Code that do not engage in the ordinary course of business in virtual currency business activity in addition to maintaining securities accounts or commodities accounts;

b a licensed money transmitter;

120 The Uniform Law Commission has also promulgated the Uniform Supplemental Commercial Law for the Uniform Regulation of Virtual-Currency Business Act to provide commercial law rules under the Uniform Commercial Code for owing, transacting and holding virtual currencies. Unif. Supplemental Com. Law for the Unif. Reg. of Virtual-Currency Bus. Act (Unif. Law Comm'n 2018), https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=de52d1fe-1f70-a568-9552-d354ade157ca&forceDialog=0.

121 Uniform Law, footnote 80.

122 id., §§ 201, 203.

123 id., § 102(23).

124 id.

125 id., § 102(24).

126 id.

127 id., § 103.

c a payment processor that facilitates clearing and settlement between exempt entities;
d entities whose activity in the jurisdiction is associated with annual transactions that have a value of US$5,000 or less;
e a virtual currency control-services vendor; and
f an entity that does not receive compensation for providing virtual currency products or services.[128]

As with state licences generally, the Uniform Act also imposes certain substantive compliance requirements, including:

a maintaining a sufficient net worth and reserves as is determined necessary by the relevant regulator;[129]
b maintaining sufficient AML, customer identification, cybersecurity, complaint programmes and anti-fraud programmes;[130]
c providing certain disclosures and receipts in connection with transactions;[131]
d maintaining certain written policies and procedures;[132]
e maintaining a sufficient surety bond;[133] and
f meeting certain record retention requirements.[134]

Licensees that hold virtual currencies on behalf of others are also required to hold virtual currencies of the same type and amount as what is owed to the beneficiary.[135]

IV ANTI-MONEY LAUNDERING

The Bank Secrecy Act (BSA)[136] is the primary federal statute that imposes AML obligations on institutions in the financial sector. FinCEN, a bureau of the US Department of the Treasury, issues and enforces AML regulations promulgated under BSA authority, generally in conjunction with other federal agencies with direct supervisory authority over impacted institutions, such as banks and broker-dealers. The BSA and its implementing regulations (BSA Regulations)[137] require that certain enumerated financial institutions that are not otherwise federally regulated must register with FinCEN, maintain a risk-based AML programme and collect, retain and share information with FinCEN.

i FinCEN guidance: a functional approach

The BSA Regulations impose AML obligations on various financial institutions, including traditional financial entities such as banks, mutual funds, brokers and dealers in securities, futures commission merchants, introducing brokers in commodities as well as certain

128 id.
129 id., § 204.
130 id., §§ 601, 602.
131 id., § 501.
132 id., § 601.
133 id., § 204.
134 id., § 302.
135 id., § 502.
136 31 U.S.C. §§ 5311–5332 (2018). Money laundering itself is also defined in the US Criminal Code. See, e.g., 18 U.S.C. §§ 1956, 1957 (2018).
137 31 C.F.R. Ch. X (2018).

non-traditional financial entities, including money services businesses (MSBs).[138] Under the BSA Regulations, persons or entities 'wherever located doing business, whether or not on a regular basis or as an organised or licensed business concern, wholly or in substantial part within the [United States]' conducting certain activities are considered MSBs.[139] MSBs include, among other things, dealers in foreign exchange, providers and sellers of prepaid access and money transmitters.[140] A money transmitter is any person or entity that provides money transmission services or is engaged in the transfer of funds.[141] The terms money transmitter and money transmission services have formed the basis for FinCEN's regulation of entities engaged in certain virtual currency activities.

In 2011, FinCEN finalised a rule[142] that expanded the definition of money transmission services to encompass 'the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means'.[143] By covering other value that substitutes for currency, FinCEN thus laid the foundation for assessing whether a particular virtual currency business constitutes acting as a money transmitter.

FinCEN then issued guidance that established key definitions and analytical principles that FinCEN uses to assess virtual currency activities under the BSA (2013 Guidance).[144] The 2013 Guidance defines virtual currency as 'a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency', distinguishing real currency from virtual currency on the basis that the latter does not have legal tender status in any jurisdiction.[145] The 2013 Guidance is limited to activities involving convertible virtual currencies (CVCs), defined as a virtual currency that 'has either an equivalent value in real currency, or acts as a substitute for real currency'.[146] The 2013 Guidance does not include any reference to whether CVCs must be convertible to real currency or some other form of value; nor does it address whether convertibility must be authorised by the virtual currency system itself, or whether a mere market for trade or exchange is sufficient.

The 2013 Guidance defines three participants in generic virtual currency arrangements: a user is a person that obtains virtual currency to purchase goods or services; an exchanger is a person engaged as a business in the exchange of virtual currency for real currency, funds or other virtual currency; and an administrator is a person engaged as a business in issuing (putting into circulation) virtual currency, and who has the authority to redeem (to withdraw

138 id., § 1010.100(t).

139 id., § 1010.100(ff).

140 id., §§ 1010.100(ff)(1), (4)–(5).

141 id., § 1010.100(ff)(5).

142 'Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses', 76 Fed. Reg. 43585 (July 21, 2011).

143 31 C.F.R. § 1010.100(ff)(5)(i)(A) (2018).

144 Fin. Crimes Enf't Network, US Dep't of the Treasury, FIN-2013-G001, 'Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' (Mar. 18, 2013).

145 id., The BSA Regulations define real currency as coin and paper money of any country that is also designated as legal tender, circulates and is customarily used and accepted as a medium of exchange in the country of issuance. 31 C.F.R. § 1010.100(m) (2018).

146 FinCEN defines prepaid access as 'access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number, or personal identification number'. 31 C.F.R. § 1010.100(ww) (2018). The 2013 Guidance distinguishes CVCs from prepaid access on the basis that prepaid access is limited to value denominated in real currency.

from circulation) such virtual currency.[147] An exchanger or administrator that accepts and transmits a CVC, or buys or sells a CVC for any reason, is a money transmitter subject to any applicable limitations or exceptions.[148] However, merely acting as a user does not fit within the definition of money transmission, and therefore users are not MSBs subject to AML obligations. The 2013 Guidance addresses both centralised CVCs and decentralised[149] CVCs such as Bitcoin.

FinCEN subsequently issued several interpretations addressing the application of the 2013 Guidance under specific fact patterns, but issued a comprehensive release in May 2019, similarly limited to CVCs,[150] that consolidated and expanded upon those interpretations (the 2019 Guidance).[151] Although FinCEN asserts that the 2019 Guidance does not create any new regulatory requirements or expectations, its discussion of business models previously unaddressed by FinCEN may, in effect, establish new ground rules for certain CVC participants.

Defining the scope of user, exchanger and administrator

CVC creators: mining and investment

The 2019 Guidance provides that, if a person mines CVC and uses it solely for purchasing goods and services on its own behalf, then that person is not an MSB under the BSA Regulations unless and until the person mines CVC for use in money transmission, reaffirming prior guidance.[152] Moreover, even where persons combine computer processing resources into 'mining pools' and the leader of such a group receives the earned CVC and transfers it to other group members, this alone is not money transmission under the BSA Regulations because such transfers are integral to the provision of services. FinCEN has

147 A person or entity may act in more than one capacity in a particular arrangement or transaction.

148 The BSA Regulations identify six circumstances under which a person is not a money transmitter despite accepting and transmitting currency, funds or value that substitutes for currency. 31 C.F.R. §§ 1010.100(ff)(5)(ii)(A)–(F) (2018). These carve-outs include: a person who merely provides the delivery, communication or network instruments used for transmission; a payment processor who facilitates payment for goods or services by agreement with the creditor or seller; and accepting or transmitting funds integral to the sale of goods or services by the person accepting or transmitting the funds. See id., §§ 1010.100(ff)(5)(ii)(A)–(B), (F).

149 These are CVCs that have no central repository and no single administrator, and may be obtained by a person's own computing or manufacturing effort.

150 The 2019 Guidance also does not address the contours of what is convertible for these purposes, but does state the definition covers value originally created for another purpose – including assets other regulatory frameworks classify as commodities, securities or futures contracts – that is repurposed as a currency substitute.

151 Fin. Crimes Enf't Network, US Dep't of the Treasury, FIN-2019-G001, 'Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies' (May 9, 2019). On the same day FinCEN also released an advisory to aid financial institutions in identifying and reporting suspicious activity by bad actors exploiting CVCs for illicit purposes, which provided examples of unregistered CVC entities used to further such activities, red flags of illicit conduct using CVCs and recommendations on information to include when filing required reports involving CVCs. See Fin. Crimes Enf't Network, US Dep't of the Treasury, FIN-2019-A003, 'Advisory on Illicit Activity Involving Convertible Virtual Currency' (May 9, 2019).

152 See Jamal El-Hindi, Assoc. Dir., Policy Div., Fin. Crimes Enf't Network, US Dep't of the Treasury, FIN-2014-R001, 'Application of FinCEN's Regulations to Virtual Currency Mining Operations' (Jan. 30, 2014).

similarly found that investors in virtual currencies for their own benefit, and not for the benefit or at the behest of others, are users of a virtual currency and therefore are not money transmitters.[153] Thus, FinCEN does not look to the label applied to a particular process of creating or obtaining a virtual currency, but rather to the function for which the person uses the CVC, and for whose benefit.

CVC trading platforms, decentralised exchanges and centralised repositories

CVC trading platforms enable CVC buyers and sellers to find one another and sometimes also function as an intermediary to facilitate trades. According to the 2019 Guidance, CVC trading platforms that merely provide a forum to post bids and offers are not money transmitters under the BSA Regulations if the parties themselves settle any matched transactions via an outside venue or service.[154] However, if a trading platform purchases the CVC from the seller and sells it to the buyer, the trading platform becomes an exchanger and is thereby subject to the BSA Regulation requirements as a money transmitter. This is the case even if an entity only effects transmissions contingent upon the occurrence of predetermined conditions or the buying and selling customers are never identified to one another.[155] Furthermore, an exchanger will be subject to the same AML obligations under the BSA Regulations regardless of whether it acts as a broker attempting to match two (mostly) simultaneous and offsetting transactions involving the acceptance of one type of currency and the transmission of another, or as a dealer transacting from its own reserve in either CVC or real currency.[156]

More broadly, in connection with CVCs for which there is a centralised repository, the 2013 Guidance concludes that the administrator of a centralised repository of CVCs is a money transmitter to the extent it allows transfers of value between persons or from one location to another, regardless of whether the transferred value is a real currency or CVC; and an exchanger that uses its access to virtual currency services provided by the administrator to accept and transmit CVCs on behalf of others also is a money transmitter.

Additional business models

P2P exchangers, CVC kiosks and decentralised applications

Peer-to-peer (P2P) exchangers that are engaged in the business of buying and selling CVCs by facilitating transfers of CVC for currency, other CVCs or other types of value must comply with BSA Regulations as money transmitters, except for a natural person engaging in such activity who does so on an infrequent basis and not for profit or gain.[157] Similarly, the

153 See Jamal El-Hindi, Assoc. Dir., Policy Div., Fin. Crimes Enf't Network, US Dep't of the Treasury, FIN-2014-R002, 'Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity' (Jan. 30, 2014). The same ruling indicated that mere development and distribution of software is not money transmission for this purpose.

154 Such platforms fit the BSA Regulation exemption from money transmitter status for merely providing the delivery, communication or network instruments used for transmission. 31 C.F.R. § 1010.100(ff)(5)(ii)(A) (2018).

155 See Jamal El-Hindi, Assoc. Dir., Policy Div., Fin. Crimes Enf't Network, US Dep't of the Treasury, FIN-2014-R011, 'Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform' (Oct. 27, 2014).

156 See Jamal El-Hindi, Assoc. Dir., Policy Div., Fin. Crimes Enf't Network, US Dep't of the Treasury, FIN-2014-R012, 'Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System' (Oct. 27, 2014).

157 31 C.F.R. § 1010.100(ff)(8) (2018).

owner-operator of a CVC kiosk (i.e., electronic terminal) that enables the exchange of CVC for currency, other CVCs or other types of value would be treated as a money transmitter subject to the BSA Regulations.

The 2019 Guidance addresses for the first time publicly FinCEN's position regarding decentralised applications (DApps), which are software programmes operating on a P2P network of computers running blockchain platforms and designed so that they are not controlled by a central administrator. The 2019 Guidance states that when DApps perform money transmission, the definition of money transmitter may apply to the DApp itself or its owners-operators, or both. The 2019 Guidance does not address who may be considered an owner or operator of a DApp or the implications of a piece of software running on a decentralised network being a money transmitter for purposes of the BSA Regulations.

Payment processing services involving CVC transmission

Financial intermediaries that enable traditional merchants to accept CVC from customers in exchange for goods and services are also money transmitters under the 2019 Guidance. CVC payment processors generally are unable to meet the conditions for the payment processor exemption in the BSA Regulations because they do not operate through clearance and settlement systems that admit only BSA-regulated financial institutions.[158]

Internet casinos

The 2019 Guidance provides that any entity engaged in the business of gambling not otherwise covered by the BSA Regulation definition of casino, gambling casino or card club[159] – which includes any virtual platform created for betting on the possible outcome of events such as predictive markets, information markets, decision markets, idea futures or event derivatives – that accepts and transmits value denominated in CVC may still be regulated as a money transmitter under the BSA.

CVC wallets

Interfaces for intermediaries in the business of storing and transferring CVCs vary based on the technology involved, including mobile wallets, software wallets and hardware wallets. FinCEN considers wallets with user funds controlled by third parties to be 'hosted wallets' and wallets with user-controlled funds to be 'unhosted wallets'. However, FinCEN's regulatory treatment of these intermediaries under the 2019 Guidance is not technology-specific, but depends on four criteria: (1) who owns the value; (2) where the value is stored; (3) whether the owner interacts directly with the payment system where the CVC runs; and (4) whether the person acting as intermediary has total independent control over the value. FinCEN does not explain how these factors would be balanced in all situations, but does describe certain providers of hosted wallets that would be treated as MSBs and specifies that a person purchasing goods or services on their own behalf via an unhosted wallet is not a money transmitter.

158 See id., § 1010.100(ff)(5)(ii)(B); El-Hindi, footnote 156.

159 31 C.F.R. §§ 1010.100(t)(5)-(6) (2018). Casinos have their own AML obligations under the BSA Regulations. When a person falls under FinCEN's definitions for both casino and MSB, the regulatory obligations of a casino generally satisfy the obligations of an MSB, with the exception of registration.

Fundraising for development of other projects – ICOs[160]

The 2019 Guidance specifically addresses two business models involving ICOs. The first involves ICOs whereby a preferential sale of CVC is made to a distinct set of preferred buyers (i.e., investors). The seller of the CVC is a money transmitter under the BSA Regulations because at the time of the initial offering the seller is the only person authorised to issue and redeem the new units of CVC and therefore would be considered an administrator of the CVC.[161] The second business model involves ICOs whereby funds are raised through the issuance of a digital token as proof of an equity or debt investment, where investors may subsequently: (1) receive new CVC in exchange for the token; (2) exchange the token for a DApp coin, which is a digital token that unlocks the use of DApps that provide various services; (3) use the original token itself as a new CVC or DApp coin; or (4) receive some other type of return on the original equity or debt investment. In this model, depending on the circumstances, participants may be exempt from MSB status under an exemption available for other types of regulated entities (but not from BSA Regulations otherwise applicable to the regulated entity) or for the acceptance and transmission of value that is integral to the sale of goods or services different from money transmission.[162] In any event, the resale of the initial token generally would not create any BSA Regulations obligations for the initial investor.

Anonymity-enhanced CVC transactions

Finally, the 2019 Guidance addresses transactions that are denominated in either (1) regular types of CVC but are structured to conceal information otherwise generally available through the CVC's native distributed public ledger or (2) types of CVC specifically engineered to prevent their tracing through distributed public ledgers (also called private coins). Operating in anonymity-enhanced CVCs is subject to the same regulatory treatment as operating in other CVCs, and may complicate compliance obligations related to communication of information in connection with certain fund transfers. Moreover, an anonymising services provider that accepts CVCs and retransmits them in a manner designed to prevent others from tracing the transmission back to its source would itself be considered a regulated money transmitter under the BSA Regulations. However, a person that merely provides anonymising software without more is not a money transmitter under the BSA Regulations.

160 The Department of the Treasury previously confirmed in a letter to Senator Ron Wyden, then the ranking member on the Senate Finance Committee, that the 2013 Guidance was intended to sweep broadly to have CVCs include ICO coins and tokens. Therefore, 'a developer that sells . . . ICO coins or tokens, in exchange for another type of value that substitutes for currency is a money transmitter and must comply with' applicable AML obligations while 'an exchange that sells ICO coins or tokens, or exchanges them for other virtual currency, fiat currency, or other value that substitutes for currency, would typically also be a money transmitter'. Letter from Drew Maloney, Assistant Sec'y for Legislative Affairs, Dep't of the Treasury to Senator Ron Wyden (Feb. 13, 2018), https://coincenter.org/files/2018-03/fincen-ico-letter-marc h-2018-coin-center.pdf.

161 Similarly, the 2019 Guidance specifies that any 'transaction where a person accepts currency, funds, or value that substitutes for currency in exchange for a new CVC at a preferential rate for a group of initial purchasers, before making the CVC available to the rest of the public, is simply engaging in money transmission, regardless of any specific label (such as 'early investors') applied to the initial purchasers'.

162 See 31 C.F.R. §§ 1010.100(ff)(8), (5)(ii)(F) (2018).

ii FinCEN enforcement activity

FinCEN has also actively pursued criminal and civil enforcement matters against virtual currency businesses and individuals. Virtual currency exchanger Ripple Labs Inc and its wholly owned subsidiary XRP II, LLC (Ripple) concurrently entered into a consent agreement with FinCEN and a settlement with the US Attorney's Office in the Northern District of California for the failure to register as an MSB and violating numerous AML-related BSA Regulation requirements.[163] Ripple agreed to pay US$700,000 and to take remedial actions, including to only conduct such exchanger activities through a registered MSB and to implement an effective, compliant AML programme. FinCEN also assessed a US$110,003,314 civil penalty against Canton Business Corporation (BTC-e) along with a 21-count criminal indictment under 18 USC Sections 1956, 1957 and 1960 for wilful violations of the BSA AML requirements, including failure to register as an MSB and maintain an effective AML compliance programme as well as criminal money laundering charges. This was the first such action against a foreign-located, internet-based virtual currency business.[164] The Ripple and BTC-e examples are representative of numerous additional civil and criminal enforcement actions stemming from failures to comply with the BSA Regulations AML requirements.

Additionally, in April 2019 FinCEN brought its first enforcement action against an individual P2P CVC exchanger, assessing a civil monetary penalty of $35,350 for Eric Powers' wilful failure to comply with any of the BSA Regulations applicable to money transmitters including developing, implementing and maintaining an AML programme, registering as an MSB and filing required transaction reports.[165] Powers was also immediately and permanently prohibited from ever providing money transmission services, engaging in any activity that would make him an MSB under the BSA Regulations and participating in any BSA-defined 'financial institution' that does any business in the United States.

iii AML compliance programme requirements

When a virtual currency business acts as an MSB, it must register with FinCEN and implement and maintain an effective written, risk-based AML programme that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities.[166] At a minimum such a programme must:

a establish policies, procedures and internal controls to verify customer identification, file reports, create and retain records and respond to law enforcement requests;

b integrate AML compliance procedures with automated data processing systems to the extent applicable;

c maintain a list of agents;

163 News release, Fin. Crimes Enf't Network, 'FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger' (May 5, 2015), https://www.fincen.gov/sites/default/files/2016-08/20150505.pdf.

164 See news release, Fin. Crimes Enf't Network, 'FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales' (July 26, 2017), https://www.fincen.gov/sites/default/files/2017-07/BTC-e%20July%2026%20Press%20Release%20FINAL1.pdf; *United States v. BTC-e a/k/a Canton Business Corporation and Alexander Vinnik*, CR 16-00227 SI (N.D. Cal. Jan. 17, 2017). One of BTC-e's founders was also arrested, indicted and assessed a US$12 million personal penalty.

165 News release, Fin. Crimes Enf't Network, 'FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws' (Apr. 18, 2019), https://www.fincen.gov/news/news-releases/fincen-penalizes-peer-peer-virtual-currency-exchanger-violations-anti-money.

166 See 31 U.S.C. §§ 5318(a)(2), (h) (2018); 31 C.F.R. § 1022.210 (2018).

d designate an AML programme compliance officer;
e provide appropriate AML education and training for relevant personnel; and
f provide for independent periodic review and monitoring to ensure programme adequacy.

Finally, MSBs also have a variety of record-keeping and reporting obligations in connection with their AML activities, including the obligation to file certain reports of suspicious activity.[167]

iv Incorporation of the BSA AML requirements into state law

In addition to federal requirements under the BSA, all US jurisdictions (with the exception of Montana) also regulate money transmitters in some capacity through licensure and other requirements. As explained in Section III, each jurisdiction's money transmitter laws differ in terms of which activities require a licence and what is required to obtain a licence. Accordingly, whether FinCEN requires a virtual currency business to be registered federally as an MSB does not necessarily mean a state will agree with the classification under its laws, which generally have consumer protection goals as well as AML goals.

Many jurisdictions expressly incorporate compliance with the AML requirements of the BSA and BSA Regulations into their own money transmission statutes and regulations, including, for example, New York and Delaware.[168] Moreover, some jurisdictions impose AML obligations in addition to the federal requirements.[169] Consequently, virtual currency businesses may be subject to enforcement of federal AML compliance from state regulators, and may also have to comply with additional AML requirements depending on whether their activities necessitate a licence.

v Office of Foreign Assets Control

OFAC implements certain statutes, regulations and executive orders related to trade and economic sanctions that have been imposed on targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction and other threats to the national security, foreign policy or economy of the United States. Those sanctions may prohibit certain types of transactions, or may require the blocking and freezing of assets associated with the targets of the sanctions regime, and are enforced with significant federal criminal sanctions. Any entity engaged in virtual currency activities in the United States must comply with the applicable OFAC regimes, and therefore must take care to assess whether its customers or counterparties are subject to relevant sanctions.

OFAC has pursued virtual currency-specific sanctions actions, including against two Iran-based individuals that helped exchange Bitcoin ransom payments into Iranian Rial as P2P exchangers on behalf of Iranian malicious cyber actors.[170] This marked the first instance

167 Other regulated financial institutions also have similar, but somewhat more extensive, AML obligations, including, for example, a more specific obligation to develop a customer identification programme. See, e.g., 31 C.F.R. § 1020.220 (2018).

168 See, e.g., N.Y. Fin. Serv. Law § 417.2 (Consol. 2018); 5 Del. Admin. Code § 2301-1.1 (2018).

169 See, e.g., Arizona Rev. Stat. Ann. § 6-1241 (2018).

170 News release, US Dep't of the Treasury, 'Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses' (Nov. 28, 2018),

of OFAC specifically identifying CVC addresses associated with sanctioned individuals. Additionally, OFAC has issued FAQs stating that all US persons are prohibited from engaging in transactions related to, providing financing for and otherwise dealing in any 'digital currency, digital coin, or digital token' that was issued by, for or on behalf of the government of Venezuela on or after 9 January 2018.[171]

V REGULATION OF MINERS

Mining of virtual currencies is generally lawful under US federal and state law. However, concerns about energy consumption and environmental impact have caused at least one local government to issue temporary bans on virtual currency mining.[172] There is no US regulatory regime that is specific to virtual currency mining; that is, virtual currency miners are not at this time regulated in the US as virtual currency miners. FinCEN has indicated that to the extent a user mines Bitcoin and uses the Bitcoin for its own purposes (i.e., not for the benefit of a third party), that user is not an MSB because the mining activity involves neither acceptance nor transmission of Bitcoin.[173] To the extent that the virtual currency being mined is a security or a commodity, the mining of the virtual currency may implicate other aspects of US federal law, including broker-dealer, investment adviser, commodity pool operator (CPO) or commodity trading adviser (CTA) registration.

US federal taxation of virtual currency mining may also prove complex and unclear. For example, miners may be required to include the fair market value of a mined currency in their gross income, and to the extent that an individual miner engages in virtual currency mining as part of a trade or business, the individual taxpayer may be required to pay self-employment tax on his or her net earnings from mining.

The treatment of virtual currency mining at the state and local levels varies. For example, Hawaii has issued guidance classifying virtual currencies as money, which subjects virtual currencies to the state's laws on money transmission.[174] The guidance is relatively short, however, and does not explain the reasoning for this treatment. It is also quite broad, and appears to imply that mining activity requires a licence.[175] Montana is the only state to not have enacted any form of money transmission statute. While Montana has no laws or regulations specific to blockchain or virtual currencies, it is the first state to take a financial stake in a Bitcoin mining operation.[176]

---

https://home.treasury.gov/news/press-releases/sm556.

171 See US Dep't of the Treasury, 'OFAC FAQs', No. 566 (Mar. 19, 2018), https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#venezuela; The White House, Exec. Order No. 13827, 'Taking Additional Steps to Address the Situation in Venezuela', 83 Fed. Reg. 12469–70 (Mar. 19, 2018).

172 Plattsburgh, NY, City Code Ch. 270, Art. V, § 270-28-J (2018).

173 El-Hindi, footnote 152.

174 Hawaii Release, footnote 106.

175 id.

176 Press release, Office of Governor Steven Bullock, 'Governor Bullock Announces $1.1 Million to Help Main Street Businesses Create Jobs, Train Employees and Plan for Growth', http://governor.mt.gov/Newsroom/governor-bullock-announces-11-million-to-help-main-street-businesses-create-jobs-train-employees-and-plan-for-growth (last visited July 5, 2019).

VI REGULATION OF ISSUERS AND SPONSORS

Issuers and sponsors of virtual currency-related investment funds (both public and private) and regulators continue to be challenged with applying an existing body of law and regulation to new technology and a new and evolving class of assets. Public interest in virtual currencies and digital tokens has prompted the formation of hundreds of virtual currency-related private investment funds,[177] and several public fund sponsors have filed registration statements with the SEC with a view to the public offering of shares of virtual currency-related investment funds.[178]

i Legal and regulatory environment overview

All offers and sales of securities in the United States, including by investment funds, must either be registered with the SEC under the Securities Act or be exempt from such registration.[179] The Securities Act imposes rigorous disclosure requirements in connection with the offer and sale of registered securities. Additionally, investment funds that invest substantially in securities[180] and wish to issue their shares to the public in the United States generally are subject to registration and regulation as investment companies under the Investment Company Act of 1940 (the Company Act). The Company Act substantively regulates virtually every aspect of the business and operations of a registered investment company. Investment advisers to investment funds that invest substantially in securities generally are subject to registration and regulation as investment advisers under the Investment Advisers Act of 1940 (the Advisers Act) unless an exemption is available. The Advisers Act substantively regulates the business of investment advisers and their relationships with their clients, including investment funds. The Director of the Division of Investment Management of the SEC, which administers the Company Act and the Advisers Act, as well as the Securities Act as applied to investment companies registered under the Company Act, has expressed particular concerns regarding investment funds that invest in virtual currencies and related assets.[181] The operators of investment funds that invest or may invest to any extent in derivatives, including virtual currency-based or digital assets-based derivatives, are also subject to regulation by the CFTC under the CEA, including disclosure, reporting and record-keeping requirements under the Part 4 Rules of the CFTC.[182] Registered CPOs and CTAs also are required to be members of the NFA, which imposes additional substantive regulation on their business activities.[183] The

177 See 'Cryptocurrency Investment Fund Industry Graphs and Charts', Crypto Fund Research, https://cryptofundresearch.com/cryptocurrency-funds-overview-infographic/ (last visited July 5, 2019).

178 See, e.g., ProShares Trust II, Registration Statement (Form S-1) (Sept. 27, 2017); Etherindex Ether Tr., Registration Statement (Form S-1) (Sep. 5, 2017); VanEck SolidX Bitcoin Tr., Registration Statement (Form S-1) (June 5, 2018); Rex Bitcoin Strategy Fund, Registration Statement (Form N-1A) (Nov. 3, 2017).

179 See Securities Act §§ 4, 5 (codified at 15 U.S.C. §§ 77d, 77e (2018)).

180 The status of virtual currencies and digital tokens as securities is addressed in Section II.

181 Letter from Dalia Blass, Dir., Div. of Inv. Mgmt., US Sec. and Exch. Comm'n, to Paul Schott Stevens, President & Chief Exec. Officer, Inv. Co. Inst., and Timothy W Cameron, Head of Asset Mgmt. Group, Sec. Indus. and Fin. Mkts. Assoc., 'Engaging on Fund Innovation and Cryptocurrency-related Holdings' (Jan. 18, 2018), https://www.sec.gov/divisions/investment/noaction/2018/cryptocurrency-011818.htm.

182 The CFTC and the CEA do not regulate investment funds directly. Rather, they regulate CPOs and CTAs in respect of their operation of, and provision of commodity derivative trading advice to, investment funds that use commodity derivatives, which the CEA and the CFTC refer to as commodity pools.

183 The NFA has implemented rules specifically addressing transactions in and offerings of virtual currencies and related assets. In December 2017, the NFA issued reporting requirements that required CPOs to notify

Exchange Act may subject an investment fund to public reporting requirements that include, among other things, quarterly and annual reports filed with the SEC that must comply with SEC rules regarding their content.[184] Generally, these reporting obligations arise when an investment fund's shares are listed on a national securities exchange, or when its equity securities are held by either 2,000 persons or 500 persons who are not accredited investors, and the issuer has total assets exceeding US$10 million.[185]

Private fund managers typically avoid the registration and disclosure obligations of the Securities Act by offering securities in the United States pursuant to Section 4(a)(2) of the Securities Act, which exempts from registration transactions 'by an issuer not involving any public offering'.[186] Regulation D under the Securities Act (Regulation D) establishes a safe harbour that assures exemption under Section 4(a)(2). Historically, a material requirement of Regulation D was a prohibition on general solicitation or general advertising.[187] However, pursuant to the Jumpstart our Business Startups Act, enacted in 2012, the SEC amended Rule 506 of Regulation D to provide that the prohibition against general solicitation will not apply where, along with the other requirements of Regulation D being met, all purchasers of the securities in the offering are accredited investors and reasonable efforts, as described in the amended rule, are undertaken to verify their status as such.[188]

Private investment funds generally avoid registration and regulation under the Company Act by relying on one of two available exclusions from the definition of the term investment company.[189] Section 3(c)(1) of the Company Act provides an exclusion for investment funds that have fewer than 100 beneficial owners, and Section 3(c)(7) provides an exclusion for investment funds that are sold exclusively to qualified purchasers (without imposing any limit on the number of beneficial owners). Both Section 3(c)(1) and Section 3(c)(7) require that the investment fund not make or propose to make a public offering of its securities (which is satisfied by complying with Regulation D). A number of investment funds that propose to invest solely in virtual currencies or their derivatives, and have sought to sell their securities to the public and list them for trading on a national securities exchange, have relied on Section 3(b)(1) of the Company Act for exclusion from registration and regulation thereunder. Section 3(b)(1) excludes any issuer primarily engaged in a business or businesses other than that of investing, reinvesting, owning, holding or trading in securities. Reliance on this exclusion requires that the digital currencies or tokens in which an investment fund will

the NFA immediately once they have executed a transaction involving any virtual currency transaction or virtual currency derivative (including futures, options or swaps) on behalf of a commodity pool. On 9 August 2018, the NFA adopted disclosure requirements for NFA members offering commodity pools that trade virtual currencies or virtual currency derivatives. The NFA's disclosure guidelines highlighted concerns with virtual currencies such as price volatility, valuation and liquidity, and virtual currency exchanges, intermediaries and custodians, cybersecurity and the opaque spot market. See NFA Notice, footnote 59.

184 Exchange Act § 13 (codified at 15 U.S.C. § 78m (2018)).

185 Exchange Act § 12(g) (codified at 15 U.S.C. § 78l (2018)).

186 15 U.S.C. § 77d (2018).

187 See Rule 502(c) of Regulation D (codified at 17 C.F.R. § 230.502(c) (2018)).

188 See Rule 506(c) of Regulation D (codified at 17 C.F.R. § 230.506(c) (2018)).

189 See Company Act § 3(a)(1)(A), (C) (codified at 15 U.S.C. §§ 80a-3(a)(1)(A), (C) (2018)).

invest are not securities (in the case of an investment fund that will hold virtual currencies, such as Bitcoin or Ether) or that the investment fund is a commodity pool (in the case of an investment fund that may invest in Bitcoin derivatives).[190]

Investment advisers to private funds have sought to avoid registration and regulation under the Advisers Act by not advising registered investment companies, and either keeping their assets under management below the threshold that would require registration under Section 203A of the Advisers Act (which may subject them to regulation at the state level) or operating as exempt reporting advisers under the private fund adviser exemption.[191] However, once a private fund adviser's assets under management exceed US$150 million, or if the adviser acts as investment adviser to a registered investment company or a separately managed account, registration and regulation under the Advisers Act are unavoidable. Compliance with the Advisers Act has proved challenging in the digital asset context. Compliance with Advisers Act Rule 206(4)-2, the custody rule, has been particularly challenging for investment advisers due to the general lack of qualified custodians to hold digital assets for the benefit of an investment fund and the lack of guidance from the SEC on how to comply with the custody rule with respect to digital assets.[192] The staff of the SEC's Division of Investment Management recently published a letter seeking public input on the applicability of the custody rule to digital assets.[193] Noting that amendments to the custody rule are on the SEC's long-term unified agenda, the staff stated that it expects to utilise what it learns from this information-gathering initiative to inform any future recommendations to the SEC with respect to any regulatory action that may be necessary or appropriate.[194]

Exemptions from registration and regulation as a CPO or CTA may be available. A CPO may be exempt from registration under the de minimis rule if commodity derivatives are not a material component of the investment fund's portfolio, and if the fund's securities are sold in transactions exempt from registration under the Securities Act and are offered and sold without marketing to the public in the United States (which is satisfied by complying with Regulation D).[195] If the de minimis exemption is not available, registration with the CFTC as a CPO and membership in NFA is required. However, once a CPO is registered, an exemption from most of the otherwise applicable CFTC disclosure, reporting and record-keeping rules is available if the investment fund is sold exclusively to qualified eligible persons in an offering exempt from registration under the Securities Act (which is satisfied by complying with Regulation D).[196] Because qualified purchasers are, by definition, qualified eligible persons, an investment fund that relies on Section 3(c)(7) for exclusion from the

190 In a line of no-action letters, the SEC has provided guidance as to how to distinguish a commodity pool from an investment company required to be registered and regulated under the Company Act. See *Peavey Commodity Funds I, II and III*, 1983 SEC No-Act. LEXIS 2576 (June 2, 1983); *EF Hutton and Company Inc* (June 22, 1983); *Ft Tryon Futures Fund Limited Partnership*, 1990 SEC No-Act. LEXIS 1192 (Aug. 16, 1990); *Managed Futures Association*, 1996 SEC No-Act. LEXIS 623 (July 15, 1996).

191 See Advisers Act Rule 203(m)-1 (codified at 17 C.F.R. § 275.203(m)-1 (2018)).

192 See Advisers Act Rule 206(4)-2 (codified at 17 C.F.R. § 275.206(4)-2 (2018)).

193 Letter from Paul G Cellupica, Deputy Dir. and Chief Counsel, Div. of Inv. Mgmt., US Sec. and Exch. Comm'n, to Karen Barr, President & Chief Exec. Officer, Inv. Adviser Assoc., 'Engaging on Non-DVP Custodial Practices and Digital Assets' (Mar. 12, 2019), https://www.sec.gov/investment/non-dvp-and-custody-digital-assets-031219-206.

194 id.

195 See CFTC Rule 4.13(a)(3) (codified at 17 C.F.R. § 4.13(a)(3) (2018)).

196 See CFTC Rule 4.7 (codified at 17 C.F.R. § 4.7 (2018)).

Company Act generally will be eligible for this relief. Exemption from registration as a CTA (and membership in NFA) is available for CTAs that have 15 or fewer advisory clients in the past 12 months and who do not hold themselves out generally to the public as CTAs.[197] Other exemptions from CTA registration may be available as well.

ii Attempts at public offerings

Several fund sponsors have filed registration statements with the SEC for virtual currency-related investment funds with a view to offering them to the public and, in some instances, listing their shares on a national securities exchange.[198] These investment funds include investment companies registered under the Company Act, commodity pools exempt from the Company Act pursuant to Section 3(b)(1) but fully compliant with the Part 4 Rules of the CFTC and investment funds that are exempt from the Company Act pursuant to Section 3(b)(1) (because they do not invest in securities) and not regulated under the CEA or the Part 4 rules of the CFTC (because they do not invest in commodity derivatives).[199] To date, the SEC has not declared effective any registration statement for any such issuer, and SEC staff have compelled the withdrawal of a number of registration statements for registered investment companies that would invest in virtual currencies, digital tokens or derivatives referencing such assets under threat of enforcement action.[200] In June 2018, the SEC disapproved the listing and trading of the Winklevoss Bitcoin Trust, finding that because Bitcoin markets are not 'uniquely resistant to manipulation', the listing of a Bitcoin fund by a securities exchange was not consistent with the requirements of the exchange to prevent fraudulent and manipulative acts and practices and to protect investors and the public interest. In August 2018, the SEC rejected nine separate applications to list Bitcoin exchange-traded funds.

Additionally, the SEC has disapproved applications by securities exchanges to list the securities of funds that would invest in digital assets. The SEC must authorise the listing of every security traded on a national securities exchange in the United States. Although generic listing rules are available for most types of securities commonly listed on national securities exchanges, if the security or issuer exhibits new or novel features, the exchange must submit an application to the SEC's Division of Trading and Markets to promulgate a new listing rule designed specifically for that issuer and security.[201] The SEC has disapproved applications to list securities of an exchange-traded investment product that would invest solely in Bitcoin, finding that the investment funds in question were inconsistent with Section 6(b)(5) of the Exchange Act, which requires that rules of national securities exchanges be designed to prevent fraudulent and manipulative acts and practices, and protect investors and the public

197 See CEA § 4m(1) (codified at 7 U.S.C. § 6m(1) (2018)); CFTC Rule 4.14(a)(10) (codified at 17 C.F.R. § 4.14(a)(10) (2018)).

198 E.g., Winklevoss Bitcoin Tr., Registration Statement (Form S-1) (Dec. 7, 2016); Etherindex Registration Statement, footnote 178; VanEck Registration Statement, footnote 178; Rex Registration Statement, footnote 178.

199 E.g., VanEck Registration Statement, footnote 178.

200 See Letter from J Garrett Stevens, President, Exch. Listed Funds Tr., to US Sec. and Exch. Comm'n, 'Exchange Listed Funds Trust (File Nos. 333-180871 and 811-22700) Request for Withdrawal of Post-Effective Amendment No. 47' (Oct. 5, 2017), https://www.sec.gov/Archives/edgar/data/1547950/000139834417012782/fp0028414_aw.htm.

201 See 17 C.F.R. § 240.19b-4 (2018).

interest.[202] Other applications for exchange-traded investment products that would invest in digital assets have also been submitted, and a number of such applications have been rejected by the SEC.

iii The Dalia Blass Letter

On 18 January 2018, the Division of Investment Management of the SEC issued a letter to the Investment Company Institute and the Securities Industry and Financial Markets Association (Blass Letter). This letter outlined the SEC's concerns regarding virtual currency-related funds in relation to valuation, liquidity, custody, arbitrage (in respect of exchange traded funds) and potential manipulation and other risks associated with virtual currency-related funds.[203] While the Blass Letter was issued in response to an attempt to register investment products under the Company Act, the SEC noted that these concerns apply also to private virtual currency-related funds.[204] The SEC also noted that 'until the questions raised [in the Blass Letter] can be addressed satisfactorily, [they] do not believe that it is appropriate for fund sponsors to initiate registration of funds that intend to invest substantially in virtual currency and related products'.[205] The Blass Letter noted that 'cryptocurrency markets are developing swiftly. Additional questions may arise from these developments'.[206] At the same time, the SEC has clearly signalled its willingness to work with the industry by indicating that, 'over the years, dialogue between fund sponsors and the [SEC] has facilitated the development of many new types of investment products'.[207]

VII CRIMINAL AND CIVIL FRAUD AND ENFORCEMENT

i Civil enforcement

Both the CFTC and SEC have declared expressly their intention to police conduct in the cryptocurrency markets. On 19 January 2018, the Directors of Enforcement for the CFTC and the SEC released a highly unusual joint statement, stating:

> *When market participants engage in fraud under the guise of offering digital instruments – whether characterised as virtual currencies, coins, tokens, or the like – the SEC and the CFTC will look beyond form, examine the substance of the activity and prosecute violations of the federal securities and commodities laws. The Divisions of Enforcement for the SEC and CFTC will continue to address violations and bring actions to stop and prevent fraud in the offer and sale of digital instruments.*[208]

202 See US Sec. and Exch. Comm'n, 'Self-Regulatory Organizations; Order Disapproving a Proposed Rule Change, as Modified by Amendments No. 1 and 2, to BZX Rule 14.11(e)(4), Commodity-Based Trust Shares, to List and Trade Shares Issued by the Winklevoss Bitcoin Trust', Exchange Act Release 34-80206 (Mar. 10, 2017), https://www.sec.gov/rules/sro/batsbzx/2017/34-80206.pdf.

203 Blass, footnote 181.

204 id.

205 id.

206 id.

207 id.

208 James McDonald et al., 'Joint statement from CFTC and SEC Enforcement Directors Regarding Virtual Currency Enforcement Actions' (Jan. 19, 2018), http://www.cftc.gov/PressRoom/SpeechesTestimony/mcdonaldstatement011918.

That same day, the CFTC Chair, J Christopher Giancarlo, delivered a speech on virtual currencies in which he stated that '[t]he CFTC believes that the responsible regulatory response to virtual currencies involves asserting CFTC legal authority over virtual currency derivatives in support of anti-fraud and manipulation enforcement, including in underlying spot markets'.[209] In another truly extraordinary event, the Chairs of the SEC and CFTC, Jay Clayton and Giancarlo, penned a joint op-ed for the *Wall Street Journal* addressing the oversight of virtual currencies. They stated their agencies 'along with other federal and state regulators and criminal authorities, will continue to work together [. . .] to deter and prosecute fraud and abuse'.[210]

SEC

The SEC's enforcement jurisdiction is somewhat more limited than the CFTC's because the SEC can only bring actions involving instruments falling within the definition of security. However, once properly regarded as a transaction in a security, the SEC's enforcement powers sweep very broadly, with possible statutory and rule violations involving registration, business conduct, trading and many other types of statutory and regulatory requirements, as well as fraud and manipulation.[211] In 2017, the SEC's Division of Enforcement formed a Cyber Unit, which it stated would focus on the following:

a market manipulation schemes involving false information spread through electronic and social media;
b hacking to obtain material non-public information and trading on that information;
c violations involving distributed ledger technology and ICOs;
d misconduct perpetrated using the dark web;
e intrusions into retail brokerage accounts; and
f cyber-related threats to trading platforms and other critical market infrastructure.[212]

As described in more detail in Section II, the SEC issued the DAO Report in July 2017, finding that the tokens offered and sold by the DAO were securities, and thus subject to the requirements of the federal securities laws.

In the wake of the DAO Report, the SEC has brought various actions for illegal ICOs, sometimes, but not always, including charges of fraud. For example, in September 2017, it brought charges against an individual and his two companies for fraud in two ICOs purported to be backed by investments in real estate and diamonds. In the former, the alleged misstatements included that the company had a 'team of lawyers, professionals, brokers, and accountants' that would invest the ICO proceeds into real estate when in fact none had been hired or even consulted. The individual and his company allegedly misrepresented they had raised between US$2 million and US$4 million from investors when the actual amount was approximately US$300,000. In the case of the second company, the allegations were that

209 J Christopher Giancarlo, 'Remarks of Chair J Christopher Giancarlo to the ABA Derivatives and Futures Section Conference, Naples, Florida' (Jan. 19, 2018), http://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo34.

210 Jay Clayton & J Christopher Giancarlo, 'Regulators Are Looking at Cryptocurrency', *Wall Street Journal* (Jan. 24, 2018), https://www.wsj.com/articles/regulators-are-looking-at-cryptocurrency-1516836363.

211 See, e.g., US Sec. and Exch. Comm'n Div. of Enf't Ann. Rep. (2017), https://www.sec.gov/files/enforcement-annual-report-2017.pdf.

212 id., at 4.

they claimed to have purchased diamonds and engaged in other business operations when they had actually done nothing in that regard.[213] The SEC obtained an emergency asset freeze against the defendants.

As another example, in December 2017, the SEC charged a Canadian and his company with fraudulently marketing tokens to US investors (and thus also violating the registration provisions of the US securities law), and obtained an emergency asset freeze.[214] In a further example, in May 2018, the SEC filed a complaint and obtained an emergency asset freeze, and then a consented-to preliminary injunction and appointment of a receiver, in connection with an alleged ongoing fraudulent ICO that had raised US$21 million by a self-described 'blockchain evangelist' who had misrepresented his business relationship with the Fed and many well-known companies.[215]

As previously noted, the SEC has demonstrated its willingness to move against unregistered ICOs that it views as securities offerings even in the absence of fraud. As described in Section II, in December 2017, the SEC filed a settled administrative proceeding against Munchee for making an illegal, unregistered securities offering. After being contacted by the SEC, Munchee agreed voluntarily to halt the offering, to return to investors the proceeds raised to that point and to the entry of the order finding a violation of the securities registration provisions of the Securities Act.[216]

In February 2018, the SEC brought an action against a former platform and its operator for operating an unregistered securities exchange and also for defrauding users of the exchange. The exchange offered what the SEC alleged were securities in 'virtual currency-related enterprises in exchange for [B]itcoins'. The operator of the exchange was also charged with fraud in connection with an illegally unregistered token offering.[217]

In September 2018, the SEC took action against an ICO website for operating as an unregistered broker-dealer in violation of the federal securities laws.[218] As previously signalled in the DAO Report and public statements by SEC staff, this action reiterated that those who directly or indirectly offer trading or other services related to digital assets that are securities must comply with the federal securities laws.

An October 2018 complaint filed by the SEC alleging securities fraud illustrates the fact specific nature of applying the *Howey* test to determine whether a security is at issue.[219] The district court judge initially denied the SEC's request to freeze the defendant's assets, finding the SEC had failed to reasonably demonstrate the tokens were securities, in part based on serious differences in the facts alleged by the SEC and the defendant. However, the SEC filed a motion for reconsideration and the court ultimately granted the injunction.

213 *SEC v. REcoin Group Foundation, LLC, et al.*, No. 17-cv-05725 (E.D.N.Y Sept. 29, 2017).

214 *SEC v. PlexCorps, et al.*, No. 1:17-cv-07007-DLI-RML (E.D.N.Y. Dec. 1 2017).

215 *SEC v. Titanium Blockchain Infrastructure Services, Inc, et al.*, CV18-4315-DSF (JPRx) (C.D. Cal. May 22, 2018); see also SEC v. Arisebank, et al., No. 18-cv-00186 (N.D. Tex. Jan. 25, 2018) (allegedly fraudulent ICO in connection with a claim of creating the world's first decentralised bank); *SEC v. Sharma, et al.*, No. 18-cv-02909-DLC (S.D.N.Y. Apr. 2, 2018) (allegedly fraudulent US$32 million ICO).

216 *Munchee*, footnote 6.

217 *SEC v. Montroll, et al.*, 1:18-cv-01582 (S.D.N.Y. Feb. 21, 2018).

218 TokenLot, LLC, et al., Securities Act Release No. 10543, Exchange Act Release No. 84075, Company Act Release No. 33221, Admin. File No. 3-18739 (Sept. 11, 2018).

219 *SEC v. Blockvest*, No. 3:18-cv-02287 (S.D. Cal. Oct. 3, 2018).

In November 2018, the SEC announced settlements against two separate ICO issuers for conducting unregistered public offerings.[220] For the first time in an SEC action settlement, each issuer in these cases agreed, under the terms of its respective settlement, to register its tokens as securities by filing a Form 10 with the SEC and to thereafter make all required filings under the Exchange Act. Such registration and periodic reporting is intended to provide the token purchasers the benefit of receiving disclosures as required by the Exchange Act. In February 2019, the SEC settled against another ICO issuer with generally similar facts.[221] In this instance, however, the SEC did not impose a penalty against the issuer because the issuer self-reported its unregistered ICO to the SEC, cooperated with the SEC's investigation and voluntarily agreed to take remedial steps.

Additionally, in November 2018, the SEC announced its enforcement settlement against the founder of a decentralised digital asset trading platform, EtherDelta, arising out of EtherDelta's alleged operation of an unregistered national securities exchange.[222] As discussed in Section II, the Exchange Act mandates that an exchange be registered with the SEC as a national securities exchange or be exempt from registration. The EtherDelta website provided users access to an order book for tokens, displayed firm bids and offers for tokens, allowed users to buy or sell tokens and employed a smart contract to execute orders. More specifically, as a decentralised exchange, EtherDelta utilised a smart contract to self-execute trades by validating orders, confirming order terms and conditions, executing pair orders and updating the Ethereum blockchain to reflect the trade.

The SEC has also acted when illegal sales of securities occur linked to sudden price increases in what were previously shell companies in the wake of announcements that they had entered into cryptocurrency-related businesses.[223] Finally, while not constituting enforcement actions, the SEC has halted trading in the shares of a number of companies involved or purportedly involved in cryptocurrency-related businesses because of unusual and unexplained market activity, concerns about the accuracy and adequacy of publicly released information about the company, or both.[224]

CFTC

The principal mechanisms that the CFTC uses to bring enforcement actions involving cryptocurrencies are the broad statutory and regulatory provisions prohibiting fraud and manipulation in connection with 'a contract of sale of any commodity in interstate

220 *In re CarrierEQ, Inc. d/b/a Airfox*, Securities Act Release No. 10575, Admin. File No. 3-18898 (Nov. 16, 2018); *In re Matter of Paragon Coin, Inc.*, Securities Act Release No. 10574, Admin. File No. 3-18897 (Nov. 16, 2018).

221 Gladius Network LLC, Securities Act Release No. 10608, Admin. File No. 3-19004 (Feb. 20, 2019).

222 *In re Coburn*, Exchange Act Release No. 84553, Admin. File No. 3-18888 (Nov. 8, 2018).

223 See, e.g., *SEC v. Jesky, et al.*, No. 1:18-cv-05980-JFK (S.D.N.Y. July 2, 2018) (sale of shares in excess of price required by registration statement); *SEC v. Longfin Corp, et al.*, No. 1:18-cv-02977-DLC (S.D.N.Y. Apr. 4, 2018) (unregistered distribution of shares and sale of restricted shares by CEO and three other affiliated individuals).

224 See, e.g., US Sec. and Exch. Comm'n, Exchange Act Release No. 83518 (June 25, 2018) (temporary suspension of trading in the securities of Evolution Blockchain Group Inc.); US Sec. and Exch. Comm'n, Exchange Act Release No. 83084 (Apr. 20, 2018) (temporary suspension in the trading of IBITX Software Inc.); US Sec. and Exch. Comm'n, Exchange Act Release No. 82452 (Jan. 5, 2018) (temporary suspension in the trading of UBI Blockchain Internet, Ltd.).

commerce'.[225] The CEA, in turn, defines a commodity to include, with very limited exceptions, 'all [. . .] goods and articles [. . .] and all services, rights and interests [. . .] in which contracts for future delivery [i.e., futures] are presently or in the future dealt in'.[226] Enforcement actions can also be brought for violations of registration and other regulatory requirements if the transactions take the form of swaps, futures or even commodity cryptocurrency transactions with retail customers (as discussed further below).

In September 2015, the CFTC brought two actions in quick succession. It first entered into a settlement agreement with a trading platform named Coinflip, Inc, which was hosting trading in Bitcoin options. The CFTC declared Bitcoin and other virtual currencies to be commodities within the meaning of the CEA, and thus the platform, which was unregistered, to be illegally hosting trading in options on commodities.[227] A week later, the CFTC brought another case against a trading platform that was registered as a SEF for failing to prevent wash trading. The CFTC asserted that the platform had arranged a transaction to 'test the pipes' by doing a round-trip trade, but then publicised the transactions without noting they were pre-arranged to test the systems, 'creating the impression of actual trading interest in the Bitcoin swap'.[228]

In June 2016, the CFTC entered a settlement order with another trading platform, Bitfinex, involving spot transactions in the virtual currency itself.[229] Bitfinex allowed trading on a 30 per cent margin, and thus potentially fell under the retail commodity transaction provisions of the CEA.[230] The CFTC concluded that there was not actual delivery of the virtual currency, and thus Bitfinex was operating illegally by not complying with the requirement to register as a DCM. In concluding that actual delivery had not taken place, the CFTC was principally concerned that 'Bitfinex retained control over the private keys' to the wallets in which the customers' coins were held.[231]

In September 2017, the CFTC charged an individual and his company with fraud, misappropriation and issuing false account statements in connection with solicited investments in Bitcoin. The defendants were accused of operating a Ponzi scheme, whereby investors were encouraged to place their funds in a pool that would be managed by using 'a high-frequency, algorithmic trading strategy'.[232]

225 7 U.S.C. § 9(1) (2018); see also 17 C.F.R. § 180.1 (2018).

226 7 U.S.C. § 1a(9) (2018).

227 *Coinflip*, footnote 53.

228 *In re TeraExchange LLC*, CFTC No. 15-33 (Sept. 24, 2015).

229 *BFXNA*, footnote 54.

230 The CEA's various regulatory requirements apply to all transactions with retail customers in any commodity involving margin, leverage or financing provided by the seller or someone acting in concert with the seller without regard to whether the contract could be characterised as a derivative or a futures transaction, as long as it is not a true spot transaction, meaning there is actual delivery of the commodity to the customer within no more than 28 days, or covered by certain other limited exceptions. See 7 U.S.C. § 2(c)(2)(D) (2018).

231 *BFXNA*, footnote 54. As the CFTC put it: 'In the context of cryptocurrencies, a 'private key' is a secret number (usually a 256-bit number) associated with a deposit wallet that allows [B]itcoins in that wallet to be spent'. id., at *3 n.4. This focus on the private key as the basis for analysing delivery raised concerns and has led the CFTC to propose an interpretation to address the issue of actual delivery in the context of virtual currencies. See Geoffrey F Aronow, 'Projections Of The Imagination: When is a Token Actually Delivered?', 38 Futures & Derivatives L. Rep. 11 (Jan. 2011).

232 *CFTC v. Gelfman Blueprint, Inc et al.*, No. 1:17-cv-07181-PKC (S.D.N.Y. Sept. 21, 2017).

On 18 January 2018, the CFTC filed two lawsuits in federal court alleging fraud in connection with the trading of virtual currencies. One involved allegations that the perpetrators were promoting a pooled investment vehicle in which the investors would contribute Bitcoin, which would be converted into fiat currency and then used to trade various commodity interests.[233] The other case involved an allegation of trading advice relating to trading of virtual currencies themselves.[234] Both involved simple allegations that the defendants misappropriated the funds.

On 24 January 2018, the CFTC announced that it had filed an action under seal on 16 January 2018, alleging misappropriation of over US$6 million in funds from customers.[235] In this instance, the allegations focused on misrepresentations about how the form of virtual currency being promoted, My Big Coin (MBC), could be used with merchants and others to process transactions with MBC. On 6 March 2018, the CFTC won affirmation from a federal district court of its antifraud authority over virtual currencies.[236] In the context of ruling on the CFTC's motion for a preliminary injunction (which the court granted), the court held that CEA Section 6(c)(1), as amended by the Dodd-Frank Wall Street Reform and Consumer Protection Act and as implemented by CFTC Rule 180.1, does grant the CFTC jurisdiction to bring cases for fraud in cash markets in general and virtual currencies in particular.[237] The alleged fraud involved purported consulting services and trading advice relating to Bitcoin and another virtual currency, Litecoin.[238] On 23 August 2018, following a non-jury trial, the case was decided in favour of the CFTC, and the defendants were ordered to pay US$1.1 million in civil monetary penalties and restitution.[239]

ii Criminal enforcement

The DOJ and other law enforcement authorities are rapidly recognising that cryptocurrencies present a variety of opportunities for engaging in fraud, money laundering and other criminal activity. As a result, the last several years have seen a noticeable uptick from prior years in criminal investigations and charges involving cryptocurrencies across a broad spectrum of crimes. Indeed, at a digital asset industry conference in June 2018, the Federal Bureau of Investigation (FBI) revealed that it had 130 cases under investigation that had been 'threat tagged' as involving cryptocurrencies, covering crimes including 'human trafficking, illicit drug sales, kidnapping and ransomware attacks'.[240]

233 *CFTC v. Dean, et al.*, No. 2:18-cv-00345 (E.D.N.Y. Jan. 18, 2018).

234 *McDonnell*, footnote 56.

235 Commodity Futures Trading Comm'n, 'CFTC Charges Randall Crater, Mark Gillespie, and My Big Coin Pay, Inc. with Fraud and Misappropriation in Ongoing Virtual Currency Scam' (Jan. 24, 2018), https://www.cftc.gov/PressRoom/PressReleases/pr7678-18.

236 *McDonnell*, footnote 56; see also *My Big Coin Pay*, footnote 56.

237 *McDonnell*, footnote 56.

238 id., at 3.

239 See *McDonnell*, footnote 57.

240 Lily Katz & Annie Massa, 'FBI Has 130 Cryptocurrency-Related Investigations, Agent Says', Bloomberg (June 27, 2018), https://www.bloomberg.com/news/articles/2018-06-27/fbi-has-130-cryptocurrency-related-investigations-agent-says.

Investment fraud

A cryptocurrency is not just a medium of exchange, but also an investment. For that reason, in several widely reported instances, the DOJ has recognised the opportunities that now exist for the perpetration of fraud against cryptocurrency investors.

In May 2018, the US Attorney for the Southern District of New York (SDNY) brought what is believed to be the first criminal fraud charges against the issuers of an ICO. Specifically, the SDNY charged three co-founders of a startup company, Centra Tech, with 'conspiring to commit, and the commission of, securities and wire fraud in connection with a scheme to induce victims to invest millions of dollars' worth of digital funds for the purchase of unregistered securities, in the form of digital currency tokens issued by Centra Tech, through material misrepresentations and omissions'.[241] In particular, the indictment alleged that the defendants' offering materials for the ICO misrepresented details about their supposed executive team, their supposed partnerships with established financial institutions and their supposed state licensing. In connection with the charges, the FBI seized 91,000 Ether units that represented US$60 million in investor funds.

More recently, in early 2019, the DOJ brought two additional significant cases against alleged large-scale cryptocurrency fraudsters. First, in February 2019, it charged Randall Crater, the founder of Las Vegas-based My Big Coin Pay, with wire fraud and engaging in illegal monetary transactions in connection with creating and marketing the fraudulent virtual currency MBC while misappropriating more than $6 million in investor funds.[242] Shortly thereafter, in March 2019, it charged Konstantin Ignatov and Ruja Ignatova with a far larger, multibillion-dollar scheme in which the defendants allegedly bilked investors in the fraudulent cryptocurrency OneCoin, which authorities asserted had 'no real value.'[243]

Focusing on a different type of fraud – market manipulation – the DOJ was reported in May 2018 to have opened a parallel investigation with the CFTC into manipulation of the market for Bitcoin and other digital currencies.[244] The DOJ's market-manipulation probe was reported to focus on a variety of illegal practices that might influence prices, including spoofing. Although reported as a seemingly broad-based investigation when it was opened, this federal criminal investigation likely soon found at least one area of particular focus in June 2018 when researchers at the University of Texas released a paper in which they purported to have identified a specific instance of fraudulent manipulation of the market for Bitcoin in

241 US Attorney's Office, S.D.N.Y., US Dep't of Justice, press release No. 18-157, 'Founders Of Cryptocurrency Company Indicted In Manhattan Federal Court With Scheme To Defraud Investors' (May 14, 2018), https://www.justice.gov/usao-sdny/pr/founders-cryptocurrency-company-indicted-manhattan-federal-court-scheme-defraud.

242 Office of Pub. Affairs, US Dep't of Justice, press release No. 19-169, 'New York Man Charged with Cryptocurrency Scheme' (Feb. 27, 2019), https://www.justice.gov/opa/pr/new-york-man-charged-cryptocurrency-scheme.

243 US Attorney's Office, S.D.N.Y., US Dep't of Justice, press release No. 19-071, 'Manhattan U.S. Attorney Announces Charges Against Leaders Of 'OneCoin,' A Multibillion-Dollar Pyramid Scheme Involving The Sale Of A Fraudulent Cryptocurrency' (Mar. 8, 2019), https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-leaders-onecoin-multibillion-dollar.

244 Matt Robinson & Tom Schoenberg, 'U.S. Launches Criminal Probe into Bitcoin Price Manipulation', Bloomberg (May 24, 2018), https://www.bloomberg.com/news/articles/2018-05-24/bitcoin-manipulation-is-said-to-be-focus-of-u-s-criminal-probe.

2017 involving activity at a specific cryptocurrency exchange.[245] It was reported in November 2018 that the DOJ is focusing on the possibility that Tether – a different cryptocurrency with a value that is supposedly tied to the US dollar – was illegally used to prop up the value of Bitcoin.[246]

Overall, the opportunities to defraud investors in cryptocurrencies are many and varied. No doubt for this reason, the DOJ's July 2018 announcement that it had created a new task force on market integrity and consumer fraud noted prominently that one of the task force's main areas of focus would be digital currency fraud.[247]

Money laundering

The use of cryptocurrencies in money laundering – a crime that can involve either laundering the proceeds of criminal activity or transmitting funds for the purpose of carrying on criminal activity[248] – is one of the most significant focuses of attention by the DOJ. Former Deputy Attorney General Rod Rosenstein observed at a Financial Services Roundtable conference in February 2018 that '[a] lot of [. . .] schemes involve [B]itcoin and other cryptocurrencies which do not flow through the traditional financial system', and that the DOJ is 'working [. . .] with our cybercrime task force [. . .] on a comprehensive strategy to deal with that'.[249]

Not surprisingly, a number of high-profile federal indictments have involved money laundering charges or allegations relating to the defendants' use of cryptocurrencies to carry out or hide the proceeds of their offences. For example, in July 2017, the then-current US Attorney of the Northern District of California, Brian Stretch,[250] announced the indictment of Russian national Alexander Vinnik and BTC-e – alleged to be one of the world's largest and most widely used digital currency exchanges – for deliberately allowing BTC-e to be used as a platform 'to facilitate transactions for cybercriminals worldwide and [to] receive[] the criminal proceeds of numerous computer intrusions and hacking incidents, ransomware scams, identity theft schemes, corrupt public officials, and narcotics distribution rings'.[251] In another big criminal takedown in March 2018, the DOJ charged seven individuals with facilitating prostitution and money laundering through their operation of the notorious prostitution advertising website, backpage.com, accusing them, among other

245 John M Griffin & Amin Shams, 'Is Bitcoin Really Un-Tethered?' (June 13, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195066; Nathaniel Popper, 'Bitcoin's Price Was Artificially Inflated, Fueling Skyrocketing Value, Researchers Say', New York Times (June 13, 2018) https://www.nytimes.com/2018/06/13/technology/bitcoin-price-manipulation.html.

246 Matt Robinson & Tom Schoenberg, 'Bitcoin-Rigging Criminal Probe Focused on Tie to Tether', Bloomberg (Nov. 20, 2018), https://www.bloomberg.com/news/articles/2018-11-20/bitcoin-rigging-criminal-probe-is-said-to-focus-on-tie-to-tether.

247 Office of Pub. Affairs, US Dep't of Justice, press release No. 18-911, 'Department of Justice, Bureau of Consumer Financial Protection, U.S. Securities and Exchange Commission, Federal Trade Commission Announce Task Force on Market Integrity and Consumer Fraud' (July 11, 2018), https://www.justice.gov/opa/pr/department-justice-bureau-consumer-financial-protection-us-securities-and-exchange-commission.

248 18 U.S.C. § 1956 (2018).

249 Sead Fadilpašić, 'US Government Working on Crypto Strategy', Cryptonews (Feb. 28, 2018), https://cryptonews.com/news/us-government-working-on-crypto-strategy-1301.htm.

250 Now a partner at Sidley Austin LLP.

251 US Attorney's Office, N.D. Cal., US Dep't of Justice, 'Russian National And Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox' (July 26, 2017), https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged.

things, of furthering their 'money laundering efforts [by] [. . .] us[ing] [B]itcoin processing companies [. . .] such as CoinBase, GoCoin, Paxful, Kraken, and Crypto Capital to receive payments from customers and/or route money through the accounts of related companies'.[252] Perhaps the most high-profile money laundering charges involving cryptocurrencies were those brought in July 2018 against 12 Russian intelligence officers charged with hacking the 2016 presidential election, who were alleged to have 'transferr[ed] cryptocurrencies through a web of transactions in order to purchase computer servers, register domains, and make other payments in furtherance of their hacking activities, while trying to conceal their identities and their links to the Russian government'.[253]

Miscellaneous crimes

Finally, beyond money laundering and investment fraud, cryptocurrencies can be either a vehicle for, or an object of, criminal activity in all of the same ways that traditional currency and investments can be. Thus, for example, in March 2018, the Internal Revenue Service (IRS) issued a notice to taxpayers reminding them to 'report the income tax consequences of virtual currency transactions' and warning that, in 'extreme situations, taxpayers could be subject to criminal prosecution for failing to properly report the income tax consequences of virtual currency transactions'.[254] In a somewhat unexpected instance of cryptocurrency crime mirroring traditional currency crime, the Manhattan District Attorney's Office reported in December 2017 that it had indicted an individual named Louis Meza for perpetrating a gunpoint armed robbery of US$1.8 million worth of Ether tokens.[255]

VIII TAX

Guidance on the US federal income tax treatment of virtual currencies such as Bitcoin is limited to a single notice (Notice) issued by the IRS,[256] which treats such virtual currency as property. From an investor's perspective, merely calling a virtual currency property leaves many questions unanswered. How does a US taxpayer treat gains on buying and selling a virtual currency? Would a US tax-exempt entity such as a private foundation be able to make an unlevered investment in a virtual currency without incurring unrelated business taxable income (UBTI)? Would a non-US investor be able to invest in a virtual currency through a US-based investment manager (whose operations, personnel and equipment are located in the United States) without being treated as engaged in a US trade or business or having effectively connected income (ECI) in respect of such virtual currency investments?

252 *United States v. Michael Lacey et al.*, No. CR-18-00422-PHX-SPL (BSB) (D. Ariz. Mar. 28, 2018).

253 US Dep't of Justice, 'Deputy Attorney General Rod J Rosenstein Delivers Remarks Announcing the Indictment of Twelve Russian Intelligence Officers for Conspiring to Interfere in the 2016 Presidential Election Through Computer Hacking and Related Offenses' (July 13, 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-announcing-indictment-twelve.

254 The Internal Revenue Serv., IR-2018-71, 'IRS Reminds Taxpayers to Report Virtual Currency Transactions' (Mar. 23, 2018), https://www.irs.gov/newsroom/irs-reminds-taxpayers-to-report-virtual-currency-transactions.

255 Press release, New York Cty. Dist. Attorney, 'DA Vance: Man Indicted for Stealing $1.8 Million in Cryptocurrency' (Dec. 12, 2017), https://www.manhattanda.org/da-vance-man-indicted-stealing-18-million-cryptocurrency/.

256 I.R.S. Notice 2014-21, 2014-16 I.R.B. 938.

Would one need to distinguish, from a US federal income tax perspective, between direct investments in virtual currencies and derivatives on assets like the Bitcoin futures on the Chicago Mercantile Exchange (CME)?

If a US taxable person recognises a gain or loss on the sale or exchange of a virtual currency, the character of such gain or loss generally depends on whether such currency is a capital asset in that person's hands.[257] Assuming the US taxable person holds the virtual currency as a capital asset for more than one year, gains are generally treated as long-term capital gain.[258] For US tax-exempt persons, gains or losses from the sale or other disposition of property are generally not taxed as UBTI.[259] This UBTI exclusion does not apply, however, to inventory or property otherwise held primarily for sale to customers in the ordinary course of business.[260]

Does investing in virtual currencies constitute investing in securities or commodities for purposes of the Section 864 safe harbour (safe harbour) under the Internal Revenue Code of 1986 (the Code)? As described in greater detail in Section II, the CFTC considers virtual currencies as commodities subject to its regulation.[261] Similarly, the SEC has asserted jurisdiction when a virtual token offering has hallmarks of a security offering under the broadly interpreted *Howey* test for investment contracts.[262]

Can these authorities be applied, by analogy, to conclude that a non-US investor can claim the protection of the safe harbour? The activities of a US-based investment manager are generally attributed to a non-US investor who invests through this manager.[263] If this manager only engages in safe harbour activities (i.e., investing or trading in securities and commodities), such activities do not create a US trade or business for the non-US investor, and gains from such safe harbour activities generally do not constitute ECI.[264] If the non-US investor is not protected by the safe harbour, the activities of the US-based investment manager could create a US trade or business generating ECI for such non-US investor, subjecting such investor to US federal net income tax (up to 37 per cent for individuals, or 21 per cent plus 30 per cent branch profits tax for corporations).

While it may be reasonable for a non-US investor to claim the protection of the safe harbour by applying CFTC and SEC authorities by analogy, there is no assurance that the IRS or the courts would agree with such claim. As a result, the tax risk of being incorrect is material. Thus, any offering document for an investment fund that invests in a virtual currency targeted at non-US investors is expected to include robust tax disclosure specifically identifying the risks associated with an investment in a virtual currency. In addition, due to the material tax risks and depending on the precise investment strategy, a fund sponsor will have to make an important gating decision on how narrowly to tailor an offering's target market.

Many fund sponsors cast their nets wide for investors while utilising the most tax-neutral vehicle to raise money from such investors (i.e., no or de minimis entity level tax

257 I.R.S. Notice Q-6/7/A-6/7.

258 26 U.S.C. § 1222(3) (2018). A taxpayer's holding period could be suspended under certain rules, including the straddle rules under Section 1092 of the Code, if the taxpayer enters into hedging positions.

259 id., § 512(b)(5)(B).

260 Treas. Reg. § 1.512(b)–1(d).

261 See, e.g., CFTC Primer, footnote 58.

262 See, e.g., DAO Report, footnote 3.

263 This could be altered by income tax treaties.

264 This treatment could be modified by rules under 26 U.S.C. §§ 897, 1445, 1446 and the Treasury Regulations thereunder.

to the extent permitted under the law). Partnerships (or local law entities that can be treated as partnerships for US federal income tax purposes) are typical vehicles used for pooled investments in commodities and derivatives thereon. Partnerships are generally not taxed at the entity level, so there is very little expected US federal income entity tax cost. However, when interests of a partnership are publicly traded for US federal income tax purposes, the publicly traded partnership (PTP) is treated as a corporation subject to a corporate level income tax of 21 per cent unless certain exceptions apply. One exception is for small offerings (e.g., an offering for a private investment fund exempt from registration as an investment company under Section 3(c)(1) of the Company Act where the number of investors cannot exceed 100 and certain other requirements are met).[265] Another is where the partnership meets the qualifying income test, such that at least 90 per cent of the partnership's annual gross income consists of certain passive-type income.[266] Notably, gains from direct virtual currency investments are not explicitly included in the definition of qualifying income.[267]

For non-US investor virtual currency funds, the listing of Bitcoin futures on the CME is a positive development.[268] The safe harbour for trading or investing in commodities covers a non-US investor only if the commodities are of a kind customarily dealt in on an organised commodity exchange and if the transaction is of a kind customarily consummated at such place.[269] Thus, a non-US investor investing solely in these particular futures (directly or through a partnership for US federal income tax purposes) has tenable support for claiming safe harbour benefits.

Similarly, the CME Bitcoin futures support partnership tax treatment in the case of a PTP where the PTP invests solely in such futures, making possible a retail offering of such PTP interests. In the case of PTPs whose principal activity is the buying and selling of commodities (that are not inventory) or options, futures or forwards with respect to commodities, income and gains from futures on commodities constitute qualifying income.[270]

In addition, because the CME Bitcoin futures meet the definition of a Section 1256 Contract under the Code,[271] a US taxable investor generally recognises annual mark-to-market gain (60 per cent long-term capital gain and 40 per cent short-term capital gain) in respect of such investments (directly or through a partnership for US federal income tax purposes).[272]

Finally, while there are many uncertain areas relating to the taxation of virtual currencies and activities related thereto, it is worth noting that mining virtual currencies, when conducted in the United States, could be treated as the business of performing services such that any virtual currency from such mining is treated as ordinary income from services, and any taxable income (i.e., receipt of virtual currencies) from mining constitutes UBTI

265 Treas. Reg. § 1.7704-1(h).

266 26 U.S.C. § 7704(c) (2018).

267 id., § 7704(d).

268 'Now Available: Bitcoin Futures', CME Group, https://www.cmegroup.com/trading/bitcoin-futures.html (last visited July 5, 2019).

269 26 U.S.C. § 864(b)(2)(B) (2018).

270 id., § 7704(d)(1)(G).

271 A Section 1256 contract includes regulated futures contracts. A regulated futures contract is a contract with respect to which the amount to be deposited and the amount that may be withdrawn depends on a system of marking to market, and which is traded on or subject to the rules of a qualified board or exchange. The term qualified board or exchange includes a domestic board of trade designated as a contract market by the CFTC. id., §§ 1256(b)(1)(A), (g)(1), (g)(7)(B).

272 id., §§ 1256(b)(1), (g)(1), (g)(7), (a)(1), (a)(3).

and ECI.[273] Once a virtual currency is earned and taxed, such currency is merely property and, depending on what the taxpayer does with such currency and where such activities are undertaken, will have varying and potentially complex results for any particular taxpayer.

IX OTHER LEGAL CONSIDERATIONS

i State uniform regulation of virtual currencies

To provide a uniform framework among the various states for the regulation of virtual currency business activities, the Uniform Law Commission developed the Uniform Act.[274] As described in greater detail in Section III, the Uniform Act includes licensure, prudential regulations and customer protection requirements relating to certain businesses engaged in activities involving exchanging, transferring or storing virtual currencies. The Uniform Act is intended to provide a clear regulatory regime tailored to address issues specifically relating to virtual currency businesses, rather than the existing patchwork of money service and money transmitter licensure laws, and other, sometimes ambiguous or duplicative, existing regulatory regimes that could be applied to such activities among the various states. The motivation for developing the Uniform Act centred on a desire to provide legal certainty, which in turn would foster continued innovation and access to capital for businesses in the virtual currency space. The drafting process involved significant input from various industry, state and federal government participants, as well as practising lawyers and academics. The Uniform Act is now available and, to date, bills modelled on the Uniform Act have been introduced for consideration by legislatures in California, Oklahoma, Rhode Island, Nevada and Hawaii.[275] Notably, Wyoming enacted a bill (known as SF0125), which went into effect on 1 July 2019, that governs activities relating to digital assets and was not modelled on the Uniform Act.[276]

ii Uniform Commercial Code

The Uniform Commercial Code (UCC) provides the often-unnoticed plumbing for a broad range of commercial transactions and property rights. Where the UCC applies, parties benefit from clarity of law and special protections. Where the UCC does not apply, parties may unexpectedly find themselves without the benefit of legal rules they took for granted. Three key questions arise under the UCC with respect to virtual currencies: are virtual currencies subject to the regimes of UCC Article 3 (negotiable instruments), Article 4 (bank deposits and collections) or Article 4A (funds transfers); can virtual currencies serve as collateral under UCC Article 9; and can virtual currencies be credited as a security or financial asset to a securities account under UCC Article 8? Although we are not aware of any cases on point, we consider each question in turn below.

Applicability of UCC Articles 3, 4 and 4A

Virtual currencies as commonly structured today would not be subject to UCC Articles 3, 4 or 4A. Virtual currencies do not constitute a negotiable instrument, because they are not a

273 See I.R.S. Notice Q-9/A-9 (income from mining that is conducted as a trade or business is subject to self-employment taxes for non-employees engaged in mining).

274 Uniform Law, footnote 80.

275 See id.

276 Wyo. Stat. Ann. §§ 34-29-101 et seq. (2019).

paper asset.[277] In addition, most virtual currencies would fail to meet the requirements for a negotiable instrument, because there is no promise or order to pay a fixed amount of money, as this presupposes a counterparty who is either the promisor or who would be subject to the order. When a party holds a virtual currency, there is no counterparty against which it has a claim (at least until it decides to transfer the virtual currency in return for value). Most virtual currencies also are not tied to a fixed amount of money (although there are purported exceptions in which the value of a virtual currency is supposedly fixed to an actual value of money in a fashion seemingly analogous to an exchange rate peg). Virtual currencies do not fit within Articles 4 or 4A owing to the absence of a bank from the scene. This leaves a significant gap in the commercial law plumbing applicable to virtual currencies. Virtual currency transactions operate without the typical UCC legal protections that strip adverse claims, provide for clear ownership or enforceability and establish transfer warranties. In 2017, the Uniform Law Commission considered – but did not fill – that gap when it created the Uniform Act.[278]

Use of virtual currencies as collateral

Like most types of personal property, virtual currencies can serve as collateral under UCC Article 9.[279] Most virtual currencies will constitute a general or payment intangible under the UCC, and may also constitute proceeds of another form of collateral.[280] As a general or payment intangible, a security interest in a virtual currency can be perfected solely by the filing of a financing statement.[281] Unfortunately for an interested secured party, however, the classification of a virtual currency as a general intangible or payment intangible means that the priority of security interests in such virtual currency is determined in order of the first to file or perfect; thus, any prior liens on the virtual currency – which may be difficult to identify or trace – could take priority over such secured party's perfected security interest.[282] The parts of the UCC plumbing that strip prior liens when transfers are made involving money or bank accounts would not apply to virtual currencies as structured today.[283]

277 Neil Cohen, 'The Calamitous Law of Notes', 68 *Ohio St. L. J.* 161, 182 (2007).

278 To date, no state has adopted the Uniform Act. Note that this section addresses the model version of the UCC. Some states, most notably Wyoming, have attempted to amend their versions of the UCC to accommodate virtual currencies.

279 See, e.g., Jeanne L Schroeder, 'Bitcoin and the Uniform Commercial Code', 24 *U. Miami Bus. L. Rev.* 1 (2016).

280 Current virtual currencies are likely not money under the UCC, although that could change. UCC Section 9-102(b)(24) defines money as a 'medium of exchange currently authorized or adopted by a domestic or foreign government. The term includes a monetary unit of account established by an intergovernmental organisation or by agreement between two or more countries.' To our knowledge, no governments or intergovernmental organisations have yet authorised or adopted a virtual currency as a medium of exchange or unit of account, so such definition is inapplicable to virtual currencies in their current vestige, though such classification could be called into question if a government or intergovernmental agency were to so authorise or adopt a virtual currency. It should be noted, however, some have argued that even if a virtual currency was adopted as a medium of exchange or unit of account, it still would not fit within the UCC definition of money. See, e.g., Schroeder, footnote 279, at 20.

281 U.C.C. § 9-310, 9-312(b) (Unif. Law Comm'n 2018).

282 id., § 9-322.

283 See id. § 9-332.

Use of securities accounts

Because of the flexibility contained in UCC Article 8, virtual currencies can be credited to a securities account (as a financial asset) at a willing securities intermediary.[284] In fact, the Uniform Law Commission has completed a companion act to the Uniform Act that would require that virtual currencies regulated by the Act be held in securities accounts at a securities intermediary. Whether this model will be readily adopted by those who hold virtual currencies on behalf of others remains to be seen, as the benefits of certainty resulting from securities account treatment come with an accompanying increase in responsibility and liability for the entity acting as securities intermediary. Of course, state law UCC characterisation as a security does not mean that a virtual currency would be characterised as a security for federal regulatory purposes, including under the federal securities laws.

X BANKRUPTCY

Below we provide an overview of certain bankruptcy-related issues that may arise relating to virtual currencies in a bankruptcy proceeding under the applicable United States law. As noted earlier, there is continuing legislation and regulation from federal agencies and states such that there is a complex web of concurrent and overlapping regulatory and legislative developments that must be considered, as such could be relevant and persuasive in the context of a bankruptcy proceeding. There have been less than a handful of bankruptcy cases that have only tenuously considered or involved issues relating to virtual currencies. As such, the development of bankruptcy law involving virtual currency issues is in its very nascent stages.

i Applicable bankruptcy regime

The first question that needs to be addressed is which bankruptcy regime would apply. This would depend on the type of entity that becomes insolvent. If the entity is a broker-dealer or an SEC-registered broker-dealer that owns or is in the business of dealing with virtual currencies, then Subchapter III of Chapter 7 of Title 11 of the United States Code (Bankruptcy Code), or perhaps even the Securities Investor Protection Act of 1970, may apply; however, neither of these currently seem likely, as we are not aware of any SEC-registered broker-dealers in the brokerage business involving virtual currencies. More likely, an entity will be eligible to commence bankruptcy proceedings either under Chapter 7 (the liquidation chapter) or Chapter 11 (the reorganisation chapter) of the Bankruptcy Code.[285]

ii Virtual currencies as property of the estate

Upon the commencement of a bankruptcy case, an estate is created under Section 541 of the Bankruptcy Code, and an automatic stay arises enjoining all creditors and entities from, among other things, taking any enforcement actions against the debtor or against property of the estate, any actions to obtain possession of property of the estate or any actions to create, perfect or enforce any lien against property of the estate. Virtual currencies owned by a debtor should be treated as part of the property of that debtor's estate. Section 541 of the

284 See id. § 8-102(a)(9)(iii), which includes 'any property that is held by a securities intermediary for another person in a securities account if the securities intermediary has expressly agreed with the other person that the property is to be treated as a financial asset under this Article'.

285 See 11 U.S.C. § 109 (2018).

Bankruptcy Code provides that the property of a debtor's estate includes 'all legal or equitable interests of the debtor in property as of the commencement of the case', and courts have held that the scope of property interests included in a debtor's estate is intended to be quite broad. Although federal law governs the extent to which a debtor's interest in property is part of that debtor's estate, state law governs the nature and existence of the debtor's right to such property. Accordingly, bankruptcy courts would look to the applicable non-bankruptcy law to determine the property interests of the debtor in any virtual currency owned by a debtor, which would form part of the debtor's estate and be afforded the protection of the automatic stay subject to certain exceptions that may apply, as discussed further below.

While Section 541 of the Bankruptcy Code should include any virtual currency owned by the debtor, given the anonymous nature of the ownership of virtual currencies (through private keys known only to the owner of the virtual currency) it may be difficult to obtain complete transparency regarding the whereabouts, amounts and transactions relating to the debtor's virtual currency without the full cooperation of the debtor. However, a debtor is required to provide a full and accurate accounting of its property and other assets as part of filling out and filing with the bankruptcy court, under penalty of perjury, its schedules and statements of financial affairs.[286] A debtor should be incentivised to provide accurate and full accounting of its property, both because it would be subject to penalties and sanctions by the bankruptcy court, and may also be denied the benefit of a discharge of its debts and liabilities if it is found to have transferred, removed, destroyed, mutilated or concealed property of the debtor within one year before the commencement of the case or after the commencement of the case.[287]

However, creditors or other interested parties in a case involving a debtor with virtual currencies may consider taking action to assure full disclosure, such as conducting discovery against the debtor for information relating to its virtual currency transactions (including virtual currency addresses, public keys, private keys, exchanges used, digital wallet information, financial and other account statements and emails and other data that may be used to confirm virtual currency transactions), and subpoenaing major exchanges and payment merchants that could have additional information regarding a debtor's virtual currency transactions and holdings. The fact that virtual currencies, digital wallets and exchanges may be located and held in foreign jurisdiction may raise additional hurdles, and discovery may be a costly exercise; however, depending on the amount and value of the virtual currencies owned by the debtor, such costs may be worth the effort of pursuing such discovery.

iii Virtual currencies as cash collateral

As discussed in Section IX, a virtual currency may serve as collateral under UCC Article 9. Thus, it is possible that a debtor in a bankruptcy may own a virtual currency that is subject to a secured creditor's lien. There may be issues with the perfection of such security interest and the virtual currency may be subject to previously filed security interests; however, assuming the debtor's virtual currency is subject to a secured creditor's validly perfected lien, then such virtual currency may constitute cash collateral under the Bankruptcy Code. Under Section 363 of the Bankruptcy Code, cash collateral is defined as 'cash, negotiable instruments, documents of title, securities, deposit accounts, or other cash equivalents whenever acquired in which the estate and an entity other than the estate have an interest and includes proceeds'.

286 See id. § 521; Bankr. Rule 1007.

287 See 11 U.S.C. §§ 521, 523 (2018); Bankr. Rule 1007.

Section 363 further provides that a debtor 'may not use, sell or lease cash collateral' unless the relevant secured creditor consents or the court, after notice and a hearing, authorises such use of such cash collateral, typically by providing such secured creditor with adequate protection. Even if the virtual currency is not considered cash collateral, a secured creditor with a valid security interest in the virtual currency may seek similar adequate protection to protect its collateral from the debtor's use, sale or lease of such property.[288] Adequate protection typically is provided in the form of a cash payment, periodic cash payments or additional or replacement liens in order to protect the secured creditor against the diminution of value of the collateral from the debtor's use of such property rather than the return of such property to the secured creditor.[289] Accordingly, a secured creditor would have some protections from the debtor's use of a virtual currency subject to its liens; however, given the volatility in value of virtual currencies, such protection may not be adequate during a bankruptcy case if the value of the virtual currency decreases.

iv Valuation issues and obtaining highest value

The volatility of the value or price of virtual currency owned by a debtor also raises concerns as to how the debtor should maximise the value of its virtual currency, given that any decrease in value would impair the debtor's ability to satisfy unsecured creditors' claims or require additional collateral to protect secured creditors. Accordingly, if a debtor uses its virtual currency as a form of payment or merely holds it as an asset, it may behove the debtor and the creditors of the debtor to convert such virtual currency to cash through a methodology that maximises its value. Depending on the circumstances, that may dictate a prompt sale or a more systematic sale that better preserves its value and captures increases in value (if any). However, if the virtual currency is instrumental to the carrying out of the debtor's business function or the value of the business, or any restructuring depends on the retention and continued use of its virtual currency, then it may be more appropriate (albeit risky, if there is a significant decrease) for the debtor to retain and use its virtual currency in its business either with the court's permission or, if appropriate and within the applicable bankruptcy case law, in the ordinary course of its business.

v Treatment of certain contracts involving virtual currencies

Different provisions of the Bankruptcy Code may apply depending on the nature and type of contract involving a virtual currency. The only case to date dealing with a contract involving a virtual currency is *In re CLI Holdings, Inc*[290] (*CLI Holdings*). In *CLI Holdings*, the debtor, an affiliate of CoinLab, Inc, doing business as Alydian, was a Bitcoin miner using rigs or supercomputers to mine Bitcoins. The debtor entered into several Bitcoin service agreements whereby Alydian agreed to use commercially reasonable efforts to use supercomputers to mine for a specified number of Bitcoins for a customer in exchange for an upfront payment. Alydian determined that it was unable to mine sufficient Bitcoins to perform all of the service agreements because the costs of deploying the supercomputers exceeded the value of the Bitcoins mined. It therefore sought to reject the burdensome contracts pursuant to Section 365 of the Bankruptcy Code, which allows a debtor to reject executory contracts

288 See 11 U.S.C. § 363(e) (2018).

289 See id. § 361.

290 Case No. 13-19746 (W.D. Wash. 2013).

(i.e., contracts where performance remains due and owing from both parties to the contract). Several of the customers and counterparties to these Bitcoin service agreements filed objections to the debtor's motion to reject the contract on the grounds that the contract was not executory since they had fully performed their end of the contract and had no remaining obligations. The court denied the debtor's motion to reject the service agreements, finding that the contracts were not executory in line with analogous cases where the only remaining obligation under the contract is to receive the agreed product. Of further interest, the debtor in *CLI Holdings* subsequently moved to sell its mining rigs on an expedited basis through a Section 363 sale in the bankruptcy case. The bankruptcy court also denied its 363 sale motion, expressing several concerns regarding the ownership of the rigs, the accuracy of the debtor's financial statements and the lack of transparency, which the court observed could cause her to appoint a trustee or dismiss the case, allowing the parties to continue litigation that had been pending but stayed in New York State and federal courts. This further underscores the need for accurate schedules and financial statements and transparency in a bankruptcy case involving virtual currencies.

vi Potential safe harbour contracts – currencies, commodities and securities

Other contracts that may be involved in a bankruptcy case involving virtual currencies may provide special protections to counterparties, depending on the determination of whether the virtual currency at issue is a currency, a security or a commodity. As noted previously, different federal regulators, state legislators and courts have given conflicting views on whether virtual currencies are currencies, securities or commodities, and such determination may depend on the specific facts and circumstances involving the virtual currency and its use. A transaction involving currency could be considered a swap agreement under the Bankruptcy Code, given that the definition of swap agreement includes a currency swap, option, future or forward agreement.[291] Similarly, if the virtual currency is considered a security, a transaction involving the 'purchase, sale or loan' of such virtual currency could meet the definition of a securities contract under the Bankruptcy Code.[292] If the virtual currency is considered a commodity, there is a higher hurdle to meet the requirements for a forward contract, which requires that the 'purchase, sale or transfer of a commodity' has a 'maturity date more than two days after the date the contract is entered into'.

If a transaction or agreement involving a virtual currency satisfies the requirements of any of these safe-harboured financial contracts (i.e., a swap agreement, securities contract or commodity contract), then the non-debtor counterparty would be afforded certain rights. Such rights include the ability to terminate, accelerate or liquidate the contracts and foreclose on any collateral held by the non-debtor counterparty, and to exercise rights of netting or set-off, notwithstanding the automatic stay that would typically enjoin non-debtor counterparties from taking such enforcement actions.

Another favourable safe harbour protection that could be available if contracts for virtual currencies are determined to satisfy the definitions of a swap agreement or forward agreement is that the Bankruptcy Code prohibits a debtor from avoiding transfers that would otherwise be a preference or fraudulent transfer (other than actual fraud). Thus, non-debtor counterparties would be protected from having virtual currencies or payments or

291 See 11 U.S.C. § 101(53B) (2018).

292 See id. § 741(7).

other transfers in connection with a swap agreement or forward contract made prior to the commencement of the bankruptcy case from being clawed back or avoided and required to be turned over to the debtor.

To be clear, there have been no bankruptcy court decisions with regard to these safe harbour protections in connection with any virtual currencies to date, and as such, the treatment or availability of these protections remain unclear. In addition, although these safe-harboured contract provisions were not legislated with virtual currencies in mind, the definitions of a swap agreement and a forward contract were drafted to include contracts regarding swaps or commodities that in the future become the subject of recurrent dealings in the swap or other derivative markets or the forward contract trade.

vii Avoidance actions

Another area in which virtual currencies and their value will be of significant importance in a bankruptcy case is in the debtor's ability to recover a virtual currency or the value of the virtual currency as an avoidable transfer (as preferences or fraudulent transfers). For the purposes of this overview, an assumption is made that transfers of virtual currencies that satisfy the requirements of a voidable preference or fraudulent transfer can be voided by a debtor pursuant to Sections 547 and 548 of the Bankruptcy Code. There may be difficulties in identifying transfers of virtual currencies and, more importantly, likely greater difficulty identifying the transferees of such transfers, but here we highlight the issue of whether a court would allow the debtor to recover the virtual currency or the value of the virtual currency under Section 550 of the Bankruptcy Code. Section 550 allows the debtor to 'recover, for the benefit of the estate, the property transferred, or, if the court so orders, the value of such property'. The issue with virtual currencies is whether they would be treated in a bankruptcy case as currency or property. If a virtual currency is treated as currency, then the debtor may only be able to recover the value of the transferred property and may not benefit from any appreciation of the virtual currency. However, a court may take the view that the appreciation of a virtual currency should be recoverable by the estate, and thereby allow the recovery of the virtual currency, which would include any appreciation thereof. The latter approach is in line with Section 550's goal of 'putting the estate back where it would have been but for the transfer'.[293] This approach is also in line with the treatment of virtual currencies as property or a commodity rather than a currency, which seems to be more consistent with the current regulatory trends for the treatment of virtual currencies.

One bankruptcy court was faced with this issue when a liquidating trustee sought to recover Bitcoins or their present value, which had appreciated from the time of transfer. The bankruptcy court ultimately did not decide whether the Bitcoins were currency or a commodity, but found instead that Bitcoins were not US dollars, leaving for a subsequent determination whether it would allow the recovery of the virtual currency or the value of the virtual currency.[294] Given the CFTC's stance that a virtual currency is a commodity, it may be that courts allow the recovery of virtual currencies, including any appreciation thereon.

293 See *Collier on Bankruptcy* ¶ 550.02[3][a].

294 See *Kasolas v. Lowe* (*In re Hashfast Techs LLC*), Adv. No. 15-3011 (Bankr. N.D. Cal.).

viii Recognition of foreign proceedings

As many virtual currency exchanges and entities doing business with virtual currencies may not be located or have their primary place of business within the jurisdiction of the United States, related bankruptcy activity may occur outside the United States; however, such foreign bankruptcy proceedings may benefit from the assistance of the United States bankruptcy courts through recognition proceedings under Chapter 15 of the Bankruptcy Code. Such was the case with the bankruptcy proceedings of MtGox Co Ltd in Tokyo, Japan, which sought and obtained recognition of the Japanese bankruptcy proceedings as foreign main proceedings through Chapter 15 of the Bankruptcy Code. Recognition of its Tokyo bankruptcy proceedings provided much-needed relief in the United States, including a stay that enjoined several lawsuits and allowed the Japanese foreign representative full and unfettered access to the US courts. The recognition order expressly provided the foreign representative with the 'right and power to examine witnesses, take evidence or deliver information concerning the [d]ebtor's assets, affairs, rights, obligations or liabilities'; and 'entrusted [the foreign representative] with the administration and realisation of all of the [d]ebtor's assets within the territorial jurisdiction of the United States'.[295] Thus, recognition by US bankruptcy courts of foreign bankruptcy proceedings involving virtual currencies may assist foreign debtors to identify and recover their property for the benefit of their creditors.

XI LOOKING AHEAD

The US regulatory environment applicable to virtual currencies and other digital assets is highly complex. US federal and state lawmakers and regulators are grappling with how to fit these new asset classes into existing legal and regulatory regimes, and whether to develop new law, rules or guidance to address the unique aspects of digital assets (and the unique issues they raise). If the authors had to characterise the overall US regulatory approach, they would say that most US regulators are educating themselves about blockchain technology and the evolving digital asset landscape. In some cases, regulators, and notably the CFTC, have attempted to protect the public while not taking aggressive actions that could stifle innovation in this area. However, notwithstanding that the CFTC and the SEC have appointed staff members to work with digital asset sponsors and issuers to understand their products and trading platforms, the agencies have brought several enforcement actions to protect the public from fraud and registration abuses. While it is impossible to predict with any certainty the future direction of virtual currency regulation in the United States, it does appear that US regulators recognise that virtual currencies are here to stay. Innovators in the virtual currency space would be well-advised to review this chapter carefully, engage actively with experienced US counsel and follow closely regulatory developments in this area. Failure to fully comply with applicable US regulatory regimes may expose market participants to an unacceptable level of legal, regulatory and reputational risk.

295 See *In re MtGox Co, Ltd*, Case No. 14-31229, D.I. 151 (Bankr. N.D. Tex. June 18, 2014).

Appendix 1

ABOUT THE AUTHORS

CHERISE ABELA GRECH

GTG Advocates

Dr Cherise Abela Grech is a senior associate at GTG Advocates who regularly advises on virtual currencies and distributed ledger technologies, including in respect of security token offerings, virtual currencies-related activities requiring investment services licensing and investment funds investing in virtual currencies. She is also highly experienced in financial services, blockchain, corporate and commercial law, insurance and captives, financial institutions, credit institutions and pension schemes. A member of the Chamber of Advocates, Dr Abela Grech holds a Doctor of Laws awarded by the University of Malta and has successfully read for a master's degree in financial services from the same institution, where she focused her thesis on exchange-traded funds and the growth opportunities for these types of structures in the Maltese investment funds industry. She also possesses a Foundation Certificate in trusts law and management, and lectures on innovative technology services and arrangements.

LUÍS ALVES DIAS

Uría Menéndez-Proença de Carvalho

Luís Alves Dias is an associate in the Lisbon office of Uría Menéndez-Proença de Carvalho, having joined the firm in December 2015.

Between September 2012 and November 2015, Luís was a member of Linklaters LLP's team in Portugal, where he mainly focused his practice on providing legal advice to domestic and international clients in the context of corporate M&A transactions, in particular sales and acquisitions of companies and businesses located in Portugal, but also in Angola and Mozambique.

Currently, his professional practice is mainly focused on providing legal advice to domestic and international clients regarding banking and finance law, fintech and insurance law in both the regulatory and in the purely transactional strands.

Luís is a founding associate of the Portuguese FinTech and InsurTech Association (AFIP), co-coordinator of the RegTech Working Group of AFIP and co-founder of the Lisbon chapter of Legal Hackers.

ADRIAN ANG

Allen & Gledhill LLP

Adrian Ang is a partner in the financial services department and is co-head of the firm's fintech and public policy practices.

Adrian has been active in the fintech sphere, being involved in contributing to policy formation and the enactment of fintech-related legislation. He has advised on a variety of fintech models, including equity and debt crowdfunding platforms, P2P lending platforms, online lending intermediary-based platforms, online money transfer systems, online payment system providers, robo-advisers, virtual stored value facility providers and initial coin offering structures.

Adrian is ranked as a Band 1 fintech practitioner in *Chambers FinTech* (2019). One source comments that he has 'never seen an external lawyer respond in such a fast, succinct way. His responsiveness is incredible.' Adrian is the only lawyer who is named as a Global Elite Thought Leader in the Asia-Pacific in *Who's Who Legal: Banking 2019*, as part of the fintech analysis. It states that he is 'one of the stars of the international fintech market. Clients enthusiastically praise his "deep understanding of capital markets, the jaw-dropping speed of his responses and his affable yet professional nature"'. *Who's Who Legal* also notes that he is 'renowned for his "unparalleled understanding of blockchain technology"', and 'clients across the board comment that they "have complete confidence in him"', praising his 'ability to connect the dots from a both technological and legal perspective'. Adrian is also recommended for his expertise in financial regulatory work by *Chambers Global* (2019), *Chambers Asia-Pacific* (2019) and *The Legal 500 Asia Pacific*.

NICHOLAS AQUILINA

Brandl & Talos Rechtsanwälte GmbH

Nicholas Aquilina is an attorney at Brandl & Talos, specialising in payments, including virtual currencies and cryptocurrencies, as well as international gaming, betting and entertainment law.

Nicholas provides regulatory advice in the field of virtual and cryptocurrencies, including the applicability of financial services regulation to the use of cryptocurrencies and in preparation of initial coin offerings and initial token offerings. He also advises on the use of virtual currencies and cryptocurrencies in the wider e-commerce sector as well as specifically for gaming and social gaming offers. Nicholas also provides regulatory, commercial, compliance and transactional legal advice to leading international online and land-based gaming and betting companies.

Since joining Brandl & Talos in 2009, Nicholas frequently contributes to Austrian and international legal journals and regularly speaks at international conferences.

GEOFFREY F ARONOW

Sidley Austin LLP

Geoffrey Aronow is a partner in the Washington, DC office of Sidley Austin LLP. He has served as counsel for over 30 years in a wide variety of government enforcement investigations and proceedings before the Commodity Futures Trading Commission, the Securities and Exchange Commission and other federal regulatory agencies. He also advises clients on compliance with regulatory requirements and related training. He has been advising clients

with regard to the impact of these agencies' regulatory schemes on various crypto and virtual asset ventures. He served as director of enforcement at the CFTC from 1995 to 1999, and in a variety of senior positions at the SEC, including general counsel, from 2013 to 2014. He was selected as a 'Leading Lawyer in Derivatives Law, Securities Regulation and Litigation – Securities' by *The Best Lawyers in America*, and has taught futures and derivatives law at the law schools at Catholic University of America and The George Washington University. He is a 1980 graduate of Yale Law School and a 1976 *summa cum laude* graduate of Yale College.

MARCUS BAGNALL

Webb Henderson

Marcus Bagnall is an experienced commercial and corporate lawyer specialising in TMT, intellectual property and privacy. His experience includes private M&A transactions, fundraising, structuring and governance. Marcus also advises entrepreneurs and investors in tech start-up and other early-stage companies on their legal and commercial issues, such as structuring, governance, incentive arrangements, fundraising, investments and exit.

MATTHIAS BERBERICH

Hengeler Mueller Partnerschaft von Rechtsanwälten mbB

Matthias Berberich, Dr iur, LLM, is counsel at Hengeler Mueller's Berlin office and part of the IT and IP and TMT practice group. He advises and represents companies and business associations, predominantly from the IT, technology, communication and media sectors. His practice focuses on IP and IT, technology-related M&A transactions, outsourcing and joint venture projects, litigation and arbitration as well as regulatory advice, inter alia, for internet, telecommunication, media, fintech, e-commerce and data-driven business models. He is author of various publications and visiting lecturer at the Humboldt University Berlin.

Matthias Berberich studied at the Humboldt University Berlin. He holds an LLM from the University of Cambridge as well as a PhD from the Humboldt University Berlin. Prior to joining Hengeler Mueller, he has worked as a researcher and teacher at the Humboldt University Berlin, and further with the German Federal Ministry of Justice and the Federal Association for Information Economy, Telecommunication and New Media (BITKOM) in Berlin.

LOUIS BIDAINE

MVR Legal BV

Louis Bidaine holds a master of laws degree from the Catholic University of Louvain, Belgium and has a strong interest in new technologies, including blockchain and virtual currencies. Louis Bidaine is currently active as the legal and ICO project manager for Profila GmbH.

JAMES B BIERY

Sidley Austin LLP

James B Biery is a partner in the investment products and derivatives group at Sidley Austin LLP in Chicago. He advises and represents clients in securities and derivatives-related regulatory and corporate matters, including the organisation, operation and offering of interests in US and offshore hedge funds, funds-of-funds, commodity pools, private equity

and control or distressed debt funds, the organisation and operation of investment advisers, commodity pool operators and commodity trading advisers, and fund restructurings. Mr Biery received a BA in philosophy from the University of Chicago in 1983 and a JD from the University of Wisconsin in 1993.

ANDREW P BLAKE

Sidley Austin LLP

Andrew Blake is a partner in Sidley's Washington, DC office in the securities and derivatives enforcement and regulatory group. Andrew focuses his practice on the regulation of financial markets and intermediaries, including clearing organisations, transfer agents, exchanges, trading platforms, broker-dealers, futures commission merchants and private funds. He has deep experience in particular with the options markets, and frequently advises clients on regulatory and operational issues regarding the clearance and settlement of equity and debt instruments, evolving regulations for swaps and security-based swaps and participation in central counterparties, depositories and trading platforms. On a regular basis, he also counsels clients on clearing arrangements, customer protection regulations, trading issues and financial contracts.

DEEMPLE BUDHIA

Russell McVeagh

Deemple Budhia is a partner in Russell McVeagh's finance and fintech teams. Deemple has 21 years' experience in financial regulation (including anti-money laundering, consumer credit, financial advice and prudential regulation of financial institutions) and debt capital markets. She has worked in both New Zealand and the United Kingdom. Prior to joining Russell McVeagh, she spent several years in London working in Allen & Overy's securitisation team, and as an originator in Citibank's European commercial property and securitisation team.

TERENCE CASSAR

GTG Advocates

Dr Terence Cassar is a senior associate at GTG Advocates who is highly experienced in TMT, IP, blockchain and cyptocurrencies, fintech, data protection and privacy, gaming and betting, e-commerce and cybercrime. In the fintech field, he specialises in advising virtual financial assets service providers and initial coin offerings (ICOs), and was one of Malta's first lawyers to advise on ICOs. Dr Cassar is currently advising various major crypto exchanges in relation to licensing under the Virtual Financial Assets Act. He has also represented various clients before the European Intellectual Property Office, negotiated a high-profile settlement against a major Malta Gaming Authority-licensed platform-provider and led the negotiations in relation to various major franchises. A member of the Chamber of Advocates, Dr Cassar was a key expert on the Malta IP Hub, an initiative to amend local IP laws, and has led the General Data Protection Regulation compliance of various organisations, including Malta's foremost utility provider.

PETER CHAPMAN

Clifford Chance LLP

Peter Chapman is a partner in the financial services and markets regulatory group at Clifford Chance in London. Peter has worked on a range of regulatory implementation projects relating to post-crisis derivatives reform (such as EMIR), securities market developments (such as MiFID II and PRIIPs), and banking and payments (such as PSD2, DGSD2, the EU Funds Transfer Regulations), often alongside colleagues in the technology, media and telecommunications group. Peter also co-leads the firm's international fintech group and has significant experience of advising on virtual currency regulation. Peter has previously undertaken client secondments at Barclays, Citibank, UBS and Nasdaq.

VICTOR CHARPIAT

Kramer Levin Naftalis & Frankel LLP

Victor Charpiat's practice focuses on financial market regulations, as well as the regulation of fintech, blockchain and cryptocurrencies. Victor also advises French and foreign financial institutions with respect to financial services (notably, the marketing of financial products, investment services and post-market regulation) and other financial market transactions (credit loans, bond issuances, Euro PP, ICOs).

BRUNO LORETTE CORRÊA

Pinheiro Neto Advogados

Bruno Lorette Corrêa is an associate in the tax area of the Pinheiro Neto Advogados office in São Paulo. His fields of expertise are tax planning at domestic and international level, judicial and administrative litigation, and advice on all tax issues. Mr Corrêa graduated with an LLB from the São Paulo Catholic University in 2018.

ALIX D'ANGLEJAN-CHATILLON

Stikeman Elliott LLP

Alix d'Anglejan-Chatillon is a partner and co-head of Stikeman Elliott LLP's financial products and services group. She practises principally in the areas of investment management, the regulation of capital markets and derivatives. Her clients include managers of North American-, European- and Asian-based investment funds, including private equity funds, hedge funds, venture capital funds, mutual funds and fund of funds, as well as other asset managers, broker-dealers, and commercial and investment banks. Alix also regularly advises on securities and derivatives regulatory matters relating to financial markets infrastructure and trading platforms, cryptoasset and blockchain technology and transactions, fintech solutions, and other emerging financial products and technologies.

CAROLINE DEVLIN

Arthur Cox

Caroline Devlin is a partner in the Arthur Cox tax group, and is an experienced partner in taxation, in particular in financial services issues. She is a member of the Law Society Taxation Committee, and represents the Law Society in many of its dealings with the Irish Revenue Commissioners. She is editor and co-author of the Institute of Tax publication,

The Law and Practice of Stamp Duty. Caroline advises domestic and international clients on tax planning, including in particular financial services, and also involving cryptocurrencies and ICOs, along with raising capital products for companies and financial institutions. She is very experienced in advising clients how to establish in the most efficient manner in Ireland.

JUAN M DIEHL MORENO

Marval, O'Farrell & Mairal

Juan M Diehl Moreno has been a partner of Marval, O'Farrell & Mairal since 2006. He specialises in foreign investments, M&A, banking, fintech and capital markets law. Several legal guides have recognised Mr Diehl Moreno for several years as one of the leading lawyers in his fields of practice in the Argentine legal sector. From 2000 to 2001, he was a foreign associate at Sidley Austin LLP (New York office). He graduated from the Catholic University of Argentina in 1993, and he obtained a master's degree in business law from Austral University in 1996 and an LLM, with honours, from Northwestern University School of Law in 2000. He has lectured at several conferences in Argentina and abroad, and has published various articles on his field of expertise.

LAURA DOUGLAS

Clifford Chance LLP

Laura Douglas is a senior associate knowledge lawyer in the financial services and markets regulatory group at Clifford Chance in London. Laura advises on a wide range of regulatory developments and current issues, including in relation to securities and markets regulation, payments, settlement and netting. With a background in physics, she is particularly interested in how technology is transforming financial services and the legal and regulatory response to these changes.

SILKE NOA ELRIFAI

Amereller

Silke Noa Elrifai is of counsel at Amereller and the general counsel/chief legal officer for GNOSIS, a leading blockchain venture building decentralised applications on the Ethereum blockchain. She practises in the field of blockchain regulation, blockchain-related investments and international arbitration, mainly in and relating to the Middle East and North Africa.

FABIO ELSENER

Schellenberg Wittmer Ltd

Fabio Elsener is a senior associate in Schellenberg Wittmer's banking and finance group in Zurich.

Fabio Elsener studied law at the University of Zurich (master of laws, 2013) and at the Maastricht University in the Netherlands (LLM, 2012). During his studies he worked as a legal associate in a fintech start-up in Zurich and completed internships in law firms in Zurich and Paris, France.

Following the completion of his studies, Fabio Elsener gained experience as a legal intern at the Enforcement Division of FINMA, the Swiss Financial Market Supervisory Authority, in Berne.

Fabio Elsener joined Schellenberg Wittmer in 2014 as a trainee lawyer. After his admission to the Bar he rejoined the firm as an associate in 2016.

DANIEL ENGOREN

Sidley Austin LLP

Dan Engoren is an associate in the securities and derivatives enforcement and regulatory practice in the firm's New York office. His practice focuses on regulatory, corporate and business issues related to digital asset trading platforms, blockchain technology projects, cryptocurrency funds and other fintech companies.

OLIVIER FAVRE

Schellenberg Wittmer Ltd

Olivier Favre is a partner in Schellenberg Wittmer's banking and finance group in Zurich. Olivier focuses on derivatives, structured finance and capital markets transactions, and advises clients on financial services, securities, commodities, fund and insurance regulation. He also advises clients on fintech solutions and their legal implementation. He acts for a broad range of clients, including financial institutions, buy-side firms, issuers, insurance companies and industry associations. He is an authorised representative at the SIX Swiss Exchange.

Olivier obtained a doctorate degree in law from the University of Zurich in 2003 (iur, 2003) and a master's degree in law from Harvard Law School (LLM, 2004). For his doctorate thesis, he received the Issekutz Award for outstanding achievements in business law from the University of Zurich.

Prior to joining Schellenberg Wittmer in 2009, Olivier practised as a lawyer in London, specialising in OTC derivatives and structured finance transactions, fund products and capital markets transactions. From 2004 to 2007, he was an associate in Allen & Overy LLP's London-based derivatives practice group. From 2007 to 2009, he was legal counsel in the derivatives and structured finance group at Goldman Sachs International in London.

VEGARD ANDRÉ FISKERSTRAND

Schjødt

Vegard is an associate in Schjødt's finance and capital markets department. He joined Schjødt in 2016, and specialises in financial markets legislation, capital markets, and securities and investment law. Vegard holds a master's degree in law from the University of Oslo. He also holds a BSc and an MSc from the Norwegian School of Economics (NHH) with a specialisation in finance. Vegard has experience gained from working with financial institutions in Norway.

HÉLDER FRIAS

Uría Menéndez-Proença de Carvalho

Hélder Frias joined the Lisbon office of Uría Menéndez-Proença de Carvalho in 2006 and became a senior associate in 2015. Hélder worked in the London office of the firm from September 2010 to August 2011.

His practice is focused on banking, finance and insurance. Notably, he advises on M&A transactions involving financial institutions, bancassurance joint ventures, the transfer of insurance portfolios, and on other regulatory matters related to these markets, including insurance and reinsurance intermediation.

Hélder frequently advises on regulatory and supervisory aspects of financial and insurance activities (including banking and financial intermediation services and payment services), such as lending, creation of security, factoring, sale and purchase of receivables, money laundering, venture capital and financial products, and investment and retail banking and insurance instruments (capital redemption transactions and unit-linked life insurance agreements).

DOMINIQUE GALLEGO

Sidley Austin LLP

Dominique 'Monique' Gallego is a tax partner in Sidley Austin LLP's New York office. She has extensive experience in providing integrated global tax planning for alternative asset managers with international operations, international investments, or both. Monique focuses on US inbound issues related to credit, real estate, digital assets and other complex investments and outbound issues involving investment platforms in Ireland, Luxembourg and similar jurisdictions. Monique provides strategic advice to fund clients subject to IRS audits on US trade or business and international tax issues. Monique advises on the creation of legal and tax optimal manager and fund entities, optimal entry and acquisition, and holding and exit of diverse and international investments, including the creation and use of financial products for financing and other business purposes.

Prior to joining Sidley as a partner, Monique was a partner and principal at Ernst and Young LLP. She was also a partner at another global law firm, and previously was an associate in Sidley's tax practice. Monique participates in various speaking engagements with the Practising Law Institute, American Bar Association, Managed Funds Association and Hedge Fund CFO Association, and was a recognised tax adviser in *The Legal 500*.

IAN GAUCI

GTG Advocates

Dr Ian Gauci is the managing partner at GTG Advocates and head of the fintech department within the firm. He has a wealth of experience in fintech, blockchain and cryptocurrencies, TMT, financial services, data protection and privacy, competition, gaming and betting, IP, e-commerce, cybercrime, consumer law, information society, broadcasting law, e-health and M&A. He is a board member of the Malta Blockchain Association (of which he was also a co-founder) and a member of the University of Malta Distributed Ledger Technologies Board and the Chamber of Advocates. Dr Gauci was also one of the founders of the Malta IT Law Association. He was appointed as the legal expert on the National Blockchain Taskforce that was entrusted with reviewing proposals and making recommendations to the government of Malta to implement its National Blockchain Strategy, which resulted in the promulgation of the Virtual Financial Assets Act, the Malta Digital Innovation Act and the Innovative Technology Arrangements and Services Act. Dr Gauci is also an adviser to the Malta Communications Authority, the Malta Financial Services Authority and the Malta Digital Innovation Authority.

ALBERTO GIL SORIANO

Uría Menéndez

Alberto Gil Soriano joined Uría Menéndez in 2012 and is a senior associate in the tax department.

He has more than six years of experience advising resident and non-resident entities in general tax law and anti-money laundering and terrorist financing matters. He has also expertise in tax planning for high net worth individuals, in tax litigation and in local taxes. In addition, he has broad experience in tax regularisations.

FERNANDO MIRANDEZ DEL NERO GOMES

Pinheiro Neto Advogados

Fernando Mirandez Del Nero Gomes joined Pinheiro Neto in 2002 and works in the São Paulo office. Fernando's practice is primarily focused on the financial institutions and payments sector, advising local and international institutions in general regulatory matters, mergers and acquisitions, joint ventures, and local and cross-border structured finance. From 2012 to 2014, he worked as an investment banker at Deutsche Bank in New York, covering financial institutions and assisting them in varied corporate finance matters. Fernando holds an LLB degree from the University of São Paulo Law School and an MBA degree from the Wharton School of the University of Pennsylvania, where he graduated as a Palmer Scholar.

RAMANDEEP K GREWAL

Stikeman Elliott LLP

Raman Grewal is a partner in Stikeman Elliott's corporate group. She practises principally in corporate finance and mergers and acquisitions, having expertise in a wide range of matters including domestic and international offerings, corporate governance and securities regulatory compliance as well as capital markets developments. As part of her practice, Raman advises on capital market infrastructure and compliance, including trading facilities and other marketplaces and market participants. Raman's expertise also extends to securities regulatory implications relating to the issuance and trading of cryptocurrencies, where she has gained unique insights into the regulatory framework, the development of policies and other emerging considerations for the industry. Raman is a former member of the Securities Advisory Committee of the Ontario Securities Commission.

CHRISTOPHER GUNSON

Amereller

Christopher Gunson is a partner at Amereller based in the firm's Dubai office. He represents a broad client base of multinational companies on all aspects of business in the Middle East region. This work includes commercial transactions, strategic investments, joint ventures, technology transactions and regulatory compliance.

IRENE HALFORTY

Webb Henderson

Irene Halforty is a commercial lawyer experienced in providing legal and regulatory advice in TMT, privacy and data, communications and IP, as well as general corporate and commercial matters.

TERESA WILTON HARMON

Sidley Austin LLP

Teresa Wilton Harmon is a partner in the firm's global finance practice area, focusing on financial transactions and commercial law. Her financial transactions experience includes secured and unsecured loans, workouts and restructurings, structured finance and securitisation. For over 20 years, Teresa's practice has placed particular emphasis on financial transactions involving regulated and emerging industries, including derivatives, clearing organisations, exchanges, financial market utilities, student loan companies, electric utilities and fintech companies. Teresa's commercial law practice includes all articles of the Uniform Commercial Code, with a special emphasis on Article 9 secured transactions. Teresa's commercial law experience includes using the tools of commercial law to help clients build and navigate blockchain, distributed ledger technology, virtual currencies, digital currencies and tokenised security platforms. Teresa has honed her UCC knowledge as an active participant in UCC drafting committees, as a member of the Permanent Editorial Board for the UCC and as an adjunct professor teaching secured transactions at The University of Illinois College of Law. She is a nationally recognised speaker on UCC and other commercial law issues, and is co-author of a widely distributed annual Commercial Law Developments update. Teresa earned her law degree from The University of Chicago Law School, where she was a member of Order of the Coif and *The Law Review*. She received a BS and an MBA from the University of Alabama.

TAREK HOUDROUGE

Schellenberg Wittmer Ltd

Tarek Houdrouge is a partner in Schellenberg Wittmer's banking and finance, and corporate and commercial group in Geneva. He is co-head of the banking and finance team in Geneva and head of the firm's African regional desk.

Tarek's main areas of expertise are banking and finance, transactions and corporate law, combining banking and finance expertise with an M&A practice. He advises banks and financial institutions on regulatory matters and clients on financing and M&A, in particular involving regulated financial institutions. Tarek's practice also covers commercial contracts and commercial transactions, including restructuring, private equity and joint ventures.

Following his Swiss Bar admission in 2006, Tarek obtained a master of laws from Northwestern University School of Law (Chicago) in 2010 and was admitted to the New York State Bar in 2011. Prior to joining Schellenberg Wittmer, where he has been a partner since 2017, Tarek worked at another big business law firm in Geneva.

NATHAN A HOWELL

Sidley Austin LLP

Nathan Howell is a partner in Sidley's Chicago office in the investment funds, advisers and derivatives practice group. His practice focuses on futures and derivatives regulation, transactions and compliance, with a core focus on Commodity Exchange Act, Commodity Futures Trading Commission (CFTC) and Dodd-Frank Act matters. Mr Howell frequently advises clients on issues related to cryptocurrency, blockchain and distributed ledger technology, and tokenised assets. He understands the complexities of the current legislative and regulatory environment in the United States in light of the disruption caused by technology. His clients rely on him to understand complexity, while providing practical and straightforward solutions.

TOM HUNT

Russell McVeagh

Tom is head of Russell McVeagh's fintech team and a partner in the finance team. Tom has a broad range of banking and financial regulation experience gained in New Zealand and the United Kingdom. He is regarded as a leading expert on New Zealand's Anti-Money Laundering and Countering Financing of Terrorism Act 2009, with particular expertise in relation to financial adviser legislation, and all aspects of the prudential regulation of banks and insurers.

KEN KAWAI

Anderson Mori & Tomotsune

Ken Kawai has extensive experience advising financial institutions, fintech start-ups, investors and corporate clients on complex finance and financial regulatory matters.

Ken focuses primarily on the fintech industry, and regularly advises fintech companies, financial institutions, international organisations and self-regulatory organisations on legal issues surrounding fintech, including the complex legal framework governing cryptocurrencies, initial coin offerings and blockchain.

Ken also specialises in derivatives, and has counselled global banks, broker-dealers and investors on regulatory matters and best practices in respect of derivatives and related products. He derives his deep and practical knowledge in this area from his 17-year career at MUFG Bank, Ltd (formerly known as the Bank of Tokyo-Mitsubishi and, prior to that, the Bank of Tokyo Ltd), where he was involved in derivatives trading and marketing.

JOON YOUNG KIM

Kim & Chang

Joon Young Kim is a senior attorney at Kim & Chang. His practice focuses on e-finance and fintech, insurance, non-bank financial companies, corporate governance, mergers and acquisitions, and foreign direct investment.

Mr Kim regularly advises financial industry clients on regulatory, governance and corporate law-related matters. He has also successfully advised clients in disputes and in litigation, as well as in responding to inquiries or investigations from government and regulatory authorities.

He also regularly advises clients on legal issues relating to the latest innovations, such as blockchain technology, cryptocurrency and cloud computing.

Mr Kim has been actively involved in various Korean and international journals, and conducting lectures related to e-finance and fintech, blockchain technology, cryptocurrency, insurance and corporate governance.

His expertise and experience has been recognised by industry experts. He has been named as a 'Next Generation Lawyer' for two consecutive years in *The Legal 500 Asia Pacific* 2017 and 2018 editions.

SAMUEL KWEK

Allen & Gledhill LLP

Samuel Kwek is a senior associate in the financial services department. He regularly advises on regulatory and compliance matters within the financial services arena, such as licensing and conduct of business requirements and anti-money laundering.

Samuel also takes a keen interest in the fintech sphere. He has advised various players in the fintech industry such as digital payment token exchanges, utility token issuers and technology companies on the regulatory issues involved in services such as digital payments, utility token offerings and blockchain technology.

Samuel graduated from the National University of Singapore with an LLB (Hons) degree in 2015. He was called to the Singapore Bar in 2016 after completing his training contract with Allen & Gledhill and has been with the firm since then.

JUNG MIN LEE

Kim & Chang

Jung Min Lee is a senior attorney at Kim & Chang who specialises in finance. He primarily provides legal advice on banking regulations, fintech, electronic banking, and personal and financial information protection. Mr Lee's clients include Korean and global financial companies, Korean and global portal and platform service providers, e-commerce and payment service providers, and IT service providers.

Since joining the firm in 2008, Mr Lee has advised clients on various legal, administrative and technical regulations related to electronic banking, and on the management and protection of financial transaction information. Mr Lee is also licensed to practise as a public accountant and is registered as a certified public accountant.

ÉRIC LÉVESQUE

Stikeman Elliott LLP

Éric Lévesque is a partner and member of the tax group. His main areas of practice include tax and legal advice on mergers and acquisitions, cross-border structuring and financing, investment fund structuring and the taxation of financial instruments. His fintech practice focuses on tax considerations applicable to virtual currencies, including mining, as well as domestic and international fintech tax matters. Éric's clients include private equity funds, tax-exempt and institutional investors, financial industry leaders, certain public companies as well as high-net-worth individuals. He is a member of the Association de planification fiscale et financière, the Canadian Tax Foundation and the International Fiscal Association, Canadian branch.

MICHAEL A LEVY

Sidley Austin LLP

Michael Levy is a partner in Sidley Austin's New York office and a member of the firm's white collar: government litigation and investigations group. Mike's practice focuses on white collar criminal defence at the trial and appellate level, securities and commodities enforcement matters, and internal corporate investigations. Prior to joining Sidley, Mike spent 13 years as a federal prosecutor in the United States Attorney's Office for the Southern District of New York. During that time, Mike prosecuted cases in a variety of the US Attorney's Office's white collar units, including the Securities and Commodities Fraud Task Force, the Complex Frauds Unit and the Public Corruption Unit, before serving three years as that office's chief appellate attorney. Mike is a graduate of Harvard College and the University of Virginia School of Law.

GRAHAM LIM

Jones Day

Graham Lim's practice covers leveraged finance, debt capital markets and private equity investments. Graham is currently based in Hong Kong. He is qualified and previously practised in New York, London and Singapore.

PILAR LLUESMA RODRIGO

Uría Menéndez

Pilar Lluesma Rodrigo is counsel in Uría Menéndez's Madrid office. She began her career at Uría Menéndez in 1995 and rejoined the firm in 2018, having worked in the legal department of INVERCO from 2016 to 2017.

She has 20 years of experience advising a wide range of financial entities, including credit entities, investment services firms, collective investment schemes management companies, and private equity management companies, in regulatory and financial matters.

In particular, within the regulatory field, she advises on matters such as authorisations, cross-border provision of services, marketing of products, rules of conduct and transparency, disciplinary proceedings, reporting to supervisory authorities, anti-money laundering, derivatives and service client agreements.

DECLAN MCBRIDE

Arthur Cox

Declan McBride is a senior member of the financial regulation group. He advises a wide range of domestic and international financial institutions, including banks, investment firms, payment institutions, e-money firms, retail credit firms, credit servicers and money lenders. Declan's experience includes providing advice on authorisation requirements, anti-money laundering, payment services, Central Bank of Ireland investigations and compliance with conduct of business rules.

NADIA MANZARI

Schiltz & Schiltz SA

Nadia Manzari is a partner at Schiltz & Schiltz. Before joining the firm in 2018, Nadia was the head of the innovation, payments, markets infrastructures and governance department at the Financial Sector Supervisory Commission (CSSF), where she started her career in 2001.

She is a regular speaker at national and international conferences covering payment services, financial technologies, remuneration policies and corporate governance.

She graduated in law from Robert Schuman University in Strasbourg and holds a master's degree in business law as well as a postgraduate diploma of corporate counsel with a focus on German–French business law. She holds a certificate in corporate governance of INSEAD and is an ILA-certified director.

ARA MARGOSSIAN

Webb Henderson

Ara Margossian is a partner in Webb Henderson's telecoms, media and technology practice. He has been involved in some of the most high-profile corporate, commercial and regulatory projects in the TMT space. His practice has a strong focus on transactions that involve new or emerging technologies such as IOT/smart cities, big data, AI/machine learning, blockchain technologies and complex systems. Ara is recognised as a leading practitioner in *International Who's Who* 2017 (TMT), *Chambers Asia-Pacific* 2018, *The Legal 500* and *Best Lawyers*.

ALESSANDRA CAROLINA ROSSI MARTINS

Pinheiro Neto Advogados

Alessandra Carolina Rossi Martins is an associate in the corporate area of the Pinheiro Neto Advogados office in São Paulo. Her fields of expertise are banking and credit cards regulation, foreign exchange controls, fintech, financing, business law, investments, corporate law, M&A, capital markets and insurance regulation. Ms Martins graduated with an LLB from the São Paulo Catholic University in 2012. In addition, Ms Martins participated in an exchange programme at Université Paris 1 – Pantheón Sorbonne in 2010 and 2011. She was admitted to the Brazilian Bar Association in 2013.

PAMELA J MARTINSON

Sidley Austin LLP

Pamela Martinson is a partner in the global finance group at Sidley Austin LLP in Palo Alto, California. Her practice incorporates work on secured lending transactions for a broad range of lenders, including banks, investment funds, equipment leasing companies and marketplace lenders. She regularly advises clients on complex UCC issues in lending and securitisation transactions, and is a member of Sidley's opinion and UCC committees.

Pamela graduated from Harvard Law School in 1989, and also earned an MBA in finance from the University of Denver. She worked as a commercial lender with a bank prior to commencing her legal practice. She is active in the American Bar Association through its UCC Committee, the Equipment Leasing and Finance Association, and as vice president

of the American College of Commercial Finance Lawyers. She participated on the Drafting Committee of the Uniform Law Commission's work on a Model Act for the Regulation of Virtual Currency Businesses.

CHRISTOPHER MASTERSON

Sidley Austin LLP

Chris Masterson is an associate in the global finance group at Sidley Austin in the Palo Alto office. Mr Masterson represents major institutional lenders, borrowers and sponsors in a range of complex financing and lending transactions, including single-bank loans, syndicated facilities, acquisition finance, structured finance transactions and securitisations. He has particular experience in venture debt financing, cross-border lending matters, lending to technology and growth companies, marketplace lending and fintech-related matters. Mr Masterson has published, spoken and advised clients on a range of lending issues including the Uniform Commercial Code, structuring of cross-border loans, intellectual property as collateral, blockchain and fintech-related financing matters. Mr Masterson received his JD *cum laude* from the University of California, Hastings College of the Law and attended New York University's Leonard N Stern School of Business for his undergraduate studies, graduating *magna cum laude* with a BSc in economics and a BSc in finance.

MAURA MCLAUGHLIN

Arthur Cox

Maura McLaughlin advises international and domestic listed, public and private companies, as well as public sector bodies, on all aspects of company law and a wide range of commercial matters, as well as advising listed companies on compliance and governance issues. She has extensive experience of advising on public and private mergers and acquisitions, with particular emphasis on takeovers, schemes of arrangement and mergers. Maura has employed this experience to achieve clients' strategic objectives, notably in the design and implementation of structures permitting the inversion or migration of holding companies to Ireland. Equity capital markets work is another area of focus: Maura regularly advises on Irish securities laws, and has acted for companies, investors and underwriters on listings and fundraisings. Prior to joining the firm, Maura worked for Linklaters' London office.

DAVID A MILLER

Sidley Austin LLP

David Miller is an associate in the banking and financial services and government strategies groups at Sidley Austin LLP in Washington, DC. His practice focuses on providing regulatory, public policy and transactional advice to a variety of financial, payments and internet-based institutions, often at the intersection of technology and the financial industry. David graduated with a degree in political science and communications studies from the University of Michigan in 2010 and received his *juris* doctor from the University of Miami School of Law in 2014.

RITAM MITRA

Webb Henderson

Ritam Mitra is a commercial TMT lawyer who has worked extensively in advising on telecoms and technology projects, procurement and outsourcing, and a range of commercial transactions.

DAVID MOALEM

Bech-Bruun

David Moalem is an expert in capital markets, financial institutions, investment funds and managers, anti-money laundering and counter-terrorist finance, payment services and fintech.

David is also highly experienced in special procedural law and criminal law, having represented a number of listed companies and financial institutions in test cases before the Danish Financial Supervisory Authority, the Danish Company Appeals Board, the Danish Public Prosecutor for Serious Economic and International Crime, and the Danish courts.

JAMES MUNSELL

Sidley Austin LLP

Jim Munsell is a partner in Sidley's New York office. He counsels investment advisers and investment funds in connection with a broad range of corporate, securities, derivatives and regulatory matters. Jim's clients range from small, closely held start-up investment management businesses to the investment management divisions of global financial institutions. He was involved in the successful development and launch of the first commodity pool to be listed on a securities exchange in the United States and continues to work on innovative exchange-traded funds (ETFs).

Jim is part of Sidley's investment funds, advisers and derivatives practice team, which has won numerous top awards as a provider of legal services to the private funds industry: two-time winner of *Chambers and Partners'* 'Investment Funds Team of the Year for the U.S.'; Institutional Investor's Alpha magazine's 2014 Alpha Awards top 'onshore' (US) law firm serving the hedge fund industry; four-time recipient of first-tier national rankings in the *U.S. News – Best Lawyers* 'Best Law Firms' rankings for private funds and hedge funds law, and derivatives and futures law; and has been ranked in the top band for hedge funds by *Chambers USA* every year since 2008. Additionally, Jim is recognised in the 2013 to 2015 editions of *The International Who's Who* of private funds, and is recommended in *The Legal 500* for mutual and registered funds and private equity funds. He is also a winner of an ETF award, which highlights outstanding performances and results achieved by corporate leaders.

TAKESHI NAGASE

Anderson Mori & Tomotsune

Takeshi Nagase handles finance and corporate transactions, and has considerable experience advising on all legal aspects of public and private mergers and acquisitions, joint ventures, fintech, and other corporate and financial advisory matters. His clients range from prominent financial institutions to cryptoasset start-ups. Between 2013 and 2014, Takeshi served on secondment in the Disclosure Department of the Financial Services Agency of Japan, where he was an instrumental part of the team that revised the laws and guidelines governing

disclosure by listed companies, and prepared the Japanese Stewardship Code. Additionally, he handled a broad range of finance and corporate transactions on a secondment stint with the legal department of a major Japanese securities firm from 2015 to 2017. As a result of the unique perspective he has gained from these professional experiences, Takeshi is often sought for his advice on finance-related matters, particularly by clients seeking to evaluate transactions from the regulator's point of view. Recently, Takeshi has extended his focus to cryptoasset laws, including regulatory requirements applicable to registration of cryptoasset exchange service providers, initial coin offerings, and the like.

VAIBHAV PARIKH

Nishith Desai Associates

Vaibhav Parikh is the leader and head of the cryptocurrency and blockchain practice of the research and strategy-driven international law firm, Nishith Desai Associates. Vaibhav heads the US office of the firm. He also leads the technology, mergers and acquisitions, and private equity practice areas.

MAXIM PERVUNIN

TFH Russia LLC

Maxim Pervunin is a highly respected expert in complex international tax planning, corporate law, risk management and finance. Maxim is a barrister, as well as an expert in the Chamber of Commerce and Industry of the Russian Federation, and a member of the International Bar Association, the International Tax Planning Association and the Transnational Taxation Network. Since 2012, Maxim has been the managing director at TFH Russia. His sphere of competence sees him consulting large and medium-sized businesses; advising on international taxation of legal entities and individuals in more than 100 foreign jurisdictions; offering comprehensive international legal expertise; structuring and supporting international transactions; building international holding structures; and restructuring holdings. Maxim graduated from the Peoples' Friendship University of Russia as a lawyer; from Plekhanov, a Russian financial academy, as a master of business administration (MBA); and from a Swiss finance institute as a financial asset management engineer. He speaks fluent English and French.

MARTIN PICHLER

Brandl & Talos Rechtsanwälte GmbH

Martin Pichler is a senior associate at Brandl & Talos and specialises in capital markets, banking, securities and data protection law. Before joining Brandl & Talos in 2015, Martin was chief compliance officer at CCP.A, the central counterparty of the Vienna Stock Exchange.

Martin provides regulatory advice in the field of virtual and cryptocurrencies with a focus on data protection, banking and security supervision law.

Martin is a regular speaker at conferences and legal seminars and frequently publishes articles in various legal journals.

KRISTOFFER PROBST LARSEN

Bech-Bruun

Kristoffer Probst Larsen is an expert within capital markets law and financial regulation. Kristoffer particularly advises investment firms, listed companies, asset managers, credit institutions and payment services providers regarding the Danish transposition of MiFID II, CRD IV, MAR, AMLD IV, AIFMD, PSD2 and UCITS V.

ARVIND RAVINDRANATH

Nishith Desai Associates

Arvind Ravindranath is a technology lawyer and a member of the cryptocurrency and blockchain practice at Nishith Desai Associates. He has spoken at academic institutions and has been quoted several times on the subject. He is based in the firm's Mumbai, BKC Office and is qualified to practise in India.

JAIDEEP REDDY

Nishith Desai Associates

Jaideep Reddy is a technology lawyer and a senior member of the cryptocurrency and blockchain practice of Nishith Desai Associates. He advises leading businesses in this industry and has also published widely on the subject. He is based in the firm's Bengaluru office and is admitted to practise in India and California, United States.

VERITY A VAN TASSEL RICHARDS

Sidley Austin LLP

Verity A Van Tassel Richards focuses her practice on representing digital asset trading platforms, blockchain technology companies, US and non-US broker-dealers, financial services firms and cryptocurrency funds. Verity is a frequent speaker and writer on various topics in fintech, with a particular focus on distributed ledger technology and blockchain tokens.

TIAGO MOREIRA VIEIRA ROCHA

Pinheiro Neto Advogados

Tiago Moreira Vieira Rocha is a senior associate in the tax area of the Pinheiro Neto Advogados office in São Paulo. His fields of expertise are direct taxes, corporate reorganisations, M&A transactions, and taxation of the banking system and of the financial and capital markets. Mr Rocha graduated with an LLB from the São Paulo Catholic University in 2007, and holds an MBA degree from the Getúlio Vargas Foundation.

NICLAS ROCKBORN

Gernandt & Danielsson Advokatbyrå

Niclas Rockborn has been a partner at Gernandt & Danielsson since 2005. He has over 20 years' experience advising in relation to the regulation of financial institutions. He has extensive experience advising in the banking and insurance, and asset management sectors, and advising insurance firms and other financial institutions. He advises on, inter alia, new licences, new products and services, sanctions and investigations, money laundering issues

and other day-to-day matters. He also has a particularly strong practice in the fintech and payments sector. Niclas advises on matters relating to developing rules and regulations, including PSD, GDPR, AIFMD, UCITS, MiFID and CRD.

ALEX R ROVIRA

Sidley Austin LLP

Alex R Rovira is a partner in Sidley's restructuring practice group in New York, and has also spent close to three years in each of Sidley's London and Hong Kong offices, representing both debtors' and creditors' rights on various aspects of corporate restructuring and workouts, creditors' rights, bankruptcy and insolvency matters in the US, UK, Asia-Pacific and the Cayman Islands. He also has significant experience advising and representing clients on broker-dealer and bank liquidation proceedings. Alex also advises on the structuring of and unwinding of complex financing transactions such as real estate financing, securitisations, repurchase agreements, security lending arrangements, swaps, forwards and other derivative agreements, sale-lease back transactions with a focus on insolvency risks, enforcement and remedies. Alex received his bachelor of arts in economics from Harvard University and his doctorate of jurisprudence from Georgetown University Law Center, and was trained in a full year course on English corporate insolvency law at the University College of London in their LLM programme.

PEARSE RYAN

Arthur Cox

Pearse Ryan is a consultant in the technology and innovation group, and a member of the firm's cross-departmental fintech group and cybersecurity group. He specialises in the following areas: digital transformation and cloud computing; commercialisation of technology innovation and technology-related IPR; computer security and fraud; cyber insurance; e-commerce; and fintech. Pearse sits on the steering group of Blockchain Ireland, as well as chairing its legal advisory group. He is also a member of the new Lex Mundi blockchain group. Pearse is a frequent writer and speaker on fintech and cybersecurity topics. This includes recurring speaking slots with the Incorporated Law Society of Ireland (PPCII and diploma courses) and the Honorable Society of King's Inns (advanced diploma in white collar crime). Pearse was a part-time lecturer in 2017 and 2018 on the National College of Ireland new MSC in fintech.

MICHAEL S SACKHEIM

Sidley Austin LLP

Michael S Sackheim is senior counsel in Sidley's New York office in the securities and derivatives enforcement and regulation group. Michael is a former assistant district attorney in Manhattan and senior trial attorney for the US Commodity Futures Trading Commission (CFTC). His practice concentrates on commodities and derivatives regulation and enforcement, with a focus on matters involving the CFTC and the National Futures Association. Michael is a former chair of the New York City Bar's Derivatives Regulation Committee and the American Bar Association Business Section's International Securities Regulation Subcommittee. He is the managing editor of the *Futures and Derivatives Law Report*, and a frequent author and lecturer on legal ethics for financial industry lawyers.

BERNICE SALIBA

GTG Advocates

Dr Bernice Saliba joined GTG Advocates in 2018 as a junior associate following a three-month stint in Luxembourg working for the European Commission as a Bluebook trainee with DG Connect.

After graduating with a Doctor of Laws from the University of Malta in 2017, Bernice was admitted to the Maltese Bar in 2018. Her Doctor of Laws thesis discussed issues of national security and law enforcement in comparison to matters of privacy arising out of the global discussion on the possibility of mandating backdoors into encrypted software and hardware.

Dr Saliba's main areas of practice with the firm concern distributed ledger technologies, cryptocurrencies and intellectual property law.

Bernice is proficient in Maltese and English and has a working knowledge of French and Italian.

TATIANA SANGADZHIEVA

TFH Russia LLC

Tatiana Sangadzhieva is a lawyer with more than four years of experience, and a master of law. In 2014, Tatiana graduated with honours from the international management department of the Moscow State Institute of International Relations (MGIMO University). Tatiana joined TFH Russia LLC in 2018. Her principal sphere of work and practice focus on civil, corporate and tax law, including international taxation of legal entities in foreign jurisdictions, structuring and supporting international transactions, and building international holding structures, although she also has experience in Russian administrative, land and labour law. Before joining TFH Russia, Tatiana worked for a tax consulting company as well for a leading Russian fashion industry group of companies. She speaks fluent English and German, and also teaches legal English to practising lawyers.

JEAN-LOUIS SCHILTZ

Schiltz & Schiltz SA

Jean-Louis Schiltz is the senior partner at Schiltz & Schiltz and a professor (Hon) at the University of Luxembourg.

Jean-Louis Schiltz is a regular speaker at tech law and innovation conferences, and has authored and co-authored a number of articles and reports in the field over the past few years.

He serves as a member for a number of companies and non-profit organisations. From 2004 to 2009, he served as a Cabinet Minister in Luxembourg. His portfolio included media, telecommunications, technology, international development and defence.

Jean-Louis joined the firm in 1989 and was admitted to the Luxembourg Bar the same year. He holds a postgraduate degree (DEA) in business law from the University of Paris I, Panthéon-Sorbonne. He taught at his alma mater in the early 1990s.

ANIL SHERGILL

Allen & Gledhill LLP

Anil Shergill is a senior associate in the financial services department and regularly advises on a wide range of fintech and financial regulatory and compliance matters affecting financial institutions and potential entrants into the financial services industry.

Anil has a keen interest in the fintech space, and has advised several fintech players, including technology companies, utility token issuers and banks, on their business models, spanning issues relating to online money transfer systems, online payment systems, stored value facilities, online lending platforms, digital payment token platforms and various initial coin offering structures. He has also been involved in policy formation initiatives and presentations to industry players.

Anil graduated from the National University of Singapore with an LLB (Hons) degree in 2015 and was called to the Singapore Bar in 2016.

DANIELLA SKOTNICKI

Harneys

Daniella Skotnicki is a partner in Harneys' Cayman Islands office. She advises blockchain, fintech and financial services clients on structuring, fundraising and regulatory matters, as well as providing advice regarding mergers and acquisitions, private placements, restructurings and joint ventures.

Prior to joining the firm in 2017, Daniella was counsel at Ogier, and practised with Cox Hallett Wilkinson in Bermuda and King & Wood Mallesons in Australia. Daniella has also served as in-house legal counsel at an administrator in the Cayman Islands.

Daniella is a chartered alternative investment analyst.

SEAN A SMITH

Sidley Austin LLP

Sean A Smith is an associate in the banking and financial services group at Sidley Austin in Washington, DC. He represents a broad range of financial services providers on regulatory and transactional matters. A significant part of his practice entails representing and advising money transmitters, including those considering engaging in virtual currency activities. Prior to working at Sidley Austin, Sean was an assistant vice president at US Bank and an assistant attorney general at the Missouri Attorney General's Office in the Consumer Protection Division.

DAVID E TEITELBAUM

Sidley Austin LLP

David E Teitelbaum is a partner in the banking and financial services group of Sidley Austin LLP. He has a broad regulatory practice for all types of entities involved in our payments and financial systems, including insured depository institutions and their holding companies, payment processors and systems, money transmitters, technology providers, virtual currency businesses and investors. David has been involved in the evolution of payment technology from its roots in credit, debit and ACH through ongoing developments in prepaid, internet, mobile and virtual currency models. He has assisted clients in projects involving blockchain-based technologies both as a form of payment and as an asset class for investment, including in connection with virtual currency brokerage, exchange, trading and investment, and has assisted clients in obtaining state licences when warranted. David is a member of the editorial board of *FinTech Law Report*, and his publications include articles in *The Journal of Payments Strategy & Systems* and *The Business Lawyer* as well as co-authorship of *The Community Reinvestment Act: Policies and Compliance* (Prentice-Hall Law and Business),

the US chapter of the International Monetary Fund book, *Payment Systems of the World*, and contributions to *The Law of Electronic Fund Transfers* (Warren, Gorham & Lamont). David has been named a 'Leading Lawyer' in *Chambers USA*, and was selected as one of Law360's 'Retail & E-Commerce MVPs' of the year for 2017. David graduated from the Stanford Law School in 1986 as a member of the Order of the Coif, and clerked for William A Norris, US Court of Appeals, 9th Circuit, during the 1986–1987 term.

KENNY TERRERO

Sidley Austin LLP

Kenny Terrero is a corporate counsel in the investment funds, advisers and derivatives practice group of Sidley Austin LLP in New York. He is also a member of the firm's fintech group, and has broad experience with investment vehicles that invest in digital assets and their derivatives. He works with both private and public fund sponsors of funds investing in digital assets, and also works with not-for-profit entities involved in initiatives in the digital asset space. He is a frequent speaker and writer on the topics of blockchain and digital assets, and has been a member of the Bitcoin Foundation since 2013. Kenny graduated from Brooklyn Law School in 2006, where he was an international business law fellow.

LILYA TESSLER

Sidley Austin LLP

Lilya Tessler is a partner and the New York head of Sidley's fintech and blockchain group. She focuses her practice on representing digital asset trading platforms, blockchain technology companies, US and non-US broker-dealers, financial services firms and cryptocurrency funds. Lilya advises technology companies on blockchain token offerings, including so-called ICOs. She also counsels financial institutions and digital asset exchanges with day-to-day securities issues, private placement agent requirements, custody rule requirements, cross-border regulatory issues, money services business registration requirements, as well as FINRA and SEC regulatory inquiries. She advises several US and non-US fintech companies, including robo-advisers and high-frequency trading firms in evaluating the broker-dealer and investment adviser registration requirements. Lilya works with transactional lawyers on structuring deals involving financial services and technology companies, digital asset exchanges and blockchain token offerings. She regularly assists both financial services firms and their vendors in negotiating US and cross-border technology agreements for all types of services and considering the US securities laws and broker-dealer regulatory issues associated with such technologies.

MICHIEL VAN ROEY

MVR Legal BV

MVR Legal BV, represented by Michiel Van Roey, is a Belgian limited liability company providing legal services. Michiel Van Roey has been a member of the Brussels Bar and was an associate in Stibbe's intellectual property and technology, media and telecommunication practice for six years before starting his independent legal consultancy firm. Michiel holds an LLM from the University of Virginia School of Law (class of 2013) and is a research assistant at the University of Antwerp. Michiel has experience with patent, trademark, copyright and design infringement cases (on a national, regional and international level) as well as

general commercial litigation cases. He advises corporate clients and start-ups on intellectual property, data protection and information technology matters. Michiel has substantial expertise in negotiating and drafting a wide variety of IP-related agreements and gained specific knowledge on technology licensing working as a legal adviser for the Knowledge Transfer Group at the European Organization for Nuclear Research (Geneva, CH). He has a special interest in blockchain technology and cryptocurrencies and has published several articles on the topic. Michiel, representing MVR Legal BV, is currently active as the general counsel, data protection and ICO legal adviser for Profila GmbH, a Swiss start-up in the field of data protection and privacy rights management, as well as the external corporate legal counsel for Cisco Belux.

HUBERT DE VAUPLANE

Kramer Levin Naftalis & Frankel LLP

Hubert de Vauplane co-leads the alternative investment management practice in the Paris office, offering a global and integrated vision on regulatory and transactional structuring and operations matters. Hubert advises on EU and French laws on banking and investment services regulatory matters, asset management and funds, insurance investment regulations, and financial/securities litigations, e-money and payment services, and financial institution mergers and acquisitions. He provides legal counsel on fintech, blockchain and cryptocurrency assets, and financial regulatory issues relating to investment advice, asset management, payment services and banking.

Hubert also advises corporates, asset managers, corporate and investment banks and institutional investors in relation to the entire range of desintermediated financings, including the structuring and setting-up of debt funds (AIFM, ELTIF, FPE) under French or Luxembourg law, factoring programmes of trade receivables (French or pan-European), and the issuance of private bonds and hybrid debt instruments (EuroPP, USPP, *bons de caisse*).

CHRISTIAN VIEIRA

Stikeman Elliott LLP

Christian Vieira is an associate in Stikeman Elliott's corporate group. His practice focuses on securities, mergers and acquisitions, corporate finance and banking as well as general corporate and commercial law. Christian's practice extends to securities regulatory matters relating to the issuance and trading of cryptocurrencies.

KLAUS HENRIK WIESE-HANSEN

Schjødt

Klaus Henrik is a partner at Schjødtand specialises in financial markets legislation, insurance, pensions and asset management. He advises domestic and international insurers, insurance intermediaries, asset managers, investment banks, credit institutions and financial holding companies.

He litigates regularly before the Norwegian courts and is admitted to the Supreme Court.

He has authored a number of books and articles regarding asset management, insurance, pensions, banking and financial regulatory matters.

Klaus Henrik is ranked among Norway's leading lawyers regarding financial regulatory, insurance and reinsurance and pensions matter, including by *The Legal 500*, the *IFLR1000*

and *PLC Which Lawyer?*, and is praised as a 'standout practitioner' and 'regulatory expert'. He has been continuously ranked among Norway's top 10 insurance lawyers since 2013, and was ranked the No. 1 insurance lawyer in Norway by his peers in the 2017 Norwegian Financial Daily lawyers survey. He has been the chair of the control committee in a life insurance company, and holds positions as the chair and a member of the boards of various commercial and financial companies.

TOBIAS WOHLFARTH

Hengeler Mueller Partnerschaft von Rechtsanwälten mbB

Tobias Wohlfarth, Dr iur, is an associate at Hengeler Mueller's Frankfurt office and part of the banking and finance group. He joined the firm in 2017 and advises and represents banks, investment firms, asset managers, insurance companies and benchmark providers. His practice focuses on financial regulation, capital markets and corporate law with a particular focus on alternative investments and fintech business models.

Tobias studied at the Universities of Freiburg, Grenoble (France) and Bonn. He received a PhD from the University of Tübingen for a law and economics thesis on regulatory requirements for hedge fund and private equity compensation structures under the EU Alternative Investment Fund Managers Directive. He has worked as a research and teaching assistant at the University of Bonn, with the German Consulate General in Ho Chi Minh City (Vietnam) and with the European Securities and Markets Authority (ESMA) in Paris. Most recently, Tobias was an expert member of a working group of the Association of German Banks, which developed reform proposals for enabling and implementing securities transactions using DLT.

ALEXANDER YAP

Allen & Gledhill LLP

Alexander Yap is a partner in the corporate and commercial department, and is co-head of the firm's fintech practice.

Alexander often advises on internet banking, online trading, electronic contracting, electronic document retention, cybersecurity and various innovations in the delivery of financial and insurance services, including preparing related user and service agreements for Singapore or global roll-outs. A contact partner and specialist on the Personal Data Protection Act 2012 (PDPA) issues, he regularly directs client's PDPA, data protection and privacy compliance activities, and advises on data breaches.

Alexander is recognised in *Who's Who Legal: Banking 2019*, in the fintech analysis, as a leading individual in the Asia-Pacific. *Who's Who Legal* notes that he is 'a highly endorsed fintech specialist who boasts extensive experience advising on a range of matters including internet banking and online trading', with a source effusing that 'Alexander not only possesses a sharp intellect but also the ability to convey and communicate legal intricacies in simple terms'. He is 'identified for his "ability to negotiate outcomes for parties", as well as his "strong skills in the tech space"'.

SAMUEL YIM

Kim & Chang

Samuel Yim is a senior foreign attorney at Kim & Chang's e-finance and fintech practice where he focuses on blockchain and cryptocurrency matters. He regularly represents token

sellers, cryptocurrency exchanges, ventures, hedge and private equity funds and their portfolio companies, token marketers and broker-dealers, funds interested in trading digital assets, global investment banks, financial institutions and asset managers, and others in the space. He has advised foreign and domestic clients on major industry-defining matters, such as initial coin offerings (ICOs) and reverse ICOs, token private placements, the establishment or acquisition of cryptocurrency exchanges, cryptocurrency arbitrage and the establishment of cryptocurrency not-for-profit foundations.

Prior to joining Kim & Chang, Mr Yim worked at Allen & Overy LLP and served in the US Army. Mr Yim received a BS from the United States Military Academy (West Point) and a JD/MA from Georgetown University Law Center and the Paul H Nitze School of Advanced International Studies, Johns Hopkins University. He received the Fulbright Fellowship and studied at Yonsei University in Seoul, Korea. Mr Yim was also an adjunct professor at Yonsei University Law School and was a term member on the Council on Foreign Relations. He is admitted to the New York Bar.

SHARON YIU

Jones Day

Sharon Yiu has been supporting various practices of the firm including the banking, finance and securities, the cybersecurity, privacy and data protection, and the intellectual property practices. Prior to joining Jones Day, Sharon has worked in the Hong Kong office of a global technology company.

ULVIA ZEYNALOVA-BOCKIN

Dentons

Ulvia Zeynalova-Bockin is counsel in the Dentons' Baku office. Her practice includes banking law, Islamic finance, real estate finance, mergers and acquisitions, as well as corporate law and finance. Ulvia also has experience in securities and financial regulation, including work with the Corporation Finance Division of the US Securities and Exchange Commission in Washington, DC, and advising clients with business interests in the CIS countries and South East Asia while working in Salans' New York office and, more recently, at Dentons Rodyk in Singapore.

She has provided legal support to local and international clientele in high-profile matters, including the first inital public offering to be listed on the Baku Stock Exchange, the first Azerbaijani law-governed syndicated loan facility and the second-largest recapitalisation and restructuring in the history of the Azerbaijani financial sector, advising major investment banks on the enforceability of ISDA master agreements, global master repurchase agreements and global master securities lending agreements, and participating in the privatisation of the largest bank in Azerbaijan.

Ms Zeynalova-Bockin qualified to practise in Azerbaijan in March 2006 and was admitted to the New York State Bar in January 2010. She is a registered foreign lawyer in Singapore as of September 2017.

She has been ranked as a 'Next Generation Lawyer' by *The Legal 500 EMEA* in the 2017, 2018 and 2019 editions, as a 'Recognised Practitioner' by *Chambers Asia-Pacific* in 2018 and *Chambers Global* in 2019, and a 'Rising Star' by *IFRL1000* in 2019.

Appendix 2

CONTRIBUTORS' CONTACT DETAILS

ALLEN & GLEDHILL LLP

One Marina Boulevard #28-00
Singapore 018989
adrian.ang@allenandgledhill.com
alexander.yap@allenandgledhill.com
anilraj.s@allenandgledhill.com
samuel.kwek@allenandgledhill.com
Tel: +65 6890 7710/7627/7474/7472
Fax: +65 6302 3194/3049/3435/3444
www.allenandgledhill.com

AMERELLER

One by Omniyat, #1402 Business Bay
PO Box 97706
Dubai
United Arab Emirates
Tel: +971 4 432 3671
Fax: +971 4 432 3673
gunson@amereller.com

Kurfürstenhöfe, Spreeufer 5
10178 Berlin
Germany
Tel: +49 30 609 895 660
Fax: +49 30 609 895 669

elrifai@amereller.com
www.amereller.com

ANDERSON MORI & TOMOTSUNE

Otemachi Park Building, 1-1-1 Otemachi
Chiyoda-ku
Tokyo 100-8136
Japan
Tel: +81 3 6775 1000
ken.kawai@amt-law.com
takeshi.nagase@amt-law.com
www.amt-law.com

ARTHUR COX

Ten Earlsfort Terrace
Dublin D02 T380
Ireland
Tel: +353 1 920 1000
maura.mclaughlin@arthurcox.com
pearse.ryan@arthurcox.com
caroline.devlin@arthurcox.com
declan.mcbride@arthurcox.com
www.arthurcox.com

BECH-BRUUN

Langelinie Allé 35
2100 Copenhagen
Denmark
Tel: +45 7227 0000
Fax: +45 7227 0027
dmm@bechbruun.com
kpl@bechbruun.com
www.bechbruun.com

BRANDL & TALOS RECHTSANWÄLTE GMBH

Mariahilfer Strasse 116
1070 Vienna
Austria
Tel: +43 1 522 57 00
Fax: +43 1 522 57 01
aquilina@btp.at
m.pichler@btp.at
www.btp.at

CLIFFORD CHANCE LLP

10 Upper Bank Street
London E14 5JJ
United Kingdom
Tel: +44 20 7006 1000
Fax: +44 20 7006 5555
peter.chapman@cliffordchance.com
laura.douglas@cliffordchance.com
www.cliffordchance.com

DENTONS

8 Izmir Street
Hyatt International Center
Hyatt Tower 2
Baku, 1065
Azerbaijan
Tel: +994 12 4 90 75 65
Fax: +994 12 4 97 10 57
ulvia.zeynalova-bockin@dentons.com
www.dentons.com

GERNANDT & DANIELSSON ADVOKATBYRÅ

Hamngatan 2
111 47 Stockholm
Sweden
Tel: +46 8 670 66 00
Fax: +46 8 662 61 01
niclas.rockborn@gda.se
www.gda.se

GTG ADVOCATES

66, Old Bakery Street
Valletta VLT 1454
Malta
Tel: +356 2124 2713
igauci@gtgadvocates.com
cabelagrech@gtgadvocates.com
tcassar@gtgadvocates.com
bsaliba@gtgadvocates.com
www.gtgadvocates.com

HARNEYS

4th Floor, Harbour Place
103 South Church Street
PO Box 10240
KY1-1002 Grand Cayman
Cayman Islands
Tel: +1 345 949 8599
Fax: +1 345 949 4451
daniella.skotnicki@harneys.com
www.harneys.com

HENGELER MUELLER PARTNERSCHAFT VON RECHTSANWÄLTEN MBB

Behrenstrasse 42
10117 Berlin
Germany
Tel: +49 30 20374 193
Fax: +49 30 20374 333
matthias.berberich@hengeler.com

Bockenheimer Landstrasse 24
60323 Frankfurt
Germany
Tel: +49 69 17095 266
Fax: +49 69 17095 099
tobias.wohlfarth@hengeler.com

www.hengeler.com

JONES DAY

31st Floor, Edinburgh Tower
The Landmark
15 Queen's Road Central
Hong Kong
Tel: +852 2526 6895
Fax: +852 2868 5871
glim@jonesday.com
syiu@jonesday.com
www.jonesday.com

KIM & CHANG

39, Sajik-ro 8-gil
Jongno-gu
Seoul 03170
Korea
Tel: +82 2 3703 1114
Fax: +82 2 737 9091/9092
jungmin.lee@kimchang.com
joonyoung.kim@kimchang.com
samuel.yim@kimchang.com
www.kimchang.com

KRAMER LEVIN NAFTALIS & FRANKEL LLP

47 avenue Hoche
75008 Paris
France
Tel: +33 1 44 09 46 00
Fax: +33 1 44 09 46 01
hdevauplane@kramerlevin.com
vcharpiat@kramerlevin.com
www.kramerlevin.com

MARVAL, O'FARRELL & MAIRAL

Av Leandro N Alem 882
C1001AAQ Buenos Aires
Argentina
Tel: +54 11 4310 0100
Fax: +54 11 4310 0200
jd@marval.com
www.marval.com

MVR LEGAL BV

Avenue de Roodebeek 213 (1)
1030 Brussels
Belgium
Tel: +32 496 05 73 48
michiel.vanroey@gmail.com
michiel@profila.com
mvanroey@cisco.com
louis-bidaine@hotmail.com

NISHITH DESAI ASSOCIATES

3, North Avenue
2nd Floor, Maker Maxity
Bandra-Kurla Complex
Mumbai 400 051
India
Tel: +91 22 6159 5000
arvind.r@nishithdesai.com

Prestige Loka
G01, 7/1 Brunton Rd
Bangalore 560 025
India
Tel: +91 80 6693 5000
jaideep.reddy@nishithdesai.com

375 Park Avenue, Suite 2607
Seagram Building
New York, NY 10152
United States
Tel: +1 917 821 6301
vaibhav.parikh@nishithdesai.com

www.nishithdesai.com

PINHEIRO NETO ADVOGADOS

Rua Hungria, 1100
01455-906 São Paulo
Brazil
Tel: +55 11 3247 8400/8839/6364/
6160/6244
Fax: +55 11 3247 8600
fgomes@pn.com.br
tvieira@pn.com.br
acmartins@pn.com.br
bcorrea@pn.com.br
www.pinheironeto.com.br

RUSSELL MCVEAGH

Level 30, Vero Centre
48 Shortland Street
PO Box 8
Auckland 1140
New Zealand
Tel: +64 9 367 8000
Fax: +64 9 367 8163
deemple.budhia@russellmcveagh.com
tom.hunt@russellmcveagh.com
www.russellmcveagh.com

SCHELLENBERG WITTMER LTD

15bis, rue des Alpes
PO Box 2088
1211 Geneva 1
Switzerland
Tel: +41 22 707 8000
Fax: +41 22 707 8001
geneva@swlegal.ch
tarek.houdrouge@swlegal.ch

Löwenstrasse 19
PO Box 2201
8021 Zurich
Switzerland
Tel: +41 44 215 5252
Fax: +41 44 215 5200
zurich@swlegal.ch
olivier.favre@swlegal.ch
fabio.elsener@swlegla.ch

www.swlegal.ch

SCHILTZ & SCHILTZ SA

24–26, avenue de la Gare
1610 Luxembourg
Tel: +352 45 64 80
Fax: +352 45 64 44
jeanlouis.schiltz@schiltz.lu
nadia.manzari@schiltz.lu
www.schiltz.lu

SCHJØDT

Ruseløkkveien 14
PO Box 2444 Solli
0201 Oslo
Norway
Tel: +47 22 01 88 00
kwh@schjodt.no
vefi@schjodt.no
www.schjodt.no

SIDLEY AUSTIN LLP

1001 Page Mill Road Building 1
Palo Alto, California 94304
United States
Tel: +1 650 565 7000
pmartinson@sidley.com
cmasterson@sidley.com

One South Dearborn Street
Chicago, Illinois 60603
United States
Tel: +1 312 853 7000
nhowell@sidley.com
jbiery@sidley.com
tharmon@sidley.com
dapplebaum@sidley.com

787 Seventh Avenue
New York, New York 10019
United States
Tel: +1 212 839 5300
msackheim@sidley.com
jmunsell@sidley.com
mlevy@sidley.com
david.miller@sidley.com
dgallego@sidley.com
arovira@sidley.com
kterrero@sidley.com
ltessler@sidley.com
dengoren@sidley.com
vvantasselrichards@sidley.com
ibell@sidley.com

1501 K Street, NW #600
Washington, District of Columbia 20005
United States
Tel: +1 202 736 8000
garonow@sidley.com
dteitelbaum@sidley.com
ablake@sidley.com
sean.smith@sidley.com

www.sidley.com

STIKEMAN ELLIOTT LLP

5300 Commerce Court West
199 Bay Street
Toronto, Ontario M5L 1B9
Canada
Tel: +1 416 869 5500 /
Toll-free: +1 877 973 5500
Fax: +1 416 947 0866
adanglejan@stikeman.com
rgrewal@stikeman.com
erlevesque@stikeman.com
cvieira@stikeman.com
www.stikeman.com

TFH RUSSIA LLC

Presnenskaya naberezhnaya, bld 8-1
MFC Capital City
IBC Moscow City
Moscow 123317
Russia
Tel: +7 499 286 00 10
Fax: +7 499 286 00 10
pma@tfh-uk.com
ts@tfh-uk.com
www.tfh-uk.com

URÍA MENÉNDEZ

Uría Menéndez-Proença de Carvalho
Praça Marquês de Pombal, 12
1250-162 Lisbon
Portugal
Tel: +351 21 030 86 00
Fax: +351 21 030 86 01
helder.frias@uria.com
luis.alvesdias@uria.com

Uría Menéndez
Calle del Príncipe de Vergara, 187
Plaza de Rodrigo Uría
28002 Madrid
Spain
Tel: +34 915 860 400
pilar.lluesma@uria.com
alberto.gil@uria.com

www.uria.com

WEBB HENDERSON

Level 18, 420 George Street
Sydney NSW 2000
Australia
Tel: +61 2 8214 3500
ara.margossian@webbhenderson.com
marcus.bagnall@webbhenderson.com
ritam.mitra@webbhenderson.com
irene.halforty@webbhenderson.com
www.webbhenderson.com

THE LAW REVIEWS

For more information, please contact info@thelawreviews.co.uk

THE ACQUISITION AND LEVERAGED FINANCE REVIEW
Marc Hanrahan
Milbank Tweed Hadley & McCloy LLP

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW
Mark F Mendelsohn
Paul, Weiss, Rifkind, Wharton & Garrison LLP

THE ASSET MANAGEMENT REVIEW
Paul Dickson
Slaughter and May

THE ASSET TRACING AND RECOVERY REVIEW
Robert Hunter
Edmonds Marshall McMahon Ltd

THE AVIATION LAW REVIEW
Sean Gates
Gates Aviation LLP

THE BANKING LITIGATION LAW REVIEW
Christa Band
Linklaters LLP

THE BANKING REGULATION REVIEW
Jan Putnis
Slaughter and May

THE CARTELS AND LENIENCY REVIEW
John Buretta and John Terzaken
Cravath Swaine & Moore LLP and Simpson Thacher & Bartlett LLP

THE CLASS ACTIONS LAW REVIEW
Camilla Sanger
Slaughter and May

THE COMPLEX COMMERCIAL LITIGATION LAW REVIEW
Steven M Bierman
Sidley Austin LLP

THE CONSUMER FINANCE LAW REVIEW
Rick Fischer, Obrea Poindexter and Jeremy Mandell
Morrison & Foerster

THE CORPORATE GOVERNANCE REVIEW
Willem J L Calkoen
NautaDutilh

THE CORPORATE IMMIGRATION REVIEW
Chris Magrath
Magrath LLP

THE CORPORATE TAX PLANNING LAW REVIEW
Jodi J Schwartz and Swift S O Edgar
Wachtell, Lipton, Rosen & Katz

THE DISPUTE RESOLUTION REVIEW
Damian Taylor
Slaughter and May

THE DOMINANCE AND MONOPOLIES REVIEW
Maurits J F M Dolmans and Henry Mostyn
Cleary Gottlieb Steen & Hamilton LLP

THE E-DISCOVERY AND INFORMATION GOVERNANCE LAW REVIEW
Tess Blair
Morgan, Lewis & Bockius LLP

THE EMPLOYMENT LAW REVIEW
Erika C Collins
Proskauer Rose LLP

THE ENERGY REGULATION AND MARKETS REVIEW
David L Schwartz
Latham & Watkins

THE ENVIRONMENT AND CLIMATE CHANGE LAW REVIEW
Theodore L Garrett
Covington & Burling LLP

THE EXECUTIVE REMUNERATION REVIEW
Arthur Kohn and Janet Cooper
Cleary Gottlieb Steen & Hamilton LLP and Tapestry Compliance

THE FINANCIAL TECHNOLOGY LAW REVIEW
Thomas A Frick
Niederer Kraft Frey

THE FOREIGN INVESTMENT REGULATION REVIEW
Calvin S Goldman QC
Goodmans LLP

THE FRANCHISE LAW REVIEW
Mark Abell
Bird & Bird LLP

THE GAMBLING LAW REVIEW
Carl Rohsler
Memery Crystal

THE GLOBAL DAMAGES REVIEW
Errol Soriano
Duff & Phelps

THE GOVERNMENT PROCUREMENT REVIEW
Jonathan Davey and Amy Gatenby
Addleshaw Goddard LLP

THE HEALTHCARE LAW REVIEW
Sarah Ellson
Fieldfisher LLP

THE INITIAL PUBLIC OFFERINGS LAW REVIEW
David J Goldschmidt
Skadden, Arps, Slate, Meagher & Flom LLP

THE INSOLVENCY REVIEW
Donald S Bernstein
Davis Polk & Wardwell LLP

THE INSURANCE AND REINSURANCE LAW REVIEW
Peter Rogan
Ince & Co

THE INSURANCE DISPUTES LAW REVIEW
Joanna Page
Allen & Overy LLP

THE INTELLECTUAL PROPERTY AND ANTITRUST REVIEW
Thomas Vinje
Clifford Chance LLP

THE INTELLECTUAL PROPERTY REVIEW
Dominick A Conde
Fitzpatrick, Cella, Harper & Scinto

THE INTERNATIONAL ARBITRATION REVIEW
James H Carter
Wilmer Cutler Pickering Hale and Dorr

THE INTERNATIONAL CAPITAL MARKETS REVIEW
Jeffrey Golden
P.R.I.M.E. Finance Foundation

THE INTERNATIONAL INVESTIGATIONS REVIEW
Nicolas Bourtin
Sullivan & Cromwell LLP

THE INTERNATIONAL TRADE LAW REVIEW
Folkert Graafsma and Joris Cornelis
Vermulst Verhaeghe Graafsma & Bronckers (VVGB)

THE INVESTMENT TREATY ARBITRATION REVIEW
Barton Legum
Dentons

THE INWARD INVESTMENT AND INTERNATIONAL TAXATION REVIEW
Tim Sanders
Skadden, Arps, Slate, Meagher & Flom LLP

THE ISLAMIC FINANCE AND MARKETS LAW REVIEW
John Dewar and Munib Hussain
Milbank Tweed Hadley & McCloy LLP

THE LABOUR AND EMPLOYMENT DISPUTES REVIEW
Nicholas Robertson
Mayer Brown

THE LENDING AND SECURED FINANCE REVIEW
Azadeh Nassiri
Slaughter and May

THE LIFE SCIENCES LAW REVIEW
Richard Kingham
Covington & Burling LLP

THE MERGER CONTROL REVIEW
Ilene Knable Gotts
Wachtell, Lipton, Rosen & Katz

THE MERGERS AND ACQUISITIONS REVIEW
Mark Zerdin
Slaughter and May

THE MINING LAW REVIEW
Erik Richer La Flèche
Stikeman Elliott LLP

THE OIL AND GAS LAW REVIEW
Christopher B Strong
Vinson & Elkins LLP

THE PATENT LITIGATION LAW REVIEW
Trevor Cook
WilmerHale

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW
Alan Charles Raul
Sidley Austin LLP

THE PRIVATE COMPETITION ENFORCEMENT REVIEW
Ilene Knable Gotts
Wachtell, Lipton, Rosen & Katz

THE PRIVATE EQUITY REVIEW
Stephen L Ritchie
Kirkland & Ellis LLP

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW
John Riches
RMW Law LLP

THE PRODUCT REGULATION AND LIABILITY REVIEW
Chilton Davis Varner and Madison Kitchens
King & Spalding LLP

THE PROFESSIONAL NEGLIGENCE LAW REVIEW
Nicholas Bird
Reynolds Porter Chamberlain LLP

THE PROJECT FINANCE LAW REVIEW
David F Asmus
Sidley Austin LLP

THE PROJECTS AND CONSTRUCTION REVIEW
Júlio César Bueno
Pinheiro Neto Advogados

THE PUBLIC COMPETITION ENFORCEMENT REVIEW
Aidan Synnott
Paul, Weiss, Rifkind, Wharton & Garrison LLP

THE PUBLIC-PRIVATE PARTNERSHIP LAW REVIEW
Bruno Werneck and Mário Saadi
Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados

THE REAL ESTATE INVESTMENT STRUCTURE TAXATION REVIEW
Giuseppe Andrea Giannantonio and Tobias Steinmann
Chiomenti / EPRA

THE REAL ESTATE LAW REVIEW
John Nevin
Slaughter and May

THE REAL ESTATE M&A AND PRIVATE EQUITY REVIEW
Adam Emmerich and Robin Panovka
Wachtell, Lipton, Rosen & Katz

THE RENEWABLE ENERGY LAW REVIEW
Karen B Wong
Milbank

THE RESTRUCTURING REVIEW
Christopher Mallon
Skadden, Arps, Slate, Meagher & Flom LLP

THE SECURITIES LITIGATION REVIEW
William Savitt
Wachtell, Lipton, Rosen & Katz

THE SHAREHOLDER RIGHTS AND ACTIVISM REVIEW
Francis J Aquila
Sullivan & Cromwell LLP

THE SHIPPING LAW REVIEW
George Eddings, Andrew Chamberlain and Holly Colaço
HFW

THE SPORTS LAW REVIEW
András Gurovits
Niederer Kraft Frey

THE TAX DISPUTES AND LITIGATION REVIEW
Simon Whitehead
Joseph Hage Aaronson LLP

THE TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS REVIEW
John P Janka
Latham & Watkins

THE THIRD PARTY LITIGATION FUNDING LAW REVIEW
Leslie Perrin
Calunius Capital LLP

THE TRADEMARKS LAW REVIEW
Jonathan Clegg
Cleveland Scott York

THE TRANSFER PRICING LAW REVIEW
Steve Edge and Dominic Robertson
Slaughter and May

THE TRANSPORT FINANCE LAW REVIEW
Harry Theochari
Norton Rose Fulbright

THE VIRTUAL CURRENCY REGULATION REVIEW
Michael S Sackheim and Nathan A Howell
Sidley Austin LLP

www.TheLawReviews.co.uk

ISBN 978-1-83862-055-4