دانشگاه صنعتی امیرکبیر

(پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

گزارش ارائه درس پروتکل‌های امن

گرایش امنیت اطلاعات

عنوان

آیا بیت کوین یک پول دیجیتال آنلاین امن است؟

نگارش

محمد مهدی احمدیان مرج

استاد راهنما

آقای دکتر بابک صادقیان

تیرماه ۱۳۹۳

(نسخه عمومی ۱,۱,۲ جهت انتشار در وب)

چکیده

بیتکوین یک نوآوری اینترنتی با کارکردی مشابه «پول بی پشتوانه»[1] است.ابزارهای مالی جدید همچون بیتکوین از جمله موارد قید شده در دستور کار مراکز سیاست پژوهی،مجالس قانونگذاری و بانک های مرکزی بسیاری از کشورها ی جهان اند.در سال های اخیر ارزش بیتکوین در بازارهای جهانی از چندصدم دلار به صدها دلار افزایش یافته است. روند گستره استقبال از بیتکوین ، مواردی همچون نحوه محاسبه مالیات بر درآمد، مبارزه با پولشویی و نظارت بر تراکنش های جاری ،امکان از میان رفتن ثبات مالی و خروج سرمایه از بازارهای مولد ، تضعیف پول های ملی و به خطر انداختن شهرت بانک های مرکزی را در مرکز توجه سیاستگذاران و مراکز تصمیم ساز جهانی قرار داده است .برخی اقتصاد دانان و بانکداران برجسته رشد اقبال جهانی به بیتکوین را همانند حباب میدانند و در مورد تبعات آن هشدار می دهند ،در مقابل برخی ایجاد و عرضه بیتکوین را همانند بیتکوین را یک واکنش قدرت گرفته از فناوری اطلاعات به نابسامانی های نظام مالی و پولی جهانی بشمار می آورند . واکنشی که با بازآفرینی مبنایی پول آغاز شده است. بعبارت دیگر از نظر منتقدین نظام مالی جهانی ، معماری نظم نوین جهانی با جایگزینی ارزهای دیجیتالی با دلار آمریکا آغاز شده است . گرچه دیدگاه های مختلف و متناقض پیرامون بیت کوین ، نیاز به بحث های پژوهشی بیشتری دارد ،اما واقعیت امکان اثرگذاری بیتکوین بر اقتصاد ملی و نظام پولی و مالی کشورها موجب لزوم توجه قانون گذاران به ابزار های مالی جدید همچون بیتکوین میشود.[۷]

واژه‌های کلیدی:

بیت کوین، پول دیجیتال ، پرداخت الکترونیک ، پروتکل امن پول دیجیتال

[1] .Fiat money

فهرست عناوین

صفحه

فهرست اشکال

صفحه

فهرست جداول و نمودار ها

صفحه

۱.

فصل اول:

مقدمه

۱.۱ مقدمه

بیتکوین توسط یک یا گروهی از برنامه نویسان با نام مستعار ساتوشی ناکوموتو ایجاد شده است. در مورد چیستی بیتکوین تعاریف متفاوتی عرضه شده است .در گزارش مرکز تحقیقات کنگره آمریکا عنوان شده که بیتکوین «یک ارز دیجیتالی نظیر به نظیر و متن باز است .» نظام پرداختی بیتکوین یک سامانه خصوصی است . اما هیچ موسسه مالی سنتی متعارفی در تراکنش ها وجود ندارد . برخلاف ارزهای دیجیتالی اولیه که یک شخص یا موجودیت مرکزی داشتند .نظام بیتکوین کاملا غیرمتمرکز است و همه تراکنش ها توسط کاربران نظام پرداخت بیتکوین انجام می شود. این تعریف با تعریف حقوقی از بیتکوین فاصله بسیاری دارد . به همین دلیل مرکز درآمدهای داخلی[۲] ایالات متحده آمریکا (مقرراتگذار امور مالیاتی آن کشور) بیتکوین را یک مایملک و دارایی میداند که قوانین و مقررات مربوط به دارایی در مورد آن جاری است .

بانک مرکزی چین نیز ماهیت ارز و پول بودن بیتکوین را رد می کند ،از دید دولت چین «بیتکوین یک کالای مجازی[۳] خاص است ،که جایگاه حقوقی ای[۴] معادل ارز ندارد و نمی تواند و نباید به عنوان ارز در بازار جریان یابد»،زیرا توسط یک مرجع پولی منتشر نمی شود .وزارت دارایی آلمان بیتکوین را بعنوان یک ابزار مالی جدید و به مثابه یک ارز شخصی و در جایگاه یک واحد محاسبه بشمار می آورد که از آن تعریف پول الکترونیکی برداشت نمی شود . از سویی دیگر همانند کشور های آمریکا و چین،در آلمان نیز بیتکوین به عنوان یک دارایی مالیات پذیر در نظر گرفته شده است و البته هر تعریفی که از بیتکوین ارائه شود آنچه بیتکوین را منحصر به فرد میسازد این ویژگی است که بیتکوین میتواند اولین نظام پرداخت دیجیتال کاملا غیرمتمرکز جهان بدون (بدون نیاز به بانک و بانک های مرکزی) باشد .

از سویی دیگر در کنار بیتکوین ابزارهای مالی دیجیتالی دیگری نیز وجود دارند ،برخی پیش بینی می کنند که معادل های دیگر بیتکوین در سال های آتی ممکن است از نظر اهمیت از بیتکوین پیشی بگیرند . بنابراین هر تعریفی که از بیتکوین عرضه شود باید دیگر مشابه هایش را نیز تحت پوشش قرار دهد . ابزار های مالی رقیب بیتکوین همگی انشعابات نرم افزاری بیتکوین محسوب میشوند . لایتکوین ،پی پی کوین

---

[2] .Internal Revenue Service(IRS)

[3] .Virtual Merchandise

[3] . Legal status

و مانند آن از جمله ارزهای قابل ذکر مشابهند ،ارزش هر لایتکوین در هنگام نگارش گزارش ۱۵ دلار است.[۷]

۲.۱ تاریخچه

بیت کوین یکی از اولین پیاده سازی ها با مفهوم پول رمزنگاری شده است که اولین بار در سال ۱۹۹۸توسط Wei Dai در لیست پستی cypherpunks مطرح شد. مفهوم بالا روی این تصور بنا شده است که پول میتواند هر شیء یا هر نوع از رکورد باشد که به عنوان پرداخت برای کالاها و خدمات و بازپرداخت بدهی ها در کشور معین یا زمینه اجتماعی-اقتصادی پذیرفته شده است. بیت کوین حول ایده‌ای جدیدی ازپول طراحی شده است که به جای اینکه بر قدرت مرکزی تکیه کند از رمزگذاری استفاده میکند تا ایجاد و تراکنش های خود را کنترل کند.

در سال ۲۰۰۹؛ اولین مشخصات و اثبات بیت کوین در یک لیست پستی رمز نویسی، توسط یک عضو با نام مستعار Satoshi Nakamoto منتشر شد. در اواخر سال ۲۰۱۰، Satoshi پروژه را رها کرد و گفت او باید به سراغ چیزهای دیگر برود. مخترع بیت کوین هرگز هویت خود را فاش نکرد و به راحتی اختراع خود را برای جهان باقی گذاشت. هنوز هم منشا و انگیزه پشت بیت کوین یک راز بزرگ است.

از سال ۲۰۱۰، انجمن بیت کوین با تعداد زیادی از توسعه دهندگان که روی این پروژه کار میکردند، توسعه یافت. در طی ژوئن و جولای ۲۰۱۱، بیت کوین ناگهان توجه رسانه ها را به دست آورد که آن را به سمت یک رالی بزرگ خرید هدایت کرد. کم کم نتیجه این اندیشه تورم را در اواخر سال ۲۰۱۱ کاهش داد و بعد از آن قیمت بیت کوین بار دیگر به آرامی با پشتوانه ارتقاع آن در ۲۰۱۱ بالا رفت.

در ۲۷ سـپتامبر ۲۰۱۲، بنیاد بیت کوین با یک کوشش برای استاندارد سازی ، محافظت ، و ترویج بیت کوین ایجاد شد. امروزه اقتصاد بیت کوین به سرعت با کاربران جدید که هر روز به آن می پیوندند توسعه می یابد.

۳.۱ زمینه بیت کوین در اقتصاد جهانی

بیتکوین یک نوآوری برخاسته از گسترش اینترنت است و به دلیل کارکرد اقتصادی یکی از مسائل علوم اجتماعی است .در علوم اجتماعی زمینه موضوع مورد مطالعه اهمیتی معادل یا شاید بیشتر از خود موضوع مورد مطالعه دارد ،بیتکوین تحقق یک ایده اقتصادی در قالب یک برنامه رایانه ای است و اگر استقبال جامعه نبود ، در رایانه به فراموشی سپرده می شد.اما بیتکوین به سرعت مرحله پذیرش از سمت جامعه را طی کرده است . [۷]

به عبارت دیگر در چندسال اخیر دانش به کارگیری بیتکوین تنها در اختیار عده محدودی از علاقمندان مجامع اینترنتی بوده.اما امروزه اندازه بازار[۵] بیتکوین از بازار کل شرکت های سهامی برخی از ملت های کوچک و متوسط دنیا بزرگتر است. ارزش بیتکوین نسبت به دیگر ارزها به واسطه عرضه و تقاضا تعیین شده و رشد و نوسان بسیاری داشته است . برخلاف رشد سریع ارزها بیتکوین نسبت به زمان آغاز به کارش ،میزان استفاده ار بیتکوین در حد یک ارز ویژه[۶] که بازار محدودی دارد باقی مانده است . در اوایل سال ۲۰۱۳ ، مقدار کل بیتکوین های در گردش به ۱۲ میلیون رسید که دو میلیون از سال های پیش بیشتر بود . در سال گذشته به طور متوسط روزانه بیش از ۵۰ هزار تراکنش بیتکوین انجام شده است . اوج ارزش بیتکوین در دسامبر ۲۰۱۳ اتفاق افتاد که ارزش هر واحد بیتکوین به بیش از ۱۲۰۳ دلار رسید در حالی که طی روزهای آغازین ،ارزش آن از چند صدم دلار تجاوز نمی کرد.تخمین زده می شود که جمع ارزش بازاری بیتکوین بیش از ۱۰ میلیارد دلار باشد. در حال حاضر حدود ۱۲ میلیون بیتکوین در گردش

[5] .Market Captialization

[6] . Niche

است.گرچه مقدار کل بیتکوین هایی که می توانند تولید شوند بصورت قراردادی در ۲۱ میلیون بیتکوین محدود شده اند .[۷]

پیش بینی می‌شود در سال ۲۱۴۰ میلادی به اندازه سقف قراردادی بیتکوین تولید شود. همچنین از آنجا که هر بیتکوین تا هشت رقم اعشار قابل تقسیم است مقدار کل بیتکوین های قابل خرج کردن بیش از دو هزار تریلیون خواهد بود . بررسی نوسانات ارزش بیتکوین در یک بازه یک ساله برحسب دلار نشان میدهد. تاکنون دو عامل اصلی توانسته اند اثر گذاری محسوسی روی بیتکوین داشته باشند .اولین عامل که تاثیر کمتری هم داشته ،از جنس عوامل فناورانه بوده است . دومین عامل یا مداخلات دولت ها و واکنش قدرت های جهانی در قالب مقررات گذاری این حوزه ،عامل مهمتری بر میزان اثرگذاری این پدیده و خط سیر تکاملی آن بوده است .همچنان انتظار می‌رود که مقررات گذاری کشورها تاثیر گذاری محوری بر بیتکوین داشته باشد.[۷]

۲

فصل دوم:

بیت کوین چیست؟

۱.۲ مقدمه

بیت‌کوین معادل پول نقد اینترنتی است. شما میتوانید بیت‌کوین را از طریق اینترنت مستقیما و بدون هیچ واسطه ای برای هرکسی در هر کجای دنیا ارسال کنید. همچون پول نقد، نقل و انتقالات بیت‌کوین هم لغو کردنی نیستند .بیت‌کوین در سراسر جهان خرید و فروش می شود.

بیت کوین یک نوآوری اینترنتی با کارکردهای مشابه "پول بی پشتوانه " یا پول حکومتی است. نوآوری بودن بیتکوین به این معناست که خالقان آن توانسته اند آنرا در مدت کوتاهی از یک ایده به یک واقعیت اثرگذار بر دنیای اقتصاد و مراکز سیاست پژوهی مبدل کنند. زیرا در چندسال گذشته ارزش بیتکوین در بازارهای جهانی از چند صدم دلار به صدها دلار افزایش یافته است[۷]

اما پول بودن یک جایگاه حقوقی است و پول بودن بیت کوین منوط به پذیرش جایگاه حقوقی آن از سوی دولت هاست. تا کنون هیچ دولتی پول بودن بیت کوین را تایید نکرده است و دولت های ایالات متحده آمریکا، جمهوری فدرال آلمان و جمهوری خلق چین بر کالا بودن بیتکوین تاکید دارند[۷]. البته از لحاظ فنی و کارکردی این عبارت صحیح است که بیت کوین نوعی پول دیجیتال بر پایه شبکه همتا به همتا، امضای دیجیتال و اثبات صفر-دانش است و به کاربران امکان می دهد که بدون هیچ واسطه ای انتقال پول غیر قابل بازگشت انجام دهند. گره های شبکه هر معامله را در شبکه اعلام می کنند که پس از تایید در یک سیستم اثبات کار، در یک تاریخچه عمومی به نام زنجیره بلاک [۷]ذخیره می شود. بیت کوین در سال ۲۰۰۹ مبتنی بر عقایدی که ساتوشی ناکاموتو در مقاله ای [۱] منتشر کرد پایه گذاری شد.

بیت کوین امکان پرداخت‌های بسیار کم هزینه را فراهم می‌کند. شبکه بیت کوین سیستم کنترل کننده متمرکز ندارد و توسط هیچ ارگان یا نهاد دولتی اداره نمی‌شود. زمان متوسط تایید هر انتقال بیت‌کوین، تقریباً ده دقیقه است. انتقال پول از یک نقطه به نقطه دیگر در تمام شبکه اطلاع رسانی شده و تمام نقاط از آن آگاه خواهند شد.

[7] Blockchain

قبل از ابداع بیت کوین، سیستم های مالی آنلاین برای امنیت به یک سیستم کنترل کننده مرکزی احتیاج داشتند. ناکاموتو با استفاده از شیوه اثبات کار در یک شبکه همتا به همتا، راهی جایگزین پیشنهاد کرد. بیت کوین نسبتاً پروژه ای جدید و شدیداً تحت توسعه است. به همین دلیل توسعه دهندگان آن به کاربران توصیه می کنند که به آن به عنوان یک نرم‌افزار آزمایشی نگاه کنند.

۲.۲ ویژگی های منحصر بفرد

اینها فهرست کارهایی است که فقط با بیت‌کوین امکانپذیر است:

ـ بیت‌کوین را به صورت بین المللی با هزینه ای ناچیز منتقل کنید.

ـ اگر قصد فروش محصولات خود را در اینترنت دارید بدون نیاز به درخواست درگاه پرداخت از بانک ها یا موسسات دیگر میتوانید فروش از طریق بیت‌کوین را آغاز کنید.

ـ ثروت خود را در برابر کاهش ارزش پول دولتها محافظت کنید.

۳.۲ ویژگی های فنی

این ها ویژگی های پایه ای از هر نوع شبکه ی بیت کوین است.

- بیت کوین می تواند بین هر نود اختیاری در شبکه منتقل شود.
- تراکنش ها تغییر ناپذیرند.
- با استفاده ازیک زنجیره بلاک از پرداخت های تکراری جلوگیری میشود.
- تراکنش ها در چند ثانیه منتشر و بین ۱۰ تا ۶۰ دقیقه تایید می شوند.
- پردازش تراکنش و صدور پول در مجموع با استخراج انجام داده می شود .
- تراکنش ها در هر زمانی صرف نظر از اینکه کامپیوتر شما خاموش باشد یا روشن دریافت می شوند .

۴.۲ مشتریان بیت کوین را می پسندند

دلایل زیادی وجود دارد که مشتریان بیت کوین را ترجیح می دهند:

پرداخت آسانتر

پرداخت با بیت‌کوین به مراتب راحتر از پرداخت با کارت بانکی است. برخلاف کارتهای بانکی با بیت‌کوین نیازی نیست که شماره کارت، تاریخ انقضا، نام صاحب کارت و رمز کارت را وارد کنید.

قیمت های ارزان تر

بانک های ارائه دهنده درگاه های پرداخت اینترنتی معمولا درصدی از فروش را از فروشندگان بابت کارمزد کسر میکنند. با استفاده از بیت‌کوین فروشندگان میتوانند این کارمزد به صورت تخفیف به مصرف کنندگان ارائه کنند.

حریم خصوصی بالاتر

با بیت‌کوین خریدار تنها اطلاعات ضروری برای خرید را در اختیار فروشنده قرار میدهد. زیرا مبنی بیت کوین Trust no one است . برای مثال اگر شما خدمتی را از سایتی خریداری کرده اید که نیازی به ارسال پستی ندارد، شما آدرس خود در اختیار فروشنده قرار نخواهید داد.

امنیت بالاتر

با بیت‌کوین خریدار مبلغ خرید را مستقیما برای فروشنده ارسال میکند و در این میان هیچ واسطه ای نیست. خریدار هیچ اطلاعاتی مانند شماره کارت یا رمز کارت را در اختیار فروشنده قرار نمیدهد تا در آینده مکان سوء استفاده از آن باشد.

استفاده از بیت‌کوین ارزش آن را بالاتر میبرد

اگر شما مقداری بیت‌کوین پس انداز کرده اید شما میتوانید با استفاده کردن از آنها ارزش بیت‌کوین را بالا ببرید. استفاده از بیت‌کوین باعث افزایش تقاضا برای آن و در نتیجه بالا رفتن ارزش آن خواهد شد.

۵.۲ فروشندگان بیت کوین را می پسندند

برگشت ناپذیر بودن تراکنش ها

فروشندگان میتوانند امکان بازگرداندن پول را در سایت خود پیش بینی کنند اما این کار در اختیار خود فروشنده است و جلوی برگشت های تقلبی را میگیرد.

کارمزد ناچیز در نقل و انتقالات

دریافت بیت‌کوین رایگان است و ارسال آن هزینه ناچیزی دارد.

پذیرش بیت‌کوین به صورت بین المللی

از هر کسی در هر جای دنیا با اطمینان پول دریافت کنید. در چند ثانیه فروشنده میتواند متوجه شود که پول در راه است و تراکنش در مدت ۱۰ دقیقه تا یک ساعت نهایی خواهد شد.

بدون کارمزد یا هزینه راه اندازی درگاه پرداخت

فروشنده ها، پرداخت های خریداران را مستقیما دریافت میکنند. فروشندگان نیازی به دریافت درگاه از هیچ بانک یا شرکت دیگری را ندارند. فروشندگان لازم نیست نگران عدم پذیرش فروشگاه برای دریافت درگاه یا پرداخت با تاخیر از طرف درگاه اینترنتی و یا فسخ قرارداد پرداخت از طریق بانک یا شرکت ارائه کننده درگاه باشند.

عدم محدودیت در تعداد تراکنش

اگرچه سیستم معمول بانکی ممکن است دارای تعدادی محدود تراکنش برای هر کاربر باشد ولی در سیستم بیت کوین هیچ محدودیتی وجود ندارد.

عدم نیاز به تنظیمات خاص(No Setup)

بدون نیاز به تنظیمات خاص و راه اندازی هایی مانند کارت های اعتباری

۶.۲ بیت‌کوین از پول های رایج بهتر است

چند دلیل برای اینکه بیت‌کوین از پول های رایج بهتر است:

ـ بیت‌کوین یک واحد پولی بین المللی است.

ـ بیت‌کوین را میشود در سراسر جهان خرج کرد.

ـ بیت‌کوین قابل جعل کردن نیست.

ـ هیچ تکنولوژی چاپی نمیتواند شبکه بیت‌کوین را فریب بدهد.

حتی قابلیت پیاده سازی با سیستم های رمزنگاری جدید مانند محاسبات کوانتومی

ـ بیت‌کوین نمیتواند بی ارزش شود.

ـــ تنها ۲۱ میلیون بیت‌کوین قابل صدور است. بر خلاف واحد پول های رایج، از آنجایی که بیت‌کوین به هیچ دولت یا بانکی وابسته نیست، افزایش سقف بدهی های دولت و تغییر در سیاست های مالی نمیتواند باعث کم شدن ارزش بیت‌کوین شود.(به نوعی تورم معمول برای آن تعریف نمی شود)

-از لحاظ اقتصادی وابسته به هیچ کالای خاصی نیست.

۷.۲ بیت‌کوین از طلا بهتر است(قوانین اقتصادی)

برای هزاران سال، طلا یکی از امن ترین سرمایه گذاری ها بود. بسیاری از مردم با نگهداری طلا ریسک کم ارزش شدن سرمایه خود را کاهش میدادند. بیت‌کوین برتری های زیادی بر طلا دارد.

ـ طلا تقسیم پذیر نیست

شما نمیتوانید به راحتی طلا را به مقدار های کوچکتر تقسیم کنم و برای معاملات استفاده کنید اما بیت‌کوین به سادگی تا هشت رقم اعشار قابل خرد کردن است. در مجموع بازده در حدود ۲۱*$۱۰^{۱۴}$ واحد پول، می باشد.

جدول ۱:واحد های بیت کوین

Bitcoins	Unit (Abbreviation)

1.0	bitcoin (BTC)
0.01	bitcent (cBTC)
0.001	millibit (mBTC)
0.000001	microbit (uBTC)
0.00000001	satoshi

ـ طلا امکان عیارسنجی بدون وقفه را ندارد

شما نمیتوانید بلافاصله متوجه شوید که طلایی که در دست دارید خالص است اما شما میتوانید بلافاصله متوجه شوید که بیت‌کوین شما واقعی است.

ـ طلا امکان وزن کردن بدون وقفه را ندارد

برای وزن کردن طلا نیاز به ترازو است اما شما به صورت آنی میتوانید بگوئید که چند بیت‌کوین دارید.

ـ طلا امکان ارسال از طریق اینترنت را ندارد

ارسال طلا برای دیگران خطرات زیادی دارد اما بیت‌کوین به راحتی از طریق اینترنت قابل ارسال است.

۸.۲ تکنولوژی استفاده شده در بیت کوین

بیت کوین به وسیله جدیدترین تکنولوژی های روز پیاده سازی شده است.

- رمزگذاری که در سیستم های بانکداری اینترنتی مورد استفاده قرار میگیرد.
- شبکه نقطه به نقطه امکان دخالت اشخاص و دولت ها را در سیستم از بین می‌برد.
- نرم افزار بیت‌کوین متن باز است و به همه اجازه میدهد تا کدها را بررسی و بهبود دهند.

۹.۲ چگونه کار با بیت کوین را شروع کنیم؟

ـ ابتدا بایستی یک حساب کاربری در یکی از سایت های ارائه دهنده خدمات بیت کوین سازید.

ـ به بخش واریز به حساب بروید و با واریز وجه به شماره حساب سایت موجودی خود را در سایت افزایش دهید.

ـ از بخش خرید بیت‌کوین مقداری بیت‌کوین خریداری کنید

۱۰.۲ با بیت کوین چه کار هایی می توان انجام داد؟

ـ بیت‌کوین های خود را برای خرید در اینترنت خرج کنید

ـ بیت‌کوین خود را پس انداز کنید

بهترین راه پس انداز بیت‌کوین این است که آن بروی سایت نگهداری کنید.

ـ بیت‌کوین خود را بفروشید

هر زمانی که بخواهید میتوانید بیت‌کوین خود را در سایت به فروش برسانید.

ـ بیت‌کوین خود را منتقل کنید

شـــما میتوانید بیت‌کوین خریداری شـــده را به کیف پول الکترونیکی خود منتقل کنید. اگر از امنیت کامپیوتر خود مطمئن هســـتید میتوانید نرم افزار کیف پول الکترونیکی را بروی کامپیوتر خود نصـــب و بیت‌کوین های خود را به کامپیوتر خود منتقل کنید.

۱۱.۲ ریسک های بیت‌کوین

هرگز تمام دارایی خود را در بیت‌کوین ســرمایه گذاری نکنید. بیت‌کوین یا هر پول دیگری بدون ریسک نیست. برای مثال، هرکدام از موارد زیر ممکن است اتفاق بیافتد:

ـ یک واحد پولی رمزگذاری دیگر بر بیت‌کوین پیشی بگیرد

تعداد زیادی قبلا سعی کرده اند اما موفق نشده اند.

ـ نقصی در الگوریتم رمزگذاری پیدا شود

این همان سیستمی است که در رمزگذاری سیستم های بانکداری اینترنتی استفاده میشود پس اگر چنین ضعفی در این الگوریتم پیدا شود، کاربران بیت‌کوین هم از الگوریتم جدید استفاده خواهند کرد.

ـ ممکن است دولت ها بیت‌کوین را ممنوع کنند

این کار شبیه ممنوع کردن اینترنت به دلیل استفاده های غیرقانونی از اینترنت است. ممنوع کردن اینترنت به دلیل ضررهای ارتباطی برای دولت و مردم آن کشور بعید است. به همین شکل هم ممنوع کردن بیت‌کوین به دلیل ضررهای اقتصادی برای دولت و مردم آن کشور دور از ذهن است.

ـ یک اشکال غیر قابل رفع در پروتکل بیت‌کوین پیدا شود

هکر ها دو سال است که به دنبال اشکال در این پروتکل هستند اما هنوز کسی موفق نشده است.

۱۲.۲ چالش های بیت‌کوین

برخی از چالش هایی که بیت کوین با آنها در گیر است را ذیلا برشمرده ایم:

- چالش های مبادله آن با واحدهای معتبر پول :هرچند که روند مبادله روز به روز بهتر می شود.
- استفاده از بیت کوین در معاملات غیرقانونی و خلافکارانه و عدم امکان پیگیری برای دولت ها
- استخراج بیت کوین نیازمند مصرف انرژی

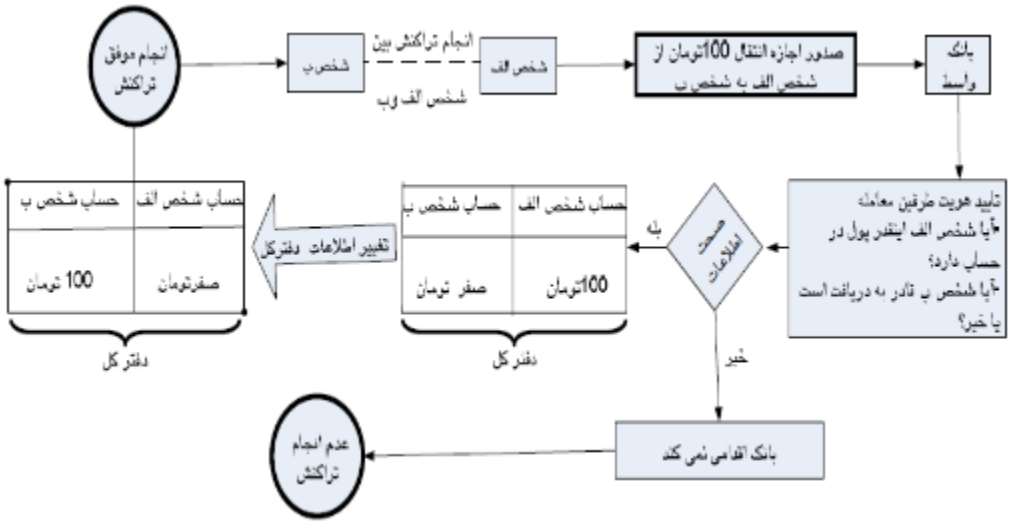
۱۳.۲ آمار

شبکه بیت کوین به طور مداوم بیش از ۴۸ ماه، ویژگی های امنیتی قابل توجهی به دست آورد و در سال گذشته رشد قابل توجهی داشته است. همانطور که از آوریل ۲۰۱۳:

- زنجیره بلاک طولانی با بیش از ۲۳۲،۰۰۰ بلاک.
- یکی از بزرگترین شـــبکه محاســـبات توزیع شـــده در جهان با بیش از ۶۵ تراکنش بر ثانیه یا terahashes/s است.
- میلیون ها دلار در حجم تجارت روزانه که در مجموع ۵۰،۰۰۰ تراکنش توزیع شده است .
- ارزش کل تمام بیت کوین های در گردش، بیش از ۱,۳ میلیارد دلار آمریکا است.
- فقط یک حادثه عمده امنیتی در پروتکل که در ماه اوت ۲۰۱۰ اصلاح شد.

۱۴.۲بیت کوین چگونه بدون نیاز به بانک کار میکند ؟

نظام تراکنش های مالی ســـنتی برای انجام تراکنش ها به بانک نیاز دارد . نمودار نمایی از یک تراکنش ساده که هردو طرف تراکنش در همان بانک حساب دارند را نشان می‌دهد.



شکل ۱: نمودار تراکنش مالی در سیستم سنتی[۷]

در نظام مالی سنتی ،بانک ها کنترل همه تراکنش ها را با تغییر اطلاعات دفتر کل در اختیار دارند ،اما در نظام بیت کوین اختیار دفتر کل در دست یک بانک مرکزی نیست . به همین دلیل ،برخی مراجع از بیتکوین با عبارت «ارزهای رمز پایه» یاد میکنند زیرا برای ارزشیابی تراکنش ها و نظارت بر تولید بیتکوین های جدید از اصول رمزنگاری (ارتباطاتی که از دید طرف های سوم شخص به دور است) استفاده شده است .هر بیتکوین و هر کاربر بیتکوین به وسیله یک هویت یکتا ،رمزنگاری شده اند و همه تراکنش ها در دفتر کل عمومی ثبت شده اند که برای همه رایانه های شبکه قابل مشاهده است ،اما هیچ اطلاعات شخصی را در مورد طرف های درگیر افشا نمی کند.دفتر کل عمومی تایید می‌کند که انتقال دهنده اولیه بیتکوین ،مالک حقیقی بیت کوین خرج شده بوده و در نتیجه تراکنش تایید شده و پذیرنده بیتکوین مالک جدید بیتکوین است [۷].

دفتر کل عمومی ویژگی اصلی بیتکوین (و دیگر ارزهای رمز پایه است) زیرا مسئله دوباره خرج کردن پول (خرج کردن پولی که مالکش نیستم با توسل به جعل وتقلب) و نیاز به وجود یک واسط سوم شخص (مانند مانند بانک یا شرکت کارت اعتباری) برای تصدیق درستی تراکنش الکترونیکی بین خریدار و فروشنده را بطور همزمان حل کرده است.[۷]

۳

فصل سوم:
جزئیات فنی بیت کوین

۱.۳ واژگان شناسی

۱.۱.۳ آدرس

یک آدرس بیت کوین مانند یک آدرس فیزیکی یا یک ایمیل است. این تنها اطلاعاتی است که شما نیاز دارید برای دریافت پرداخت بیت کوین به کسی ارائه دهید.به طور دقیق تر باید بگوییم که بیت کوین مقدار درهم سازی شده کلید عومی مالک کلید است که مقداری مشابه ذیل می باشد:

1MikiSPbrhCFk7S4wzZP7gQqhwWH866DCb

Public key: 32 characters starting with 1 or 3

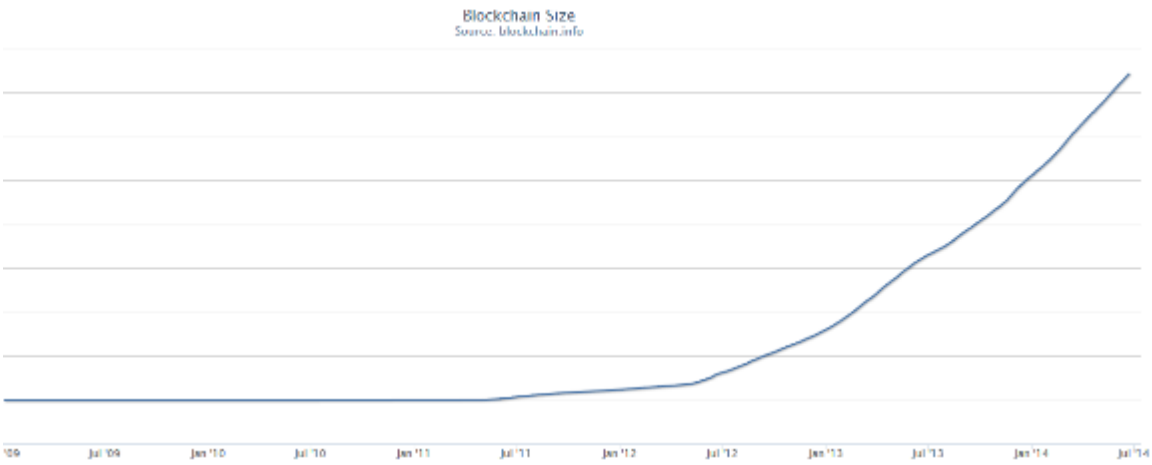
Private key: 51 characters starting with 5

۲.۱.۳ زنجیره ی بلاک[1]

زنجیره ی بلاک رکورد عمومی تمام تراکنش های بیت کوین ، به ترتیب زمان وقوع است.در حقیقت زنجیره بلاک تراکنش هایی است که مورد بررسی و تایید قرارگرفته اند و عمومی شده اند.زنجیره‌ی بلاک بین تمام کاربران بیت کوین به اشتراک گذاشته شده است. این برای بررسی مانده حساب آدرس های بیت کوین و جلوگیری از پرداخت تکراری استفاده می شود.در نمودار ذیل حجم این زنجیره از آغاز تا کنون را نمایش می دهد.

[1] Blockchain

نمودار ۱: نمودار حجم زنجیره بلاک از ابتدا تا کنون



۳.۱.۳ بلاک

هر تراکنش انجام گرفته تحت عنوان بلاک به بقیه انتشار پیدا می کند،البته در این بلاک علاوه بر تراکنش فعلی اطلاعاتی از کلیه تراکنش های قبلی(زنجیره بلاک) سیستم نیز قرار دارد. تقریباً هر ۱۰ دقیقه ، به طور میانگین ، یک بلاک جدید که شامل تراکنش ها است به زنجیره ی بلاک از طریق استخراج یا ماینینگ اضافه می شود.

در صورتی که یک گره مولد بلوک موفق به تولید یک بلوک شود، آن را به تمام گره‌هایی که با آنها در ارتباط است می‌فرستد. این گره‌ها درستی بلوک را بررسی می‌کنند و در صورت صحت بلوک و تمام درخواست‌های داخل آن، آن را برای تمام گره‌های مرتبط خود می‌فرستند. به این روش هر بلوک معتبر، به سرعت در شبکه پخش می‌شود. مولدهای دیگر، در صورت دریافت یک بلوک معتبر، کار روی درخواست‌های انتقالی که داخل این بلوک است را رها می‌کنند و شروع به تلاش برای تولید بلوک بعدی می‌کنند. به همین دلیل درخواستی که داخل یک بلوک ثبت می‌شود در واقع توسط اکثریت شبکه تایید شده است. مولدی که موفق به تولید یک بلوک می‌شود، یک درخواست انتقال ویژه به آن اضافه می‌کند

که هیچ فرستنده‌ای ندارد و ۲۵ بیت‌کوین به آدرس خودش واریز می‌کند. این ۲۵ بیت‌کوین به عنوان پاداش مولد محسوب می‌شود و با اینکه هیچ فرستنده‌ای ندارد، توسط بقیه گره‌ها یک انتقال وجه درست محسوب می‌شود. البته این جایزه در ابتدا ۵۰ بیت‌کوین بود. این جایزه هر ۲۱۰۰۰۰ بلوک نصف می‌شود.
BTC

BTC واحد مشترک پول بیت کوین است ، که این می تواند به شکلی شبیه USD برای دلار آمریکا به جای $ از ฿ استفاده شود.

۴.۱.۳ تایید

تایید به این معناست که یک تراکنش توسط شبکه بررسی شده و بسیار بعید است که بتوان آن را برگرداند. یک تایید بسیار امن است. اگرچه برای مقادیر بزرگ تر (مثلاً ۱۰۰۰ دلار و بالاتر) ، فرد می تواند برای تعداد بیشتری از تایید تراکنش صبر کند .

۵.۱.۳ پرداخت تکراری[1]

اگر یک کاربر بدخواه سعی داشته باشد بیت کوین ها را در یک لحظه برای دو دریافت کننده ی متفاوت خرج کند ، این خرج یا پرداخت دو برابر یا تکراری است. استخراج بیت کوین و زنجیره ی بلاک آن جا هستند تا به یک توافق عمومی در شبکه درباره ی این که کدام یک از دو تراکنش برنده خواهند بود برسند.

۶.۱.۳ نرخ درهم سازی

[1] Double-spending

نرخ درهم سازی واحد اندازه گیری قدرت پردازشی شبکه ی بیت کوین است(H/s). شبکه ی بیت کوین باید عملیات ریاضی متمرکز و شدیدی برای مقاصد امنیتی انجام دهد. وقتی که شبکه به نرخ درهم سازی ۱۰ TH/sبرسد ، به این معناست که می تواند ۱۰ تریلیون محاسبه درهم سازی در هر ثانیه انجام دهد.

۷.۱.۳ استخراج

استخراج بیت کوین به پروسه ی بکارگیری سخت افزار کامپیوتر به انجام محاسبات ریاضی برای شبکه ی بیت کوین جهت تایید تراکنش ها و بالا بردن امنیت می گویند. به عنوان یک جایزه برای خدماتشان ، استخراج کنندگان بیت کوین می توانند هزینه ی تراکنش ها را برای تراکنش هایی که تایید می کنند ، همراه با بیت کوین های تازه تولید شده جمع آوری کنند. استخراج یک بازار تخصصی و رقابتی است که در آن جوایز با توجه به میزان محاسبات انجام شده تقسیم می شوند. تمام کاربران بیت کوین استخراج بیت کوین انجام نمی دهند ، و این یک راه ساده برای پول در آوردن نیست.

۸.۱.۳ شبکه P2P

نظیر-به-نظیر به سامانه هایی که مانند یک اجتماع سازماندهی شده کار می کنند با دادن اجازه ی تعامل مستقیم به هر فرد با افراد دیگر اشاره دارد. در مورد بیت کوین ، شبکه طوری ساخته شده که هر کاربر تراکنش های کاربران دیگر را منتشر می کند. و این مهم است که هیچ بانکی به عنوان شخص ثالث نیاز نیست.در بیت کوین شبکه نظیر-به-نظیر از بستر شبکه اینترنت استفاده می کند.تعداد گره های شبکه در سال ۲۰۱ برابر ۱۸۰۰۰ گره بود که هر گره نیز به طور متوسط با ۱۰ الی ۱۰۰ گره در ارتباط بود.

۹.۱.۳ کلید خصوصی

یک کلید خصوصی مقداری داده مخفیانه است که حق شما برای خرج کردن بیت کوین ها را از یک آدرس بیت کوین خاص از طریق یک امضای رمزنگاری شده ثابت می کند. هر آدرس بیت کوین کلید خصوصی خود را دارد. اگر از یک کیف پول نرم افزاری استفاده کنید کلیدهای خصوصی شما بر روی کامپیوتر شما ذخیره شده اند ؛ اگر از یک کیف پول تحت وب استفاده کنید آن ها بر روی تعدادی ریموت سرور یا سرور از راه دور ذخیره شده اند. از آن جایی که آن ها به شما اجازه ی خرج کردن بیت کوین های آدرس بیت کوین مربوطیشان را می دهند کلید های خصوصی هرگز نباید نشان داده شوند.

۱۰.۱.۳ امضا

یک امضای رمزنگاری شده یک مکانیزم ریاضی است که به یک فرد اجازه می دهد تا مالکیتش را اثبات کند. در مورد بیت کوین ، یک آدرس بیت کوین و کلید خصوصی اش با یکسری عملیات های ریاضی به هم متصل شده اند. وقتی نرم افزار بیت کوین شما یک تراکنش را با کلید خصوصی مناسب امضا می کند ، تمام شبکه می توانند ببینند که امضا با آدرس بیت کوین هم خوانی دارد. اما ، هیچ راهی وجود ندارد که کلید خصوصی شما را حدس بزنند تا بیت کوین های به سختی به دست آمده ی شما را بدزدند.
به طور دقیق تر باید بگوییم که الگوریتم امضای رقمی بیت کوین EC/DSA[1] است که نسبت به امضای رقمی RSA (RSA/DSA)طول کلید کوچک تر و سرعت محاسباتی بالاتری دارد .

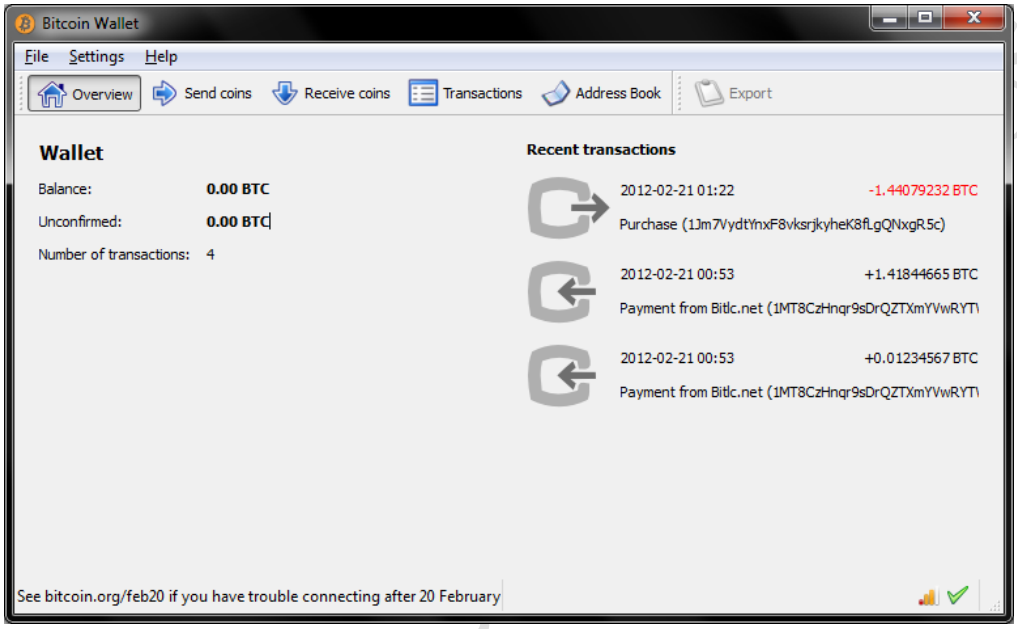
۱۱.۱.۳ کیف پول[2]

یک کیف پول بیت کوین به زبان ساده معادل یک کیف پول فیزیکی در شبکه ی بیت کوین است. کیف پول در حقیقت کلید های خصوصی شما را شامل می شود که به شما اجازه ی خرج کردن بیت کوین های اختصاص یافته به آدرس بیت کوینتان در زنجیره ی بلاک را می دهد. هر کیف پول بیت کوین می تواند

[1] Elliptic Curve Digital Signature Algorithm

[2] Wallet

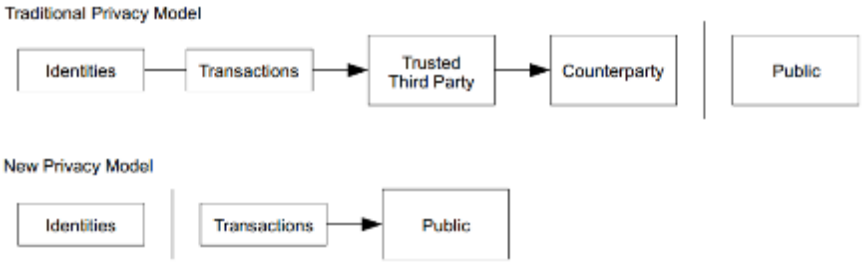
به شما مانده حساب کل آدرس های بیت کوینی را که شامل می شود نشان دهد و به شما اجازه می دهد که یک مقدار خاص را به یک فرد خاص پرداخت کنید ، درست مانند یک کیف پول واقعی. این با کارت های اعتباری متفاوت است که پول از حساب شما توسط فروشنده کم می شود.



شکل ۲:نمونه ای از کیف پول بیت کوین

۲.۳ حریم خصوصی در بیت کوین [۱]

همانطور که در شکل ۳مشاهده می کنید در سیستم سنتی حفظ حریم خصوصی در تراکنش ها مالی وابسته به شخص ثالث مورد اعتماد بود که کلیه تراکنش ها و اطلاعات محرمانه را حفظ می کند اگرچه خود این شخص ثالث مورد اعتماد می تواند به این اطلاعات دسترسی داشته باشد ،اما در پروتکل بیت کوین از آنجایی که هیچ نهاد مرکزی وجود ندارد و از طرفی کلیه تراکنش های به اطلاع همه می رسد آنچه که تضمین کنند حفظ حریم خصوصی است آدرس هایی هستند که در بیت کوین تولید می شوند.در واقع حریم خصوصی با بی نام سازی کلیدهای عمومی در پروتکل بیت کوین ممکن می شود.



شکل ۱:مدل حریم خصوصی سنتی و جدید [۱]

۳.۳ تراکنش انتقال بیت کوین

در این بخش به دنبال تشریح نحوه انتقال پول در بیت کوین هستم،همانطور که در شکل۴ می بینیم به عنوان مثال باب قصد دارد مبلغ 100BTC رابه آلیس منتقل کند.

شکل ۴: مثال انتقال در بیت کوین

پروتکل بیت کوین به نحوی عمل می کند که برای هر نقل انتقال آدرس های گیرنده و فرستند طبق توضیحات فصل قبل بر اساس آدرس محاسبه شده از کلیدعمومی فرد همانطور که در شکل۵ می بینید انجام می شود .

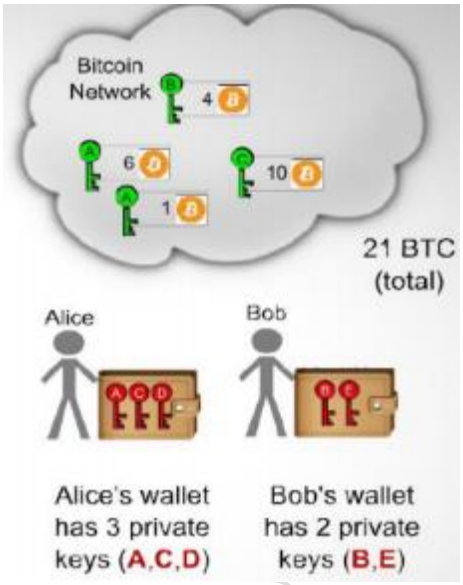
شکل ۵: مثال انتقال در بیت کوین با آدرس های حقیقی

بعد از ارسال تراکنش به آدرس عمومی مورد نظر به کمک پخش تراکنش در شبکه مرحله بررسی اعتبار این تراکنش توسط سایر گره های استخراج کننده همانطور که ادامه توضیح خواهد داده شد بررسی می‌شود.

شکل ۶: مثال انتقال در بیت کوین در هنگام بررسی

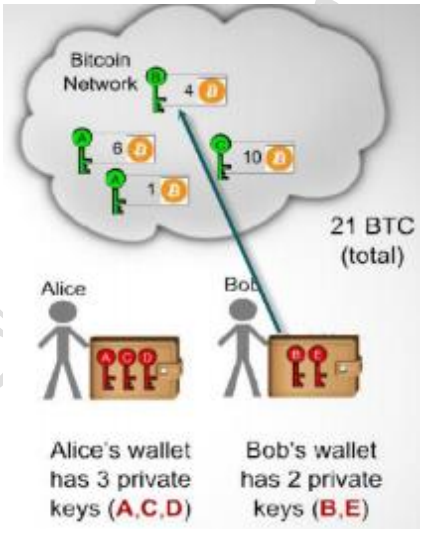
۴.۳ انتقال وجه با خرد کردن

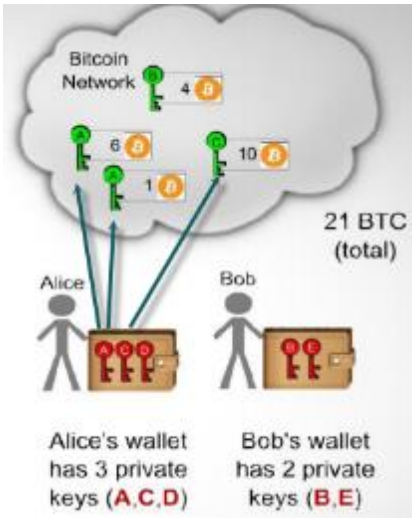
در این بخش قصد داریم با بیان یک مقال نحوه انتقال وجه در عمل را برای پروتکل بیت کوین شرح دهیم.همانطور که در شکل۷می بینیم در این شبکه بیت کوین جمعا 21BTC وجود دارد .



شکل ۷: مثال انتقال وجه

که 17BTC آن متعلق یه آلیس و 4BTC متعلق به باب است.



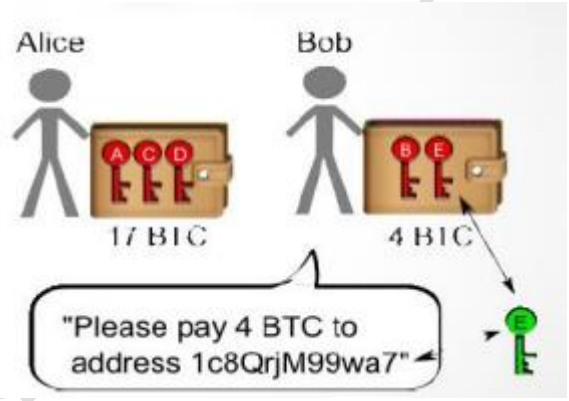


شکل ۸: صورت حساب های متعلق به هر شخص

همانطور که مشاهده می کنیم در شبکه بیت کوین هر صورت حساب همراه با یک کلید عمومی است.
در پروتکل بیت کوین امکان داشتن تعداد نامحدود کلید عمومی برای افراد وجود دارد. و تعداد کل کلیدهای عمومی شبکه بیت کوین برابربا $۲^{۱۶۰}$ می تواند باشد که همانطور که مشاهده می کنید در ذیل عدد بسیار بزرگی است.

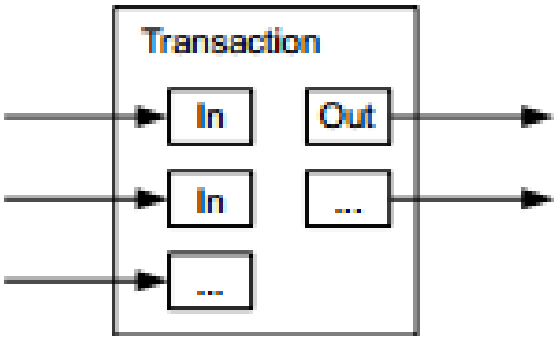
$2^{160}=1.461501637330902918203684832716 3e+48$

در شبکه بیت کوین تنها کسی که صورت حسابی را امضا کرده است مجوز این را دارد که آن را با کلید عمومی دیگر امضا کند.حال در این مرحله باب با کلید عمومی استفاده نشده E یک آدرس تولید می کند و از آلیس می خواهد تا 4BTC را به آدرس تولید شده بفرستد.برای هر تراکنش نیاز به زوج کلید استفاده نشده ای داریم تا ضامن حریم خصوصی باشد.



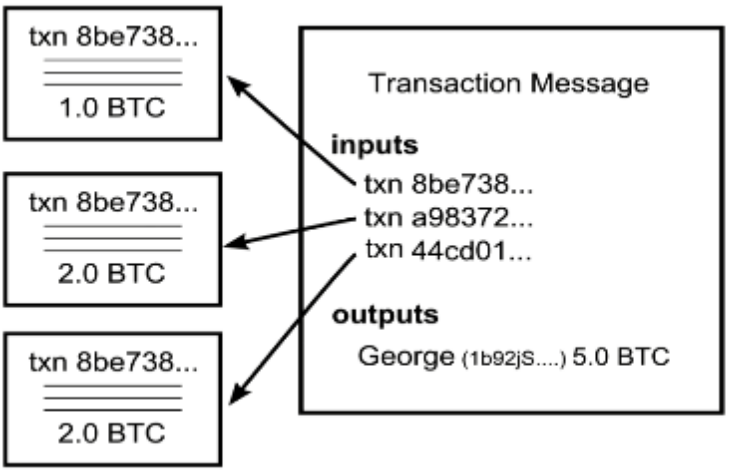
شکل ۹: تولید آدرس توسط باب

نکته ای که در اینجا وجود دارد این است که آلیس صورت حساب 4BTC ندارد، بنابراین باید یکی از صورت حساب های خود را خرد کند . برای ایجاد امکان وجود خرد کردن و ترکیب کردن پول ها هر تراکنش چندین ورودی و حداکثر دو خروجی دارد که زمانی که قرار باشد پولی خرد شود از هر دو خروجی تراکنش استفاده می شود. [۱]



شکل ۱۰:ورودی و خروجی های تراکنش ها [۱]

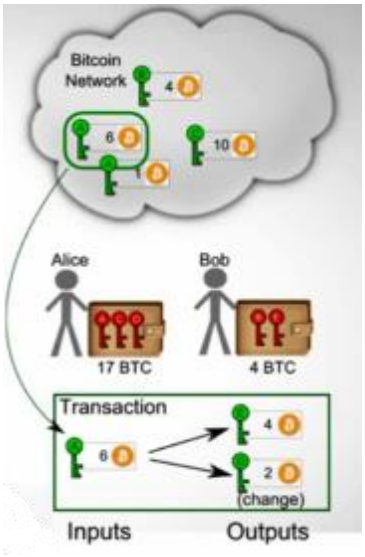
در شکل ۱۱ یک نمونه عملیاتی از تراکنش با ورودی و خروجی هایش را مشاهده می کنید که در این تراکنش سه تراکنش ورودی و یک تراکنش خروجی دارد که بر این اساس در صورت معتبر بودن تراکنش تقاضای ارسال 5BTC به جورج شده است.



شکل ۱۱: نمونه عملیاتی از تراکنش با ورودی و خروجی

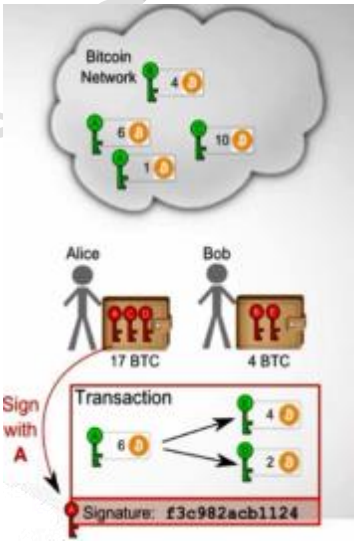
حال به مثال خود بر می گردیم در این مرحله همانطور که در شکل۱۲ مشاهده می کنید آلیس یک تراکنش ایجاد می کند حاوی 4BTC. با آدرس کلید عمومیE متعلق به باب به عنوان خروجی اول و 2BTCبا آدرس کلید عمومی D متعلق به آلیس

به عنوان خروجی دوم تراکنش



شکل ۱۲: نحوه تولید بلاک تراکنش

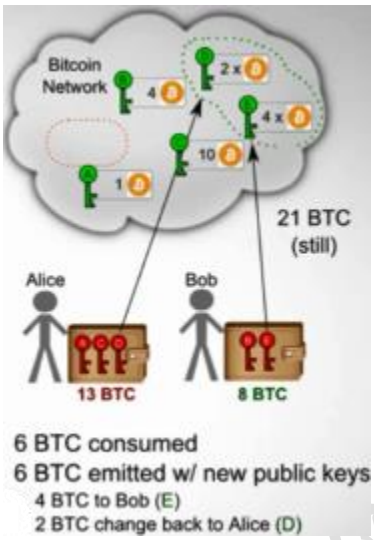
سپس این بلاک تراکنش را با کلید خصوصی تراکنش ورودی (کلید خصوصی متناظر با کلید عمومی A)امضا می کند و تراکنش را در شبکه پخش می کند.این بلاک به همسایگان آلیس می رسد و همسایگان وی نیز این بسته را به سایر همسایگان خود در گراف شبکه پخش می کنند تا به دست همه برسد.



شکل ۱۳: امضای بلاک تراکنش

بعد از دریافت این بلاک توسط سایرین آنها بررسی اعتبار تراکنش را به این نحو انجام می دهند مطمیئ شوند که ۶ BTC قبلا توسط آلیس خرج نشده باشد. واز طرفی امضا با کلید عمومی A انجام شده باشد

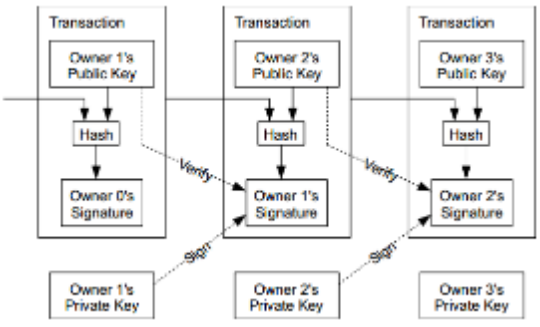
که تصدیق اصالت امضای A را شامل می شود. بعد از بررسی توسط سایر کاربران در بازی زمانی ده دقیقه با اپدیت تراکنش ها در غالب زنجیره بلاک حدف شدن ۶ BTC از شبکه تایید می شود.



شکل ۱۴: مرحله تایید تراکنش و خروجی نهایی

۵.۳ ساختار بلاک تراکنش ها [۱]

در حقیقت تراکنش ها در بیت کوین تعریف دنباله از امضای های رقمی هستند که هر مالک به وسیله امضایی که روی هش تراکنش قبلی و کلید عمومی مالک بعدی انجام می دهد سکه را به مالک بعدی منتقل می کند.

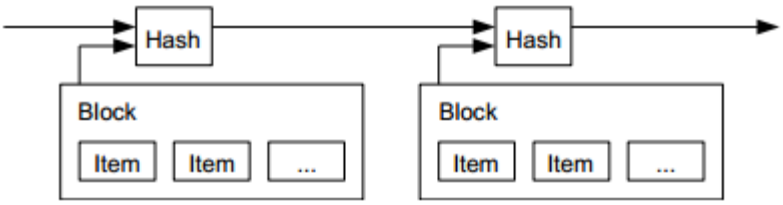


شکل ۱۵: ساختار بلاکی تراکنش ها[۱]

مسئله ای که با وجود این ساختار نمود پیدا می کند نحوه کنترل خرج شدن پول و ممانعت از خرج کردن مجدد آن توسط گره های متقلب است که برای اینکار این راه حل به ذهن می رسد که نیاز به یک نهاد مرکزی است اما همانطور که بیان کردیم در پروتکل بیت کوین به دنبال این هستیم که هرکس بانک خودش باشد و هیچ نهاد مرکزی نداشته باشیم از این رو در این شبکه هر تراکنش باید عموما اعلام شود و زمان آن در تاریخچه ای ذخیره شود که همان زنجیره بلاک نامیده می شود.

۶.۳ سرور برچسب زمانی [۱]

راه حل پیشنهادی به این نحو است که از یک سرور برچسب زمانی استفاده می شود که به این نحو عمل می کند که مقدار درهم سازی شده بلاک ها را دریافت می کند که باید برچسب زمانی بخورند و آنها را عموما منتشر می کند.در حقیقت هر برچسب زمانی شامل برچسب زمانی مقدار درهم سازی شده قبلی نیز به شکل۱۶ است که همه این مقادیر در غالب زنجیره ای مطرح می شوند.



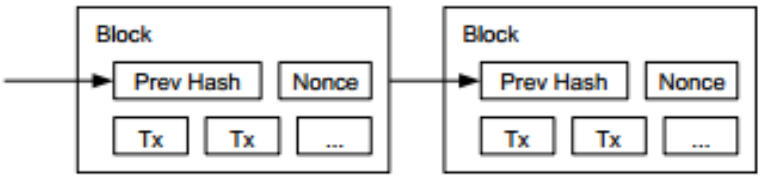
شکل ۱۶: تراکنش ها و برچسب زمانی[۱]

۱.۳ اثبات کاری[1] [۱]

برای پیاده سازی یک سرور برچسب زمانی توزیع شده در شبکه نظیر-به-نظیر نیاز به یک سیستم اثبات کاری داریم،پیاده سـازی به کمک افزایش مقدار نانس در بلاک تا جایی که مقدار هدف پیدا شود انجام می گیرد.

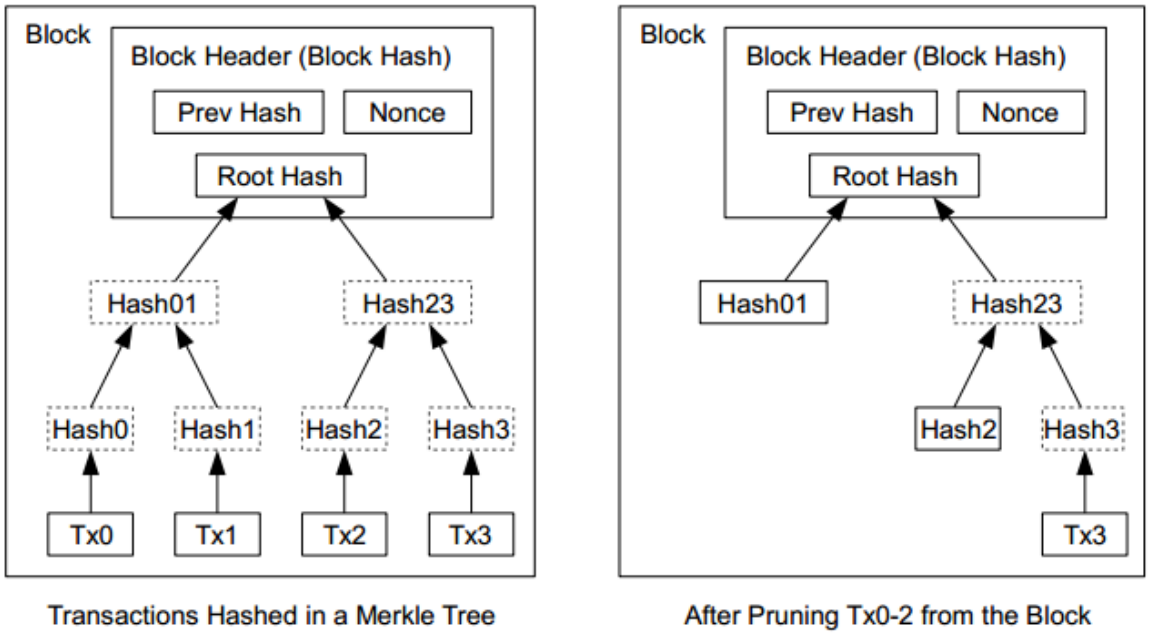
[1] Proof of work

مقدار هدف بلاک در هم سازی شده ای است که تعداد صفر لازم را داشته باشد یا به تعبیر دیگر از مقدار خاصی کمتر باشد.



شکل ۱۷: نحوه تولید زنجیره بلاک[۱]

به منظور نگه داری سوابق تراکنش ها اگر قرار باشد در هر بلاک کلیه این اطلاعات ذخیره شود با مشکل کمبود فضای ذخیره سازی مواجه می شویم از این رو از ساختار درخت مرکل[1] برای حل این مشکل همانطور که در شکل۱۸ آمده است استفاده می شود.در این ساختار تنها یک مقدار درهم سازی شده ریشه دخیره می شود و سایر مقادیر هرس می شوند.



شکل۱۸: استفاده از درخت مرکل[۱]

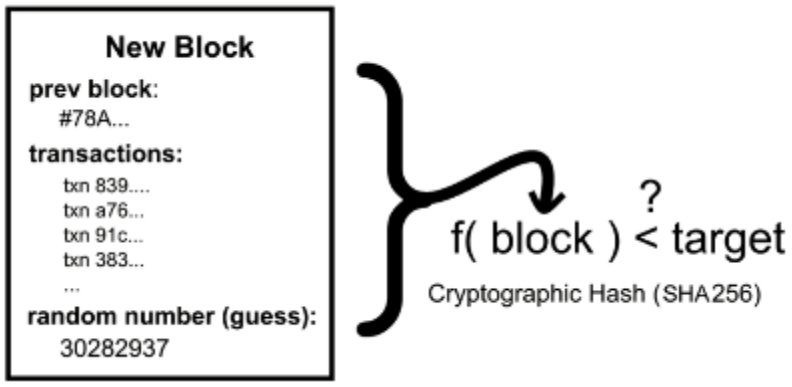
[1] Merkle Tree

اندازه سرآیند بلاک در حدود ۸۰ بایت است و اگر فرض کنیم در هر ده دقیقه یک بلاک تولید شود بنابراین برای یک سال این اندازه برابر خواهد شد با:

80 bytes * 6 * 24 * 365 = 4.2MB

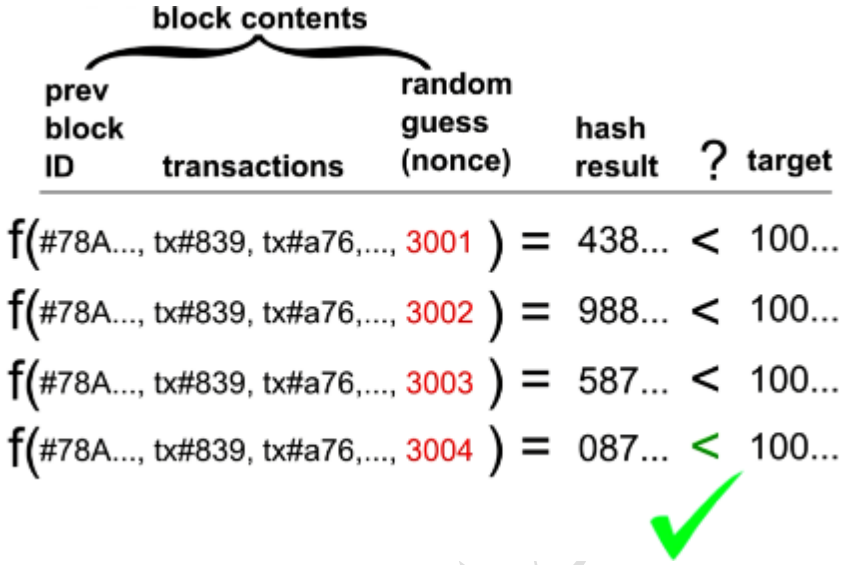
که با توجه به حجم معمول یک حافظه اصلی به اندازه 2GB در سال ۲۰۰۸ و با درنظر گرفتن قانون مور در مورد میزان رشد سخت افزار ها در سال به میزان 1.2GB مشهود است که فضای ذخیره سازی این میزان داده یک چالش در این شبمه نخواهد بود حتی اگر قرار باشد تمامی این مقدار داده در حافظه ذخیره شود.

برای درک مفهوم تولید این مقدار نانس با یک مثال سیستم اثبات کاری را شرح می دهم.همانطور که در شکل۱۷ مشخص شده است و در شکل ۱۹ نیز به تصویر کشیده شد در مرحله اثبات کاری یک تابع در همسازی که مقادیر ورودی آن شامل مقدار درهم سازی شده بلاک قبل،شناسه تراکنش های در حال تایید و یک مقدار نانس است باید توسط گره های استخراج کننده اعمال شود تا مقدار خروجی این تابع درهمسازی f کمتر از مقدار هدف باشد،اگر کسی توانست با آزمودن های بسیار مقدار نانسی را تولید کند که مقدار خروجی از هدف کمتر شود این مقدار را در غالب تراکنشی به اطلاع دیگران می رساند. هدف در محاسبات تا ۲۰۱۶ مین بلاک تعیین شده است و اگر بیش از دو هفته طول بکشد تا بلاک ۲۰۱۶ امین تولید شود هدف بالا می رود در غیر این صورت پایین می آید.



شکل ۱۹: نحوه عملکرد تابع درهمسازی[۱]

به عنوان مثال در شکل ۲۰ گره ای اقدام به پیدا کردن نانس با توجه به هدف ۱۰۰ و مقادیر درهمسازی شده بلاک قبل،شناسه تراکنش های در حال تایید می کند و می تواند به مصرف انرژی و داشتند مقداری شانس این مقدار نانس را پیدا کند.



شکل ۲۰:پیدا کردن نانس[۱]

حال این گره که توانست این مقدار نانس را پیدا کند در قالب بلاکی به شکل۲۱ این تراکنش را منتشر می کند

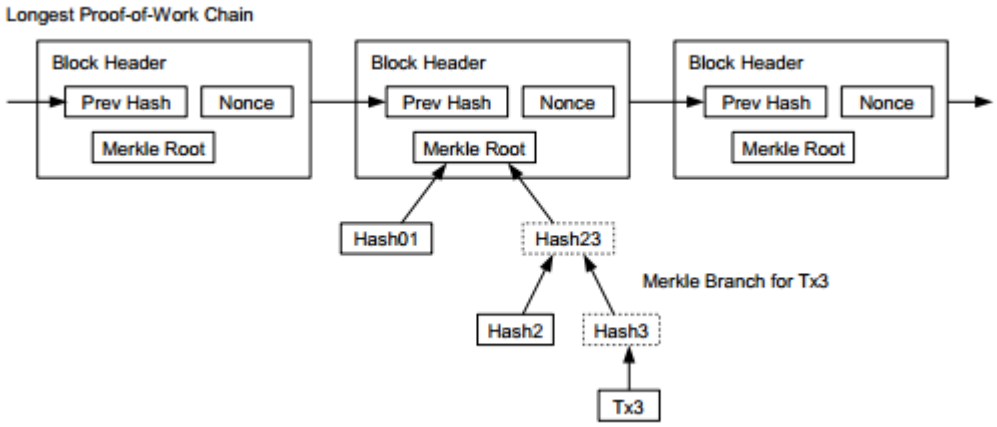
Hash: 000000000043a8c0fd1d6f726790caa2a406010d19efd2780db27bdbbd93baf6
Previous block: 00000000001937917bd2caba204bb1aa530ec1de9d0f6736e5d85d96da9c8bba
Next block: 00000000000036312a44ab7711afa46f475913fbd9727cf508ed4af3bc933d16
Time: 2010-09-16 05:03:47
Difficulty: 712.884864
Transactions: 2
Total BTC: 100
Size: 373 bytes
Merkle root: 8fb300e3fdb6f30a4c67233b997f99fdd518b968b9a3fd65857bfe78b2600719
Nonce: 1462756097

Input/Previous Output	Source & Amount	Recipient & Amount
N/A	Generation: 50 + 0 total fees	Generation: 50 + 0 total fees
f5d8ee39a430...:0	1JBSCVF6VM6QjFZyTnbpLjoCJ...: 50	16ro3Jptwo4asSevZnsRX6vf...: 50

شکل ۲۱:بلاک تراکنش پیدا کردن نانس[۲]

بعد از انتشار عمومی ای بلاک، این بلاک توسط سایر گره ها برررسی و تایید می شود اگر مقدار نانس درست باشد و خروجی کمتر از هدف را تولید کند و تمام تراکنش های داخل آن معتبر باشند. سپس

سایرگره ها تایید کردن بلاک تولید شده را با کار بر روی بلاک بعدی اعلام می کند که در آن بلاک جدید تولید شده به عنوان مقدار درهمسازی شده قبلی[1] مطرح می شود. هر گره تنها کافیست یک کپی از سرآیند بلاک های طولانی ترین زنجیره اثبات کار را ذخیره کند،که این کار را می تواند با درخواست از کاربران دیگر دریافت می کند سپس به کمک درخت مرکل تا برچسب زمانی پیش رود. هر کاربر نمی تواند تراکنش خودش را بررسی کند اما می تواند با بررسی بلاک هایی که بعدا اضافه می شود متوجه شود که بلاک وی تایید شده است یا نه.



شکل ۲۲:زنجیره اثبات کاری[۱]

بلاک تراکنش پیدا کردن نانس شامل دو تراکنش است بخش اطلاعات نانس و بخش پاداش. پاداشی که برای تولید بلاک جدید داده می شود باعث می شود که تمامی گره ها به دنبال درستکاری باشند چرا که به سود آنهاست، حتی برای مهاجمان!

مقدار این پاداش در ابتدا شروع کار شبکه بیت کوین 50BTC بود اما در حال حاضر این مبلغ 25BTC است.مقدار پاداش هر هر ۲۱۰هزار بلاک نصف می‌شود که حدودا می شود هر چهار سال که اطلاعات آن در جدول ۲ آمده است:

جدول ۲:بلاک تراکنش پیدا کردن نانس

سال	مبلغ پاداش(BTC)

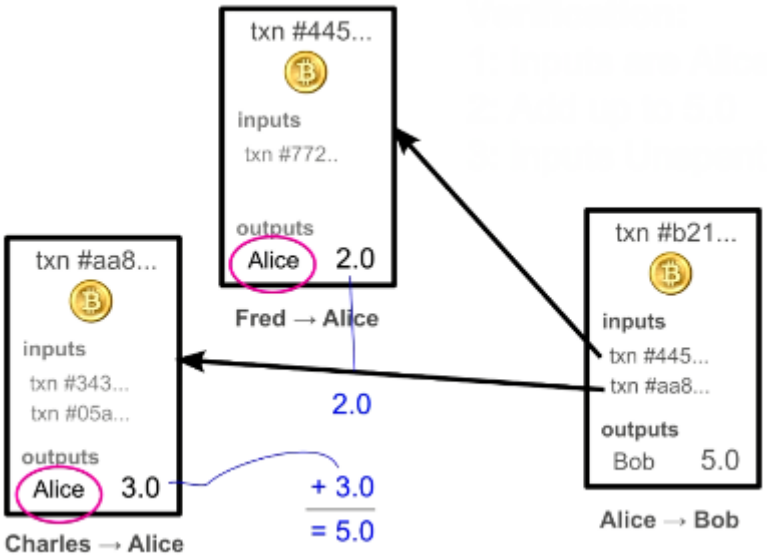
[1] previous hash

۲۰۱۳-۲۰۰۹	۵۰
۲۰۱۷-۲۰۱۳	۲۵
۲۰۲۱-۲۰۱۷	۱۲,۵
۲۰۲۵-۲۰۲۱	۶,۲۵
۲۰۲۹-۲۰۲۵	۳,۱۲۵
۲۰۳۳-۲۰۲۹	۱,۵۶۲۵
۲۰۳۷-۲۰۳۳	۰,۷۸۱۲۵
...	...

امکان تغییر بلاک بدون تکرار عمل اثبات کاری وجود ندارد.زنجیره بلاک ها که وسیله گره های درستکار تولید شده است بسیار طولانی می شود از این رو مهاجمی که قصد تقلب دارد برای انجام تقلب مجبور است که اثبات کاری را بر روی همه بلاک های این زنجیره مجددا انجام دهد و بتواند از گره های درستکار پیشی بگیرد هرچه توان محاسباتی مهاجم کمتر باشد به صورت نمایی توان وی برای جایگزین کردن بلاک های تقلبی کاهش پیدا می کند.

۲.۳ ارزیابی اعتبار تراکنش ها [۱]

در این قسمت اینکه چگونه اعتبار تراکنش های بیت کوین بررسی می شود با ذکر یک مثال بیان می شود، فرض کنید گره ها می خواهند اعتبار تراکنش شکل ۲۳ را بررسی کنند:



شکل ۲۳:بررسی اعتبار تراکنش

در اینجا باید براساس تراکنش شماره #b21 سه نکته را مورد توجه قرار بدهند اول اینکه ورودی های تراکنش شماره #b21 باید متعلق به آلیس باشد، دوم اینکه جمع مبالغ ورودی ها برابر با ۵BTC باشد و سوم اینکه سکه ها ورودی قبلا خرج نشده باشند. در واقع در هر تراکنش باید این نکات مورد توجه قرار گیرد بررسی پیش نیاز اول و دوم به راحتی به کمکم بلاک تراکنش و ورودی های آنها میسر می شود اما در مورد پیش نیاز سوم کار قدری پیچیده تر می شود. برابری بررسی اینکه سکه ها در قالب صورت حساب ها خرج نشده باشد نیاز به مراجعه به زنجیره بلاک و بررسی سوابق تراکنش های ورودی است. در شکل ۲۴ یک نمونه از زنجیره بلاک نمایش داده شده است.

Transactions

Transaction	Fee	Size (kB)	From (amount)	To (amount)
8d4a198310...	0	0.142	Generation: 50 + 0.004 total fees	1GjUMt4pGHeAZitDj9ZiZaRztRL5JKtKR: 50.004
2175f7f1fc...	0	0.258	1KVi9u1G6XL6dRsEcukwpTDX9F2fMdD2ct: 5	1HMuf6zcPEuWfkBENpZu3KSzrW4nvWfexH: 4 1CBr5J9vPMVzf5S22vdMUXkcLw8p4w7JgU: 1
9d869c9b24...	0	0.259	1KUCp7YP5FP8ViRxhfszSUJCTAajK6viGy: 50.04200002	17nMZ3de59A73KgmoECWBN1gun1MVSZemQ: 49.57360824 1HTxTCDjDEW8smt3FCeiuf34ig8ua3vfvk: 0.46839178
45c8492c11...	0	0.271	17hzyiu9sDkybgsrZ6SSVPQ6Euyp9GkM7x: 50.0005 1DXNEgaXZy4NqvTahTu6QQCLy9A3jv8Vh8: 50	1VayNert3x1KzbpzMGt2qdqrAThiRovi8: 100.0005
4aldd2ae5e...	0	0.258	1H7MMoemmmefft5LfHHWT57ZLae51CcobX: 12.7	1AUedJf6iMEUnquWvCNUaVui1FUEBi86XZ: 12.68 1GHd3GEUdAzUra5DygSXtuarSdjPEn9ZN6: 0.02

شکل ۲۴:بخشی از زنجیره بلاک

۴

فصل چهارم:

حمله double-spending

۱.۴ یک چالش

فرض کنید تراکنش ها گره به گره در شبکه منتقل شوند

شکل ۲۵:انتقال دو تراکنش

در شـکل بالا در سـمت راسـت دو تراکنش در شـبکه ارسال می شوند ،با اینکه در سمت چپ تراکنش پایینی زودتر ارسال می شود اما در سمت راست مشاهده می کنیم که تراکنش بالایی زودتر به برخی گره ها می رسـد که این مسئله در اثر ساختار و توپولوژی شبکه پیش می آید و این نشان می دهد که هیچ تضـــمینی وجود ندارد که همان ترتیبی که تراکنش ها را دریافت می کنیم همان ترتیب زمانی تولیدی آنها باشـد از طرفی نمی توان تنها به برچسـب زمانی تراکنش ها اعتماد کرد زیرا که گره ارسـال کننده تراکنش می تواند تقلب کند و زمان نادرستی را در تراکنش درج کند.

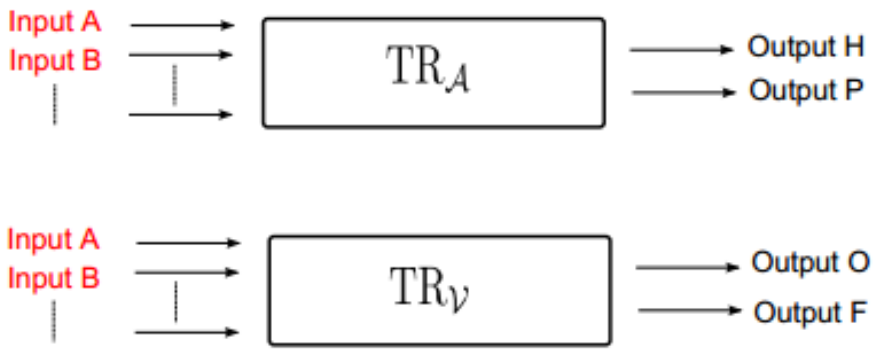
۲.۴ پرداخت های سریع در بیت کوین

در تراکنش های شبکه بیت کوین ایده آل ترین حالت این است که فروشنده صبر کند تا تراکنش تایید شـود سـپس به مشتری خدمات بدهد که این نوعی پرداخت کند در شبکه بیت کوین است اما در روش پرداخت سـریع اسـتفاده از برچسـب زمانی نمی تواند جلوی حمله double-spending را بگیرد و تا version 0.5.2 پروتکل بیت کوین هیچ تدبیری برای آن اندیشیده نشده بود.[۲]

۳.۴ مدل حمله

برای بیان حمله double-spending ابتدا فرض های حمله را به شرح ذیل عنوان می کنیم: [۲]

- فرض A قابلیت ملحق شدن به شبکه بیت کوین را دارد.
- فرض می کنیم که A متقلبی است که سعی دارد سرویس را از V بدون خرج بیت کوین بگیرد.که برای این کار از double-spending استفاده می کند.
- A تنها قادر است به تعداد محدودی گره عضویت داشته باشد(در شبکه بیت کوین محدودیتی در تعداد عضویت نداریم)
- A قدرت محاسباتی بالایی ندارد.
- A دسترسی به کلید های محرمانه و سیستم فروشنده ندارد.
- وقتی تراکنشی تایید شد دیگر A نمی تواند آن را تغییر دهد.
- A کلید عمومی V را برای ارسال محرمانه دارد.
- فرض سایر گره ها درستکار هستند، نحوه دستکاری بلاک ها برای DS به شکل ۲۶ می باشد:



شکل ۲۶: دو تراکنش (بالایی معتبر و پایینی جعلی)

۴.۴ شرایط لازم برای حمله [۲]

در صورتی که تراکنشهایی در شبکه موجود باشد که ورودی هایشان دقیقا یکی باشد تنها یکی از آن دو معتبر خواهد بود.در جدول ۳ نماد های این مدل حمله معرفی شده اند.

جدول ۲:نماد های مدل حمله

T_i^v	زمانی است که گره i تراکنش TR_V را دریافت کند.
T_i^A	زمانی است که گره i تراکنش TR_A را دریافت کند.
T_v^v	زمانی است که گره V تراکنش TR_V را دریافت کند.
T_v^A	زمانی است که گره V تراکنش TR_A را دریافت کند.
δt_{AV}^V	زمانی که طول می کشد تا تراکنش TR_V از A به Vبرسد.
δt_{HV}^A	زمانی که طول می کشد تا تراکنش TR_A از H به Vبرسد.

پیشنیاز اول:در این مدل اگر $T_v^A > T_v^v$ آنگاه حمله موفق خواهد بود ، اما اگر $T_v^A < T_v^v$ آنگاه V در ابتدا TR_A را دریافت می کند و آن را درمخزن حافظه قرار می دهد. سپس هنگامی که TR_V را دریافت می کند آن را نمی پذیرد و از Aدر خواست می کند تا دوباره پرداخت را انجام دهد.

پیشنیاز دوم:TR_A تایید شود و در زنجیره بلاک قرار گیرد.

برای اینکه پیشنیاز اول براورده شود فرض کنید که گره هایی مانند H وجود دارند که به A کمک می کنند(که حتی می توانند روی یک ماشین باشند) و تاخیر میان Aو H زیاد نباشد. با این فرض A در زمان T_V تراکنش TR_V را به V ارسال می کند و سپس در زمان T_A تراکنش TR_A را به H ارسال می کند بنابر این:

$$T_A = T_V + \Delta t$$

که خواهیم داشت:

$$T_v^A - T_v^v \approx T_A + \boldsymbol{\delta t_{HV}^A} - (T_V + \delta t_{AV}^V)$$

$$\approx \Delta t + \boldsymbol{\delta t_{HV}^A} - \boldsymbol{\delta t_{AV}^V}$$

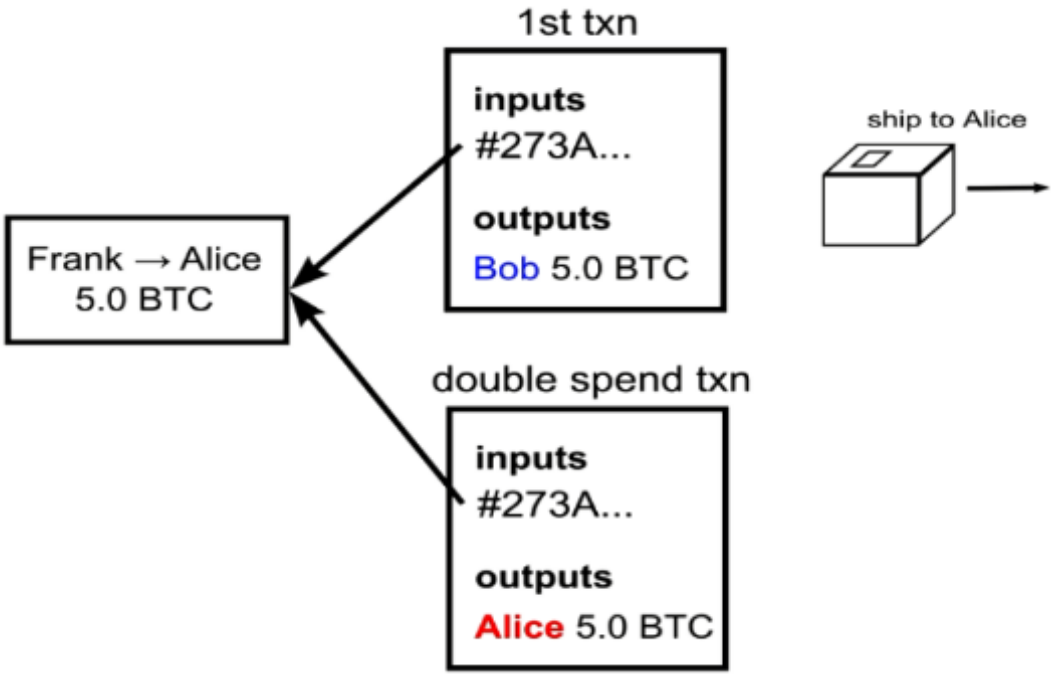
باید به این نکته توجه کرد که فرض این است که H همسایه V نیست و حداقل یک گام بین آنها فاصله است در صورتی که A همسایه Vاست و هیچ گونه ازدحامی در مسیر آن دو وجود ندارد.از این روز پیشنیاز اول یعنی $T_v^A > T_v^v$ با فرض $\Delta t > 0$ارضا می شود.

در مورد پیش نیاز دوم از آنجایی که H وV به احتمالا زیاد همسایه های متفاوتی دارند پیام هایی که منتشر می شونددر شبکه پخش می شوند به نحوی که گره ها مختلف TR_Aو TR_V را در مخزن حافظه خود دارند.در اینجا به دنبال تخمین احتمالی هستیم که ابتدا TR_Aتایید می شود.با فرض اینکه در زمان t_0 هر دو تراکنش TR_Aو TR_V در شبکه پخش شده باشند.از آنجایی که در شبکه تاخیر وجود دارد و ممکن است مسیر های تراکنش های TR_Aو TR_Vمتفاوت باشد از این رو یکی از آنها زودتر به دست گره های مختلف می رسد که بسته به محل گره ترتیب دریافت متفاوت خواهد بود.

با محاسبات آماری متعدد که در *[2]* آمده است ثابت می شود با افزایش تعداد گره هایی در شبکه که TR_Aزودتر TR_V از دریافت می کنند به وسیله استفاده از حداکثر تاخیر ممکن میتوان احتمال موفقیت متقلب بالا رود.

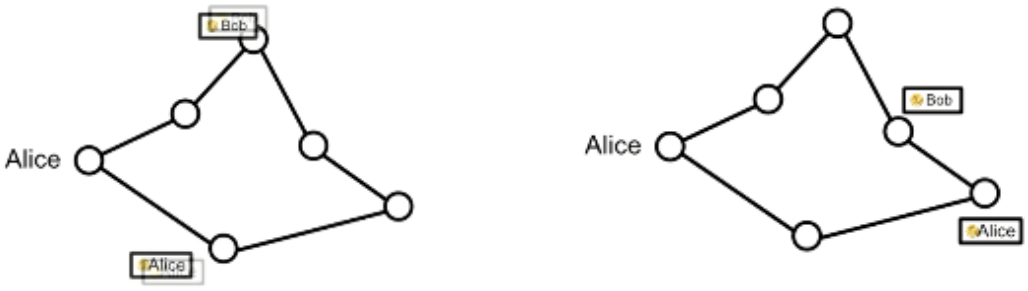
۵.۴ سناریو حمله

برای درک بهتر این حمله سناریوای فرض را در اینجا توضیح می دهیم،در شکل آلیس به عنوان متقلب سعی می کند ضمن ارسال تراکنش $5BTC$ به باب همزمان با تولید بلاک تراکنش نامعتبر این مبلغ را به خودش برگرداند.



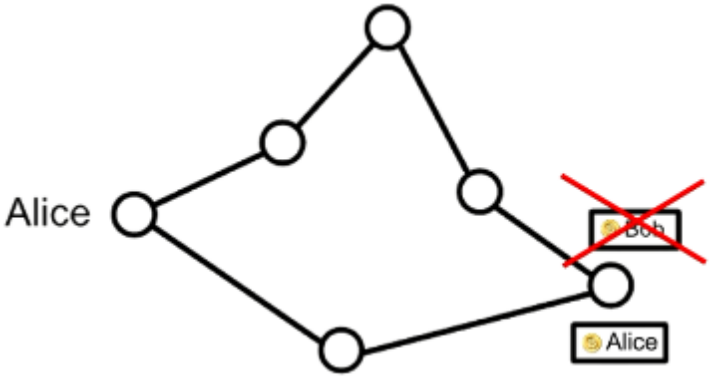
شکل ۲۷: سناریو تقلب با دو تراکنش

حال آلیس سعی می کند از چالش مطرح شده در ابتدای این فصل سواستفاده کند و به شکل ۲۸ عمل کند:



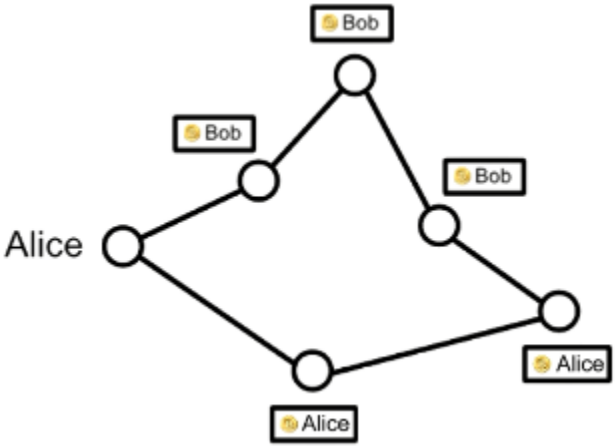
شکل ۲۸: ارسال دو تراکنش

در اثر عدم دریافت تراکنش ها مطالبق با زمان تولید گره ها در نگاه اول تراکنشی را که زودتر دریافت می کنند را قبول می کنند و دیگری را ظاهرا معتبر نمی دانند.



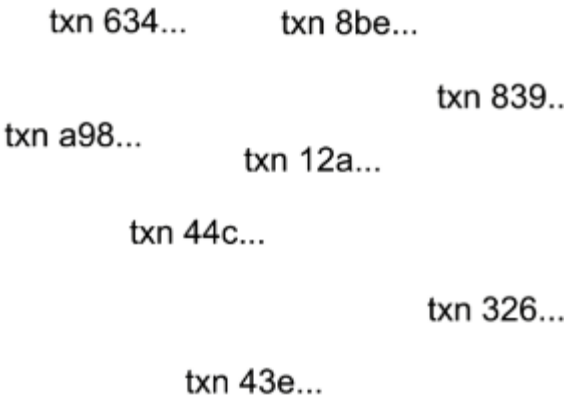
شکل۲۹: دریافت تراکنش دریافتی نخست

در نتیجه تراکنش ها در شبکه به شکل ۳۰ در می آیند:



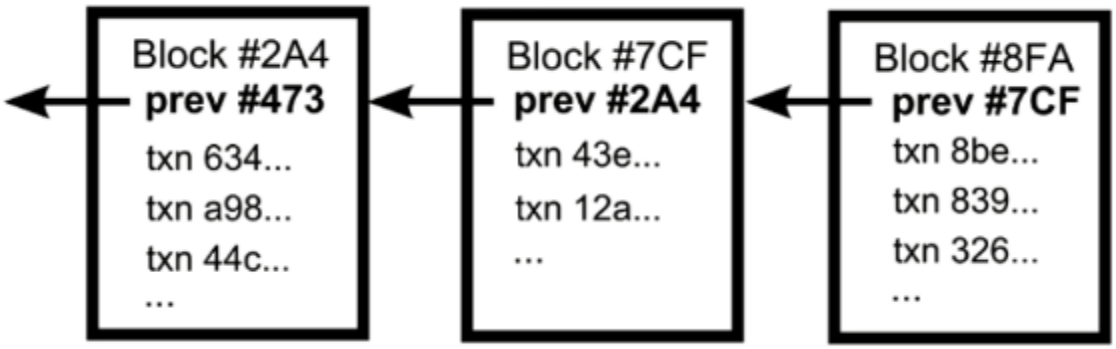
شکل۳۰: تناقض در تراکنش ها درشبکه

حال این سوال پیش می آید که اگر قرار باشد در شبکه چنین تناقضی پیش بیاید که تراکنش ها هیچ اعتباری نخواهند داشت،اما اینگونه نیست، به منظور تعیین ترتیب تراکنش ها آنها باید در قالب بلاک هایی قرار بگیرند.



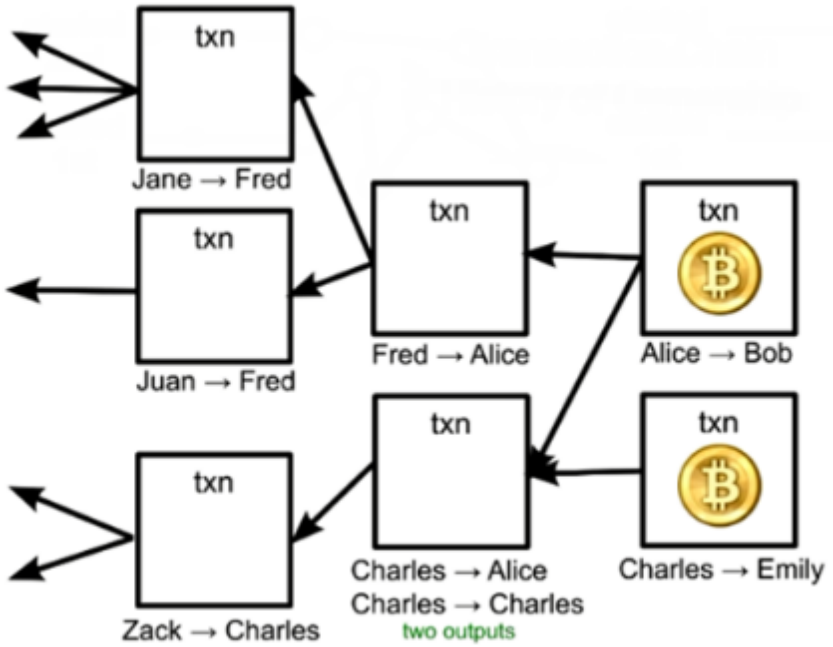
شکل ۳۱: تراکنش ها بدون وجود ترتیب مشخص

که این تراکنش ها با توجه به مفهوم زنجیره بلاک و درهم سازی بیان شده در قالب مرتب مانند شکل قرار می گیرند:



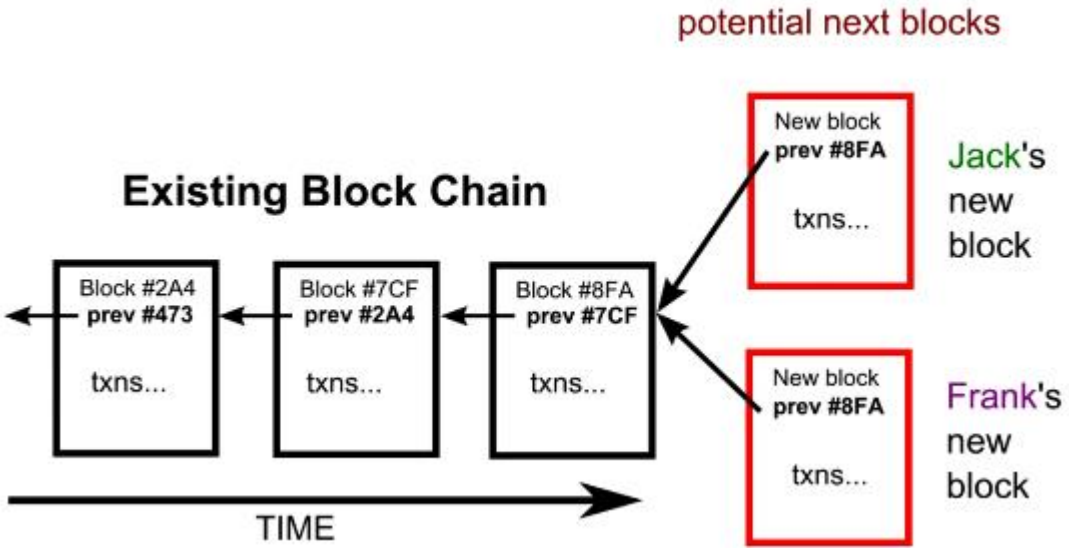
شکل ۳۲: نمونه ای از زنجیره بلاک

همانطور که در شکل ۳۲ مشاهده می کنید زنجیره بلاک در واقع برای مشخص کردن ترتیب تراکنش هاست.در حالی که زنجیره تراکنش ها برای مشخص کردن نحوه تغییر مالکیت سکه های شبکه است.



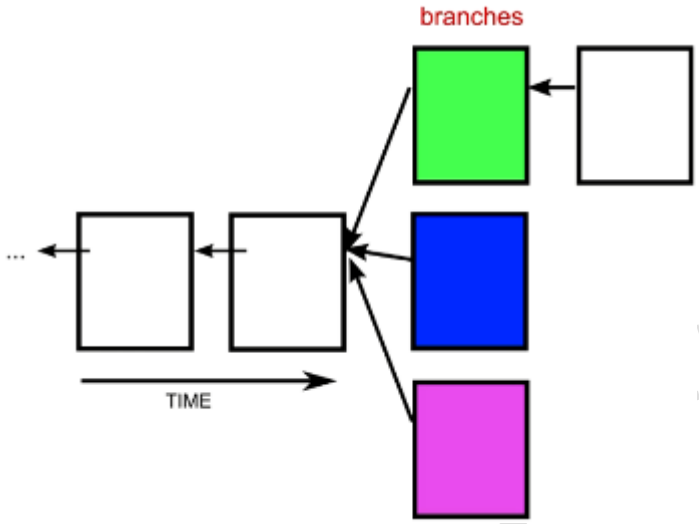
شکل ۳۳: نمونه ای از زنجیره تراکنش ها

از آنجایی که افراد متعددی می توانند همزمان بلاک را ایجاد کنند چندین انتخاب برای بلاک می تواند وجود داشته باشد به عنوان مثال در شکل ۳۴ دو بلاک متفاوت وجود دارد که می توانند پتانسیل بلاک بعدی شدن را داشته باشند.



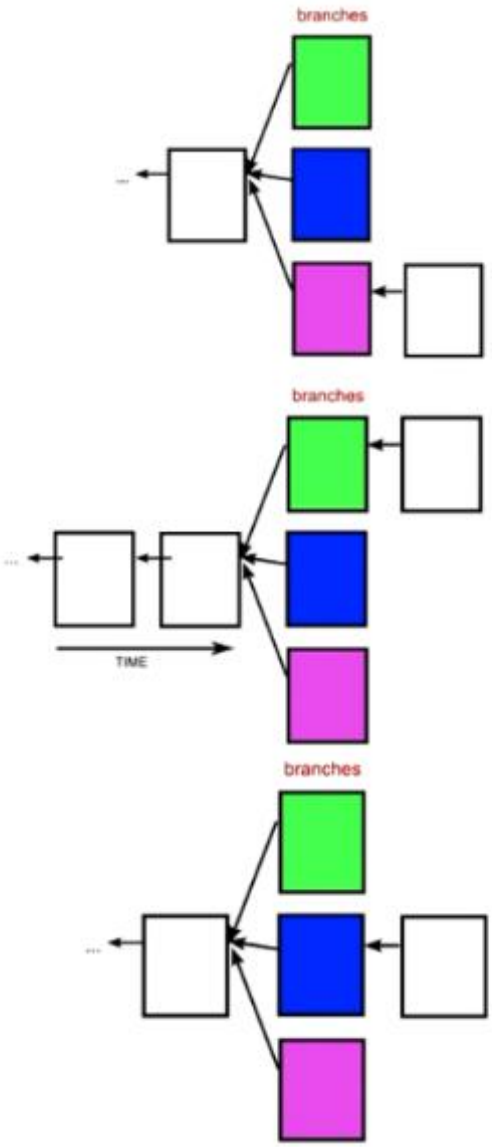
شکل ۳۴: بلاک های متفاوت برای قرارگیری در زنجیره بلاک

زمانی که چنین اتفاقی در شبکه می افتد هر گره به ترتیبی خاص تراکنش ها را دریافت می کند هر گره اولین تراکنش دریافتی را مورد توجه قرار می دهد به عنوان مثال در شکل ۳۵ بلاک بالایی نخستین یلاک دریافتی این گره بوده است.



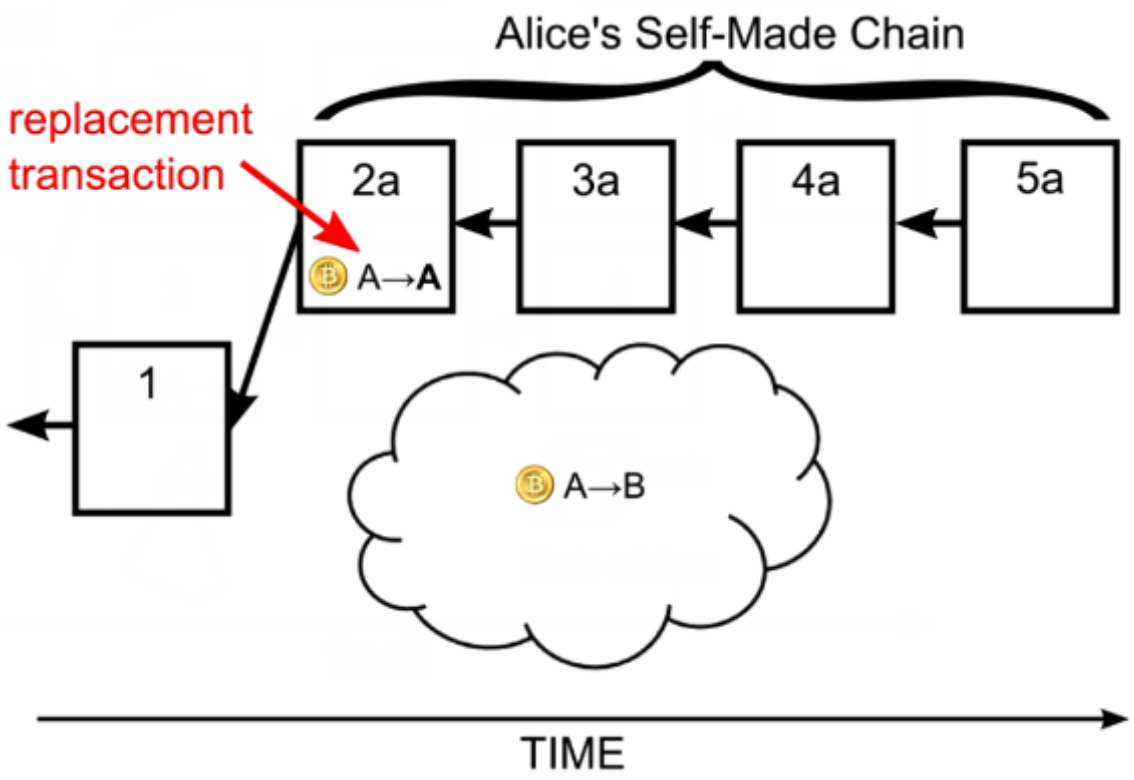
شکل ۳۵: سه بلاک متفاوت برای قرارگیری در زنجیره بلاک

اما ممکن است سایر گره ها با ترتیبی متفاوت تراکنش ها را دریافت کنند از این رو زنجیره ها متفاوتی امکان ایجاد پیدا خواهد کرد که در شکل ۳۶ به تصویر کشیده شده است.



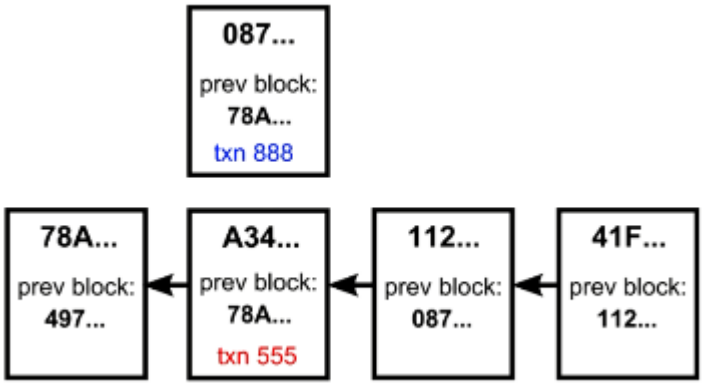
شکل ۳۶: ترتیب مختلف دریافتی در زنجیره بلاک توسط گره ها

اگر قرار باشد هر کسی به ترتیب دریافتی روی اولین تراکنش کار کند این سبب تناقض در شبکه می شود از این رو قرار داد می شود که کلیه گره ها روی بزرگترین زنجیره کار کنند. حال اگر مهاجم بخواهد تقلب کند سعی می کند یک انشعاب بزرگتری تولید کند که این مبلغ به خودش پرداخت شده است.



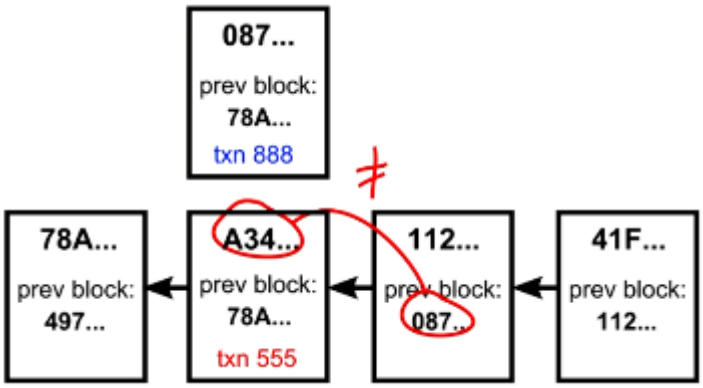
شکل ۳۷: تولید انشعاب جایگزین

اگر قرار باشد تقلب به درستی انجام شود مهاجم باید بتواند انشعابی بلندتر تولید کند که بتواند انشعاب دیگر را نامعتبرجلوه دهد.به عنوان مثال یعنی باید بتواند در شکل ۳۸ این بلاک جایگزین را ایجاد کند یعنی بتواند با اثبات کاری روی تراکنش *txn888* مقدار نانسی را تولید کند که بتواند تراکنش *txn555* را جایگزین آن کند.



شکل ۳۸: تولید بلاک جایگزین

اما نکته ای که وجود دارد این است که به صرف پیدا کردن نانس در یک بلاک این جایگزینی قابل اعمال نیست و باید در کلیه زنجیره جایگزینی انجام شود که کاری بس دشوار است.



شکل ۳۹: عدم موفقیت تولید بلاک جایگزین

۶.۴ استفاده از بازه شنود [۲]

با استفاده از بازه زمانی شنود و پیاده سازی ناظرهایی و تولید پیام های هشدار می توان DS را تشخیص داد. در حالت عادی زمانی که برنامه بیت کوین روی یک گره، دو تراکنش با ورودی های یکسان دریافت می کند پیام خطا تولید می کند در حالی که کاربر این پیام را نشان نمی دهد. بنابراین می توان با تعریف یک بازه شنود[1] در چند ثانیه قبل از اینکه V خدماتی را به A بدهد تمام تراکنش های ورودی را مانیتور کند و اگر DS را تشخیص داد جلوی آن را بگیرد.

اما این راه حل یک ایراد دارد چرا که همانطور که در فصل قبل گفتیم می توان با درنظر گرفتن

$$T = \boldsymbol{T_v^A} - \boldsymbol{T_v^v}$$

و بیشتر کردن زمان T نسبت به مقدار آستانه ی بازه شنود بازهم V را فریب داد.

[1] Listening Period

۵

فصل پنجم:
چالش های بیت کوین

۱.۵ چالش ها

از جمله چالش هایی که بیت کوین با آن درگیر است می توان به موارد ذیل اشاره کرد:

- مبادله ی بیت کوین با واحدهای معتبر پول
- استفاده در معاملات غیرقانونی و خلافکارانه
- استخراج بیت کوین نیازمند مصرف انرژی
- برخی اقتصاد دانان و بانکداران برجسته، رشد اقبال جهانی به بیت کوین را همانند حباب میدانند و در مورد تبعات آن هشدار می دهند.[۷]
- برخی اقتصاد دانان و بانکداران بیتکوین را یک واکنش قدرت گرفته از فناوری اطلاعات به نابسامانی های نظام مالی و پولی جهانی بشمار می آورند[۷]
- این ایده که تولید پول به مرور زمان کم می شود خوب است یا بد؟!
- سایر پول ها دولت یا سازمان هایی دارند که در صورت مشکل پاسخگو باشند اما بیت کوین چطور؟!

۶

فصل ششم

جمع‌بندی و نتیجه‌گیری

جمع‌بندی و نتیجه‌گیری

بیتکوین در سال ۲۰۰۹ توسط هکر یا هکرهایی ناشناس پا به عرصه وجود گذاشت .مهمترین ارز دیجیتالی رمز پایه همان اولین ارز دیجیتالی است و از آن با بیتکوین یاد میشود . پول از جمله ابزارهای اعمال کنترل برا قتصاد کلان کشورها و بخشی مهم از زندگی انسان هاست. طی دهه های گذشته تاکنون فناوری اطلاعات و ارتباطات به نظام بانکی خدمات بزرگی عرضه کرده است ،بانکداری الکترونیکی بهترین شاهد این مدعاست.اما بحران مالی سال ۲۰۰۸ مهر تاییدی بر دیدگاه اقتصاددانان به حاشیه رفته ای بود که ادعا داشتند نظام پولی و بانکی مبتنی بر دلار بی پشتوانه مشکلات ریشه ای دارد و بحران اقتصادی آمریکا را تهدید می کند. بررسی ها نشان میدهند ،مکانیزم خلق پول و دیگر اقدامات تورم‌زای بانک های مرکزی که اغلب منافع کوتاه مدت دولت ها را بر عقلانیت و ثبات بلندمدت مودنیاز بازار مرجع می دانند .

میتواند یکی از مهم ترین دلایلی باشد که برخی از هکرهای فعال اجتماعی[1] را به تکاپو واداشت تا با قدرت اندیشه و ایده های تازه به معماری یک نظام مالی جدید بپردازند.صاحبنظران ،دو آینده کاملا متناقض (شکست نظام بیتکوین یا تحقق نظام بیتکوین جهانی جدید) در مقابل بیتکوین را پیش بینی کرده اند.اما در هرصورت بیتکوین در طول پنج سال از آغاز وجودش آنقدر تاثیرگذار بوده است که مراکز سیاست پژوهی و دستگاه های اجرایی کشورها به مطالعه و مقرراتگذاری پیرامون آن بپردازند .آینده بیتکوین منوط به تاثیر و تاثر عوامل پیرامونی آن است.اما چه بیتکوین موفق به تحقق آینده مطلوب ایجادکنندگانش شود و چه کاملا از هم فرو پاشد،در برهه کنونی تاثیرپذیری نظم جهانی از جنبش های فناورانه شواهد تاریخی به خود گرفته است ،بنابراین مراکز سیاست پژوهی دنیا و کشورمان باید به طور مداوم تغییرات فناورانه اینچنینی را رصد کنندتا در صورت نیاز با تدوین مقررات سیاستی به موقع منافع کشورمان حفظ شود.

مطالعه سه کشور آمریکا ،آلمان و چین نشان میدهد ،پدیده بیتکوین در این کشورها در سطح اجرایی و با تنظیم مقررات از سوی قوه مجریه حل و فصل شده است .قوه مقننه کشور آمریکا پس از بررسی بیتکوین به این نتیجه رسیده است که بیتکوین نیاز به تدوین قانون جدید ندارد و قوه مجریه این کشور باید در چارچوب قوانین و مقررات پیشین ،پدیده بیتکوین را مدیریت کند.قوه مقننه آلمان نیز بر کار قوه مجریه

[1] . Hacktivists

نظارت دارد و یکی از نمایندگان مجلس ملی آلمان با طرح برخی سوالات از قوه مجریه کشور آلمان حل وفصل وضعیت حقوقی بیتکوین در چارچوب قوانین موضوعه (قوانین مصوب پیشین) را درخواست کرده است .قوه مجریه کشورهای آلمان ،آمریکا و چین ارزهای دیجیتالی همچون بیتکوین را کالا محسوب کرده اندو قوانین موضوعه مربوط به کالا را از نظر مالیاتی و در مراودات مالی بر آن جاری می‌دانند . قوه مجریه کشور آمریکا بر تبادل کنندگان بیتکوین قوانین مربوط به انتقال دهندگان پول[1] را جاری می‌داند.[۷]

بیت کوین امکان پرداخت‌های بسیار کم هزینه را فراهم می‌کند. شبکه بیت کوین سیستم کنترل کننده متمرکز ندارد و توسط هیچ ارگان یا نهاد دولتی اداره نمی‌شود. بیت کوین دارای ویژگی های استقلال،امنیت،حافظ حریم خصوصی،قابلیت پرداخت آفلاین،قابلیت انتقال،قابلیت خرد شدن است . زمان متوسط تایید هر انتقال بیت‌کوین، تقریباً ده دقیقه است. انتقال پول از یک نقطه به نقطه دیگر در تمام شبکه اطلاع رسانی شده و تمام نقاط از آن آگاه خواهند شد.

[1] . money Transmitters

۷

فصل هفتم

مسائل باز و پروژه پیشنهادی کارشناسی ارشد

۱.۷ مسائل باز

- حذف شده

۲.۷ پروژه کارشناسی ارشد

- حذف شده

منابع و مراجع

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." *Consulted* 1.**2012** (**2008**): 28.

[2] Karame, Ghassan O., Elli Androulaki, and Srdjan Capkun. "Double-spending fast payments in bitcoin." Proceedings of the 2012 ACM conference on Computer and Communications Security. ACM, (**2012**).

[3] Murdoch, Steven J., and Ross Anderson. "Security protocols and evidence: Where many payment systems fail." Proceedings of Financial Cryptography and Data Security (**2014**)

[4] Kroll, Joshua A., Ian C. Davey, and Edward W. Felten. "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries." Proceedings of WEIS. Vol. 2013.(**2013**)

[5] Eyal, Ittay, and Emin Gün Sirer. "Majority is not enough: Bitcoin mining is vulnerable." arXiv preprint arXiv:1311.0243 (**2013**).

[6] Bradbury, Danny. "The problem with Bitcoin." *Computer Fraud & Security* 2013.11 (**2013**): 5-8.

[۷] بیتکوین؛ ابزاری نوین در نظام پرداخت های الکترونیکی، مرکز پژوهش های مجلس شورای اسلامی،۱۳۹۳