Electronic cash payment systems

Chapter 6

Contents

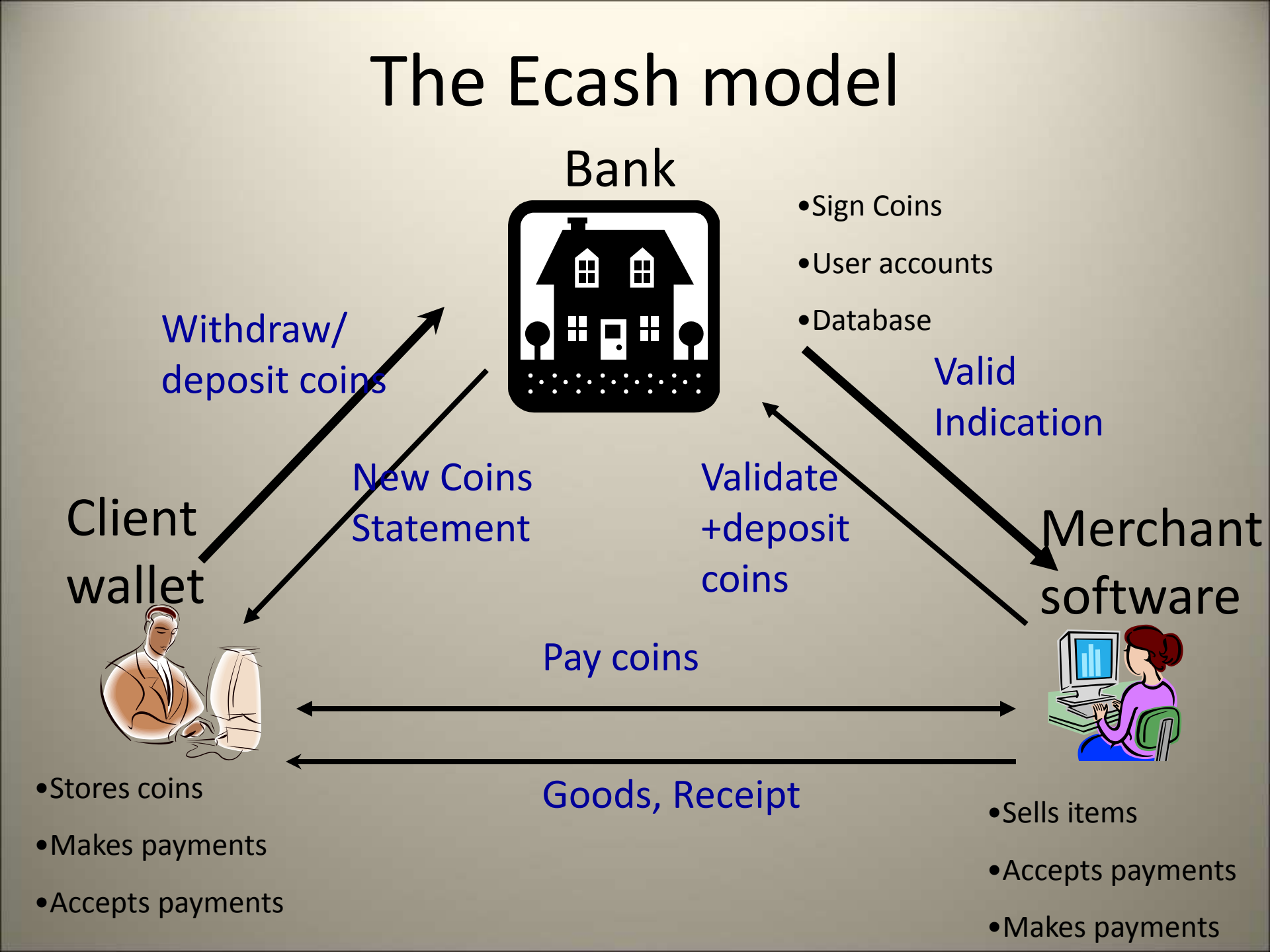
Cash

- Acceptability
- Guaranteed payment
  - No risk that the payment will not be honored at a later stage
- No transaction charges
  - No authorization required
  - No communications traffic or charges
- Anonymity

Ecash

- David Chaum
  - ”the father of digital cash”
- The bank cannot know the serial numbers of coins that clients withdraw.
- The coins can be spent anonymously with a merchant,
  - Collusion between both the bank and merchant will fail to identify the spender.

The Ecash model



Ecash coins

- Uniqueness
  - chosen randomly and large enough
- Coins' serial number is generated by the client's cyberwallet
- Blind signature protocol
  - The bank is unable to see the serial number on the coin it is signing

Coin keys

- Problem
  - Bank cannot see what it is signing
- Sloution
  - The bank signs the coin with the signature key representing worth.
- $1 coin =

Serial#, keyversion, $\{Serial\#\}SK_{Bank.s\ \$1\ Key}$

Indication of which public key to use

Forgery using the inverse relation of RSA

- Choose a large random number R

$S = \{R\}PK_{Bank's\ \$1\ Key}$

$\{S\}SK_{Bank's\ \$1\ Key} = \{\{R\}PK_{Bank's\ \$1\ Key}\}SK_{Bank's\ \$1\ Key}$

$= R$

- *Forged_coin =*
- *{S, keyversion, R = {S}SK$_{Bank's\ \$1\ Key}$}*

Solution

- Applying a one-way function H to The serial number
- *S, {H(S)}SK*$_{Bank's\ \$1\ Key}$

Coin = Serial#, keyversion, {f(Serial#)}SK$_{Bank.s\ \$1\ Key}$

Redundancy-adding function

$f(s) = s_t, s_{t-1}, .., s_1, s_0$

$s_0 = s$

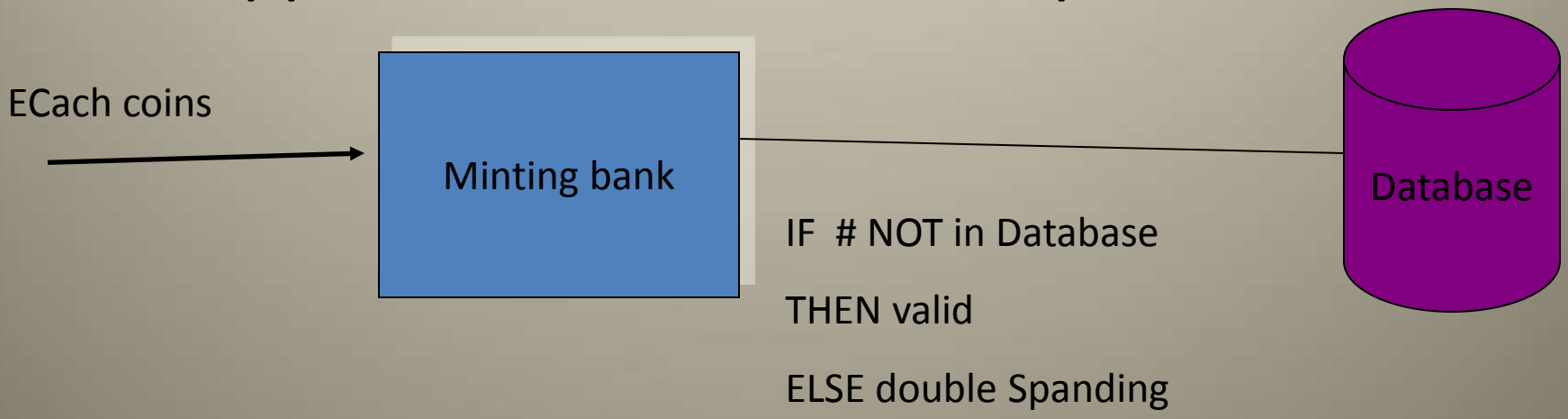
$s_t = H(s_0, s_1, .., s_{t-1})$

Double-spending prevention

- A serial number is spent twice.
- The minting bank records every coin that is deposited back
  - Database of all spent serial numbers

A valid unspent coin

- Be signed, with any denominational signature, by the bank;
- Have an expiry date associated with it that is later than the present date;
    - Keeping database small
- Not appear in the database of spent coins.



RSA public-key

- To create key pairs for different denominations, different values of ***e*** and ***d*** are generated for the same modulus ***m***.

Withdrawing coins

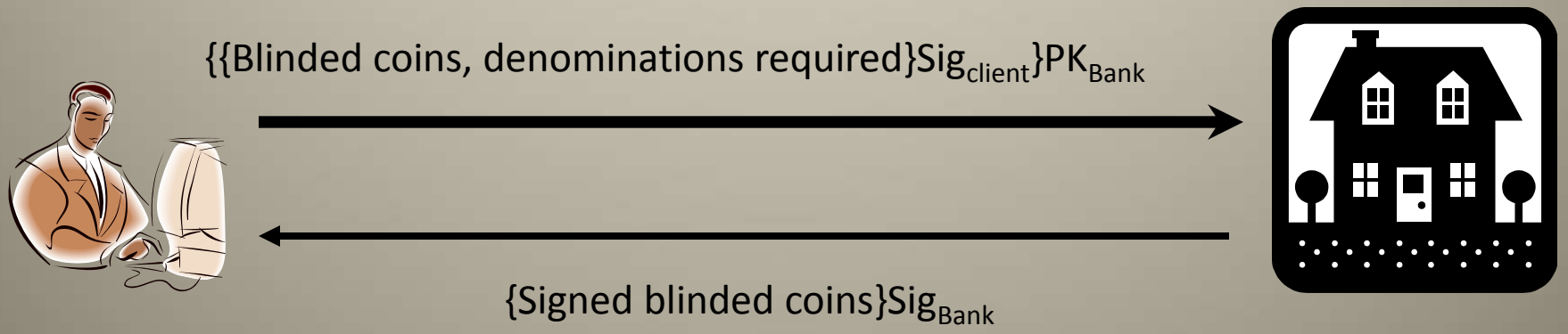
- wallet software
  - r: Random
  - e2: Public key for the 2-cent denomination
  - serial# × r^{e2} (mod m)

Withdrawing coins

- The bank
  - d_2: 2-cent secret signature key
  - $(\text{serial\#} \times r^{e2)\, d2} = (\text{serial\#})^{d2} \times r \pmod m$
- user
  - $(\text{serial\#})^{d2} \times r \,/r = (\text{serial\#})^{d2} \pmod m$

single withdrawal request

- The request must be
  - signed with the client's secret key,
  - encrypted using bank's public key



An Ecash purchase

- merchant ‘s payment request
  - payreq = {currency, amount, timestamp, merchantbankID, merchant_accID, description}

Making the payment

- Client → Merchant: payment

  {payment_info,{Coins}PK_{Bank}}

Encrypted with the bank's public key

  – payment_info :

  {bankID, amount, currency, ncoins, timestamp, merchant_IDs,H(description), H(payer_code)}

Proving payment

- Client's *H(Payer_code)*
- Later prove to the bank that the client made the payment.
- {Coins, H(Payment_info)} PK_{Bank}

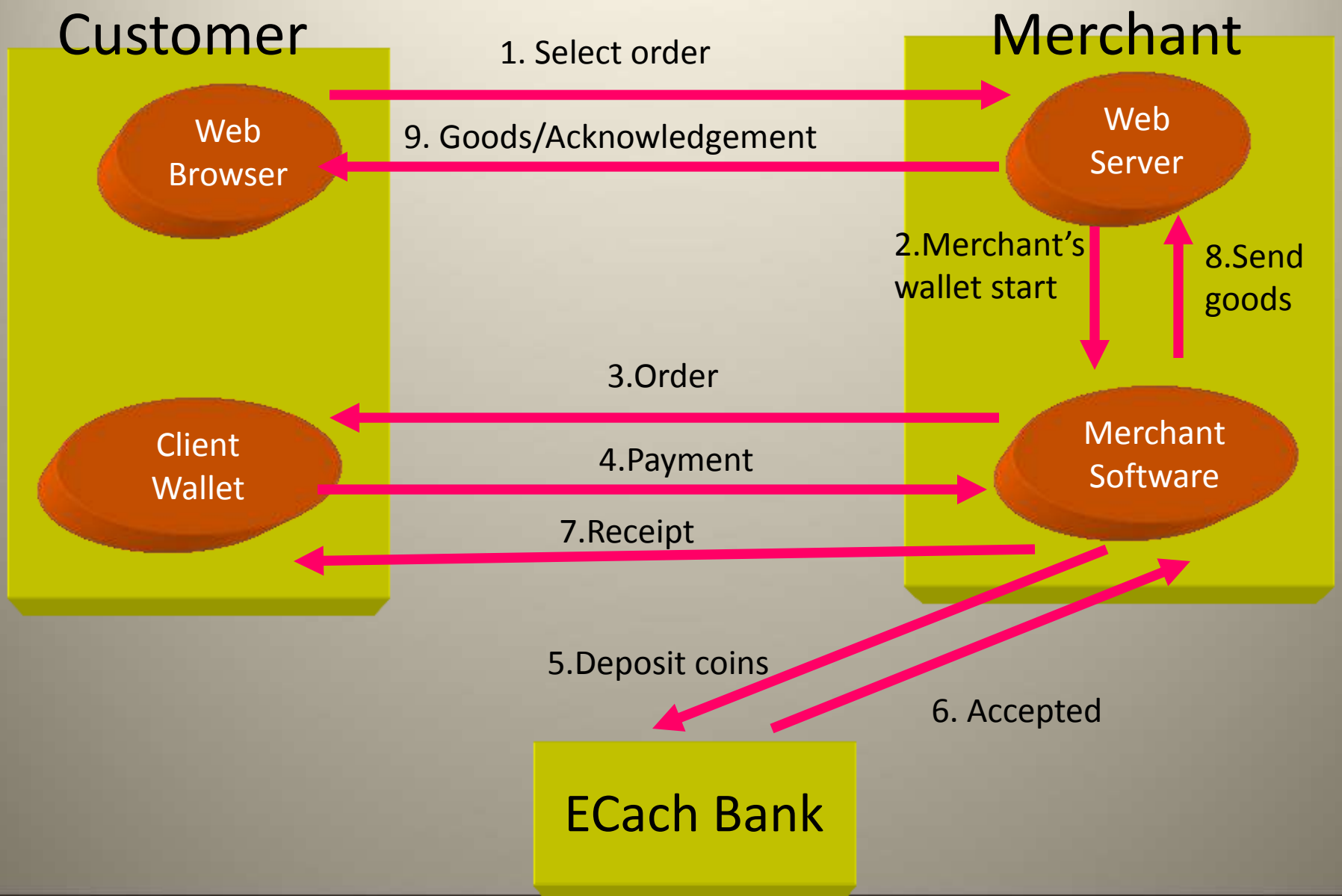
- The payers (clients) remain anonymous, unless they decide later to prove the payment.

Payment deposit

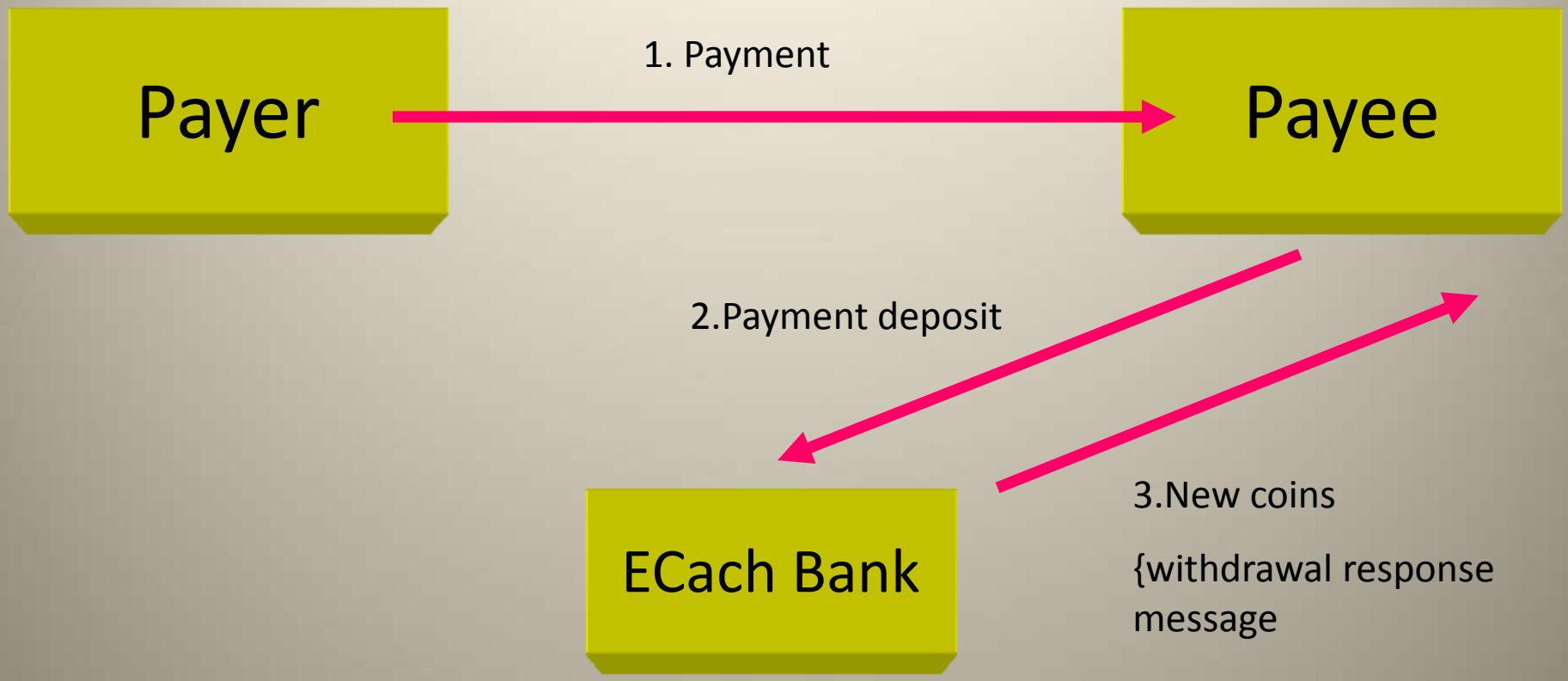
- The merchant forwards payment to the bank
- deposit = { {payment}$Sig_{Merchant}$ }PK_{Bank}

- Bank → merchant
  - deposit_ack = {result, amount}Sig_{Bank}

Integration with the Web

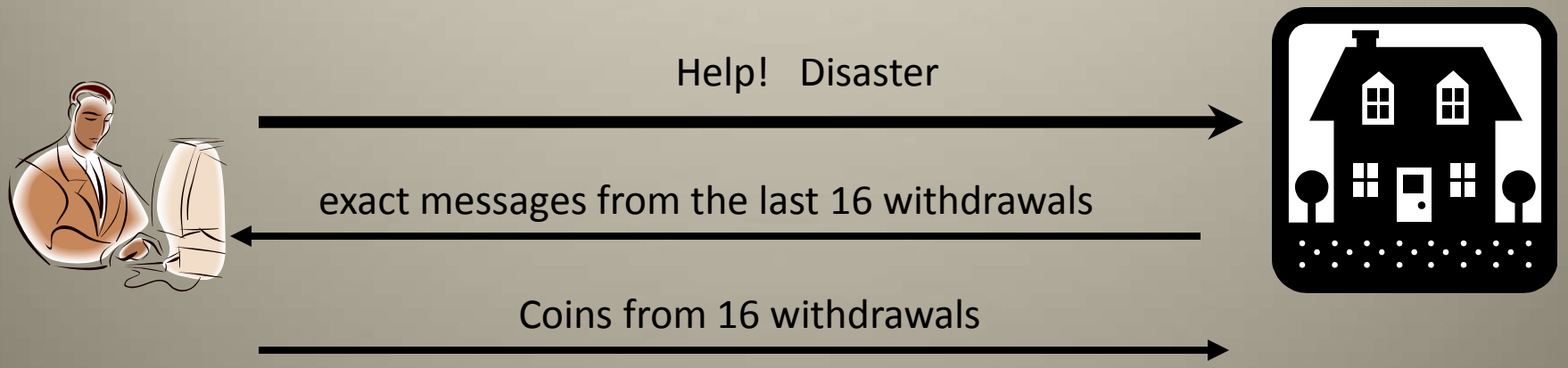


Transferring Ecash



Lost coins

The network fails or the computer crashes during a payment



Ecash and crime

- To hide the identity of criminals
  - money laundering,
  - tax evasion,
  - bribes,
  - black markets
- The payee (merchant) is not anonymous

perfect crime

- Anonymous kidnapper prepares a large number of blinded coins.
- The signed blinded coins is published in a public place such as a newspaper
  - This will prevent the pickup being traced
- The coins are then unblinded and spent.

Remarks

- Advantages
  - secure, fully anonymous electronic cash
  - Web and e-mail
- Disadvantages
  - Computationally intensive cryptography,
  - Multiple messages,
  - Database lookups
  - Limited scalability

Project CAFE

Chapter 6

Part 2

Introduction

- CAFE: Conditional Access for Europe
- The project aim→
  - To develop a general system to administer rights to users
  - An advanced electronic payment system
- Ideas
  - Untraceable (anonymous) electronic cash
  - Checks with counters
    - the user sign checks up to a specified amount

Goals of CAFE

- Multiparty security
  - Guaranty of the security of each entity without the need to trust a third party
  - Each party must be able to trust the device that they are using
  - Open procedures and algorithms
    - Available for inspection by all

Goals of CAFE

- Off-line payments
  - no need for a merchant to contact a central database
- Detection of double spending
  - If the tamper resistance of a device is broken, then double spending can take place
  - Detection:
    - Maintaining a database of recently spent payment slips by the financial institutions (losing the balance)
- Untraceable payments

CAFE Architecture

- Payer
  - With smart card or an electronic wallet
- Payee
  - merchant
- Bank
  - Issuer
  - acquirer

CAFE Architecture

Clearing Center

Issuer

Acquire

Banking Network

Payment

Payer

Payee

CAFE devices

- Tamper resistant secure electronic devices for
  - Storing electronic money
  - Cryptographic operations
  - Making payments to merchant

CAFE devices

- Smart card
  - An embedded microprocessor powered by an external source
  - Referred to as the α (alpha) system

CAFE devices

- Wallets
  - Observer
    - Protects the bank's interests
  - Purse
    - Protects the user's interests

The observer cannot divulge any secret information to the bank without the user's knowledge

Wallets

- Two-button wallet α^{+}
  - Verifing and monitoring of the payment
- Full wallet
  - Γ (gamma) system

NetCash

طرحی عملی برای پول الکترونیک در اینترنت

فهرست

- NetCash
- مدل/چارچوب
- سکه های NetCash
- جلوگیری از خرج مجدد
- انتقال سکه ها
- خرید
  - دریافت سکه
  - پرداخت به فروشنده
  - اعتبارسنجی سکه ها
- ایجاد گمنامی محدود
- نقل و انتقال بانکی
- گسترش سیستم
  - جلوگیری از تقلب فروشنده
  - عملیات off-line
- جمع بندی

NetCash

- سیستم پول الکترونیک on-line
- طراحی شده در دانشگاه Southern california
- Macro payment
- گمنامی محدود
- استفاده از هر دوی سیستم های رمزنگاری متقارن و نا متقارن
- scalable

مدل/چارچوب

- شامل خریدار، فروشنده و سرورهای توزیع شده ی پول

- هر سرور ۴ سرویس زیر را فراهم می کند :
  - بررسی سکه ها برای جلوگیری از خرج مجدد
  - ضرب سکه
  - بازخرید سکه ها
  - مبادله ی سکه های معتبر با سکه های جدید

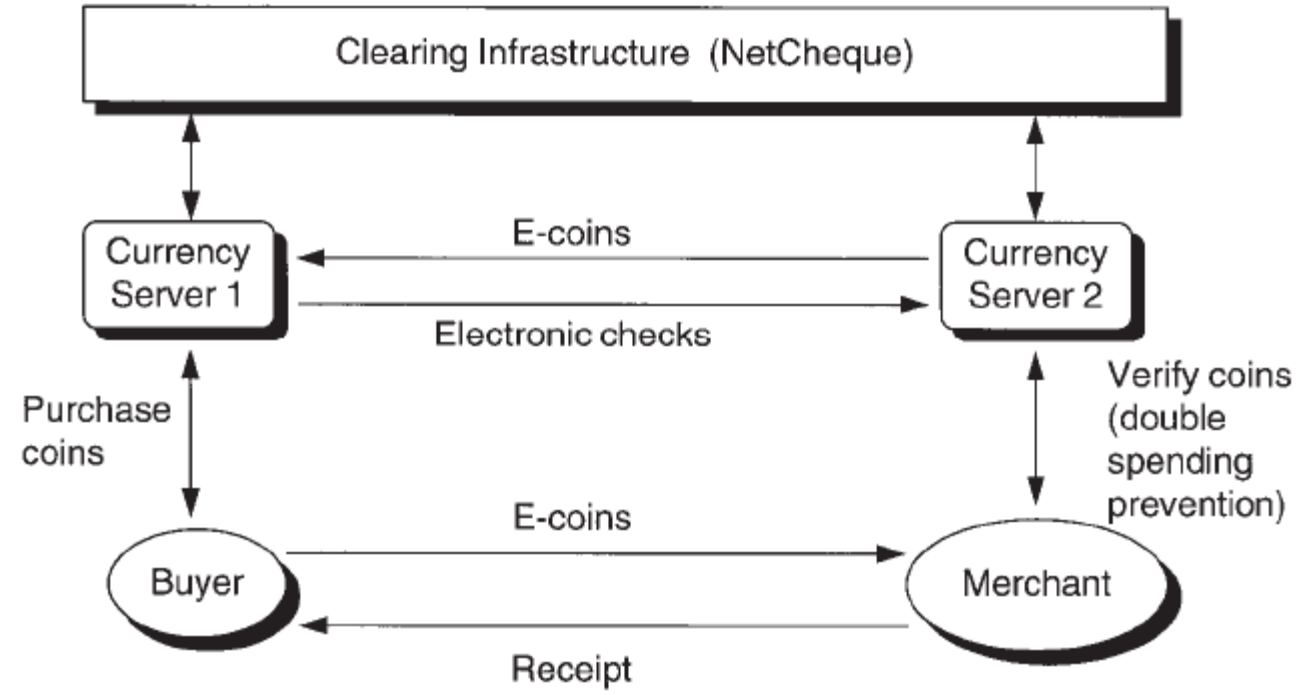


Figure 6.13 The NetCash system.

سکه های NetCash

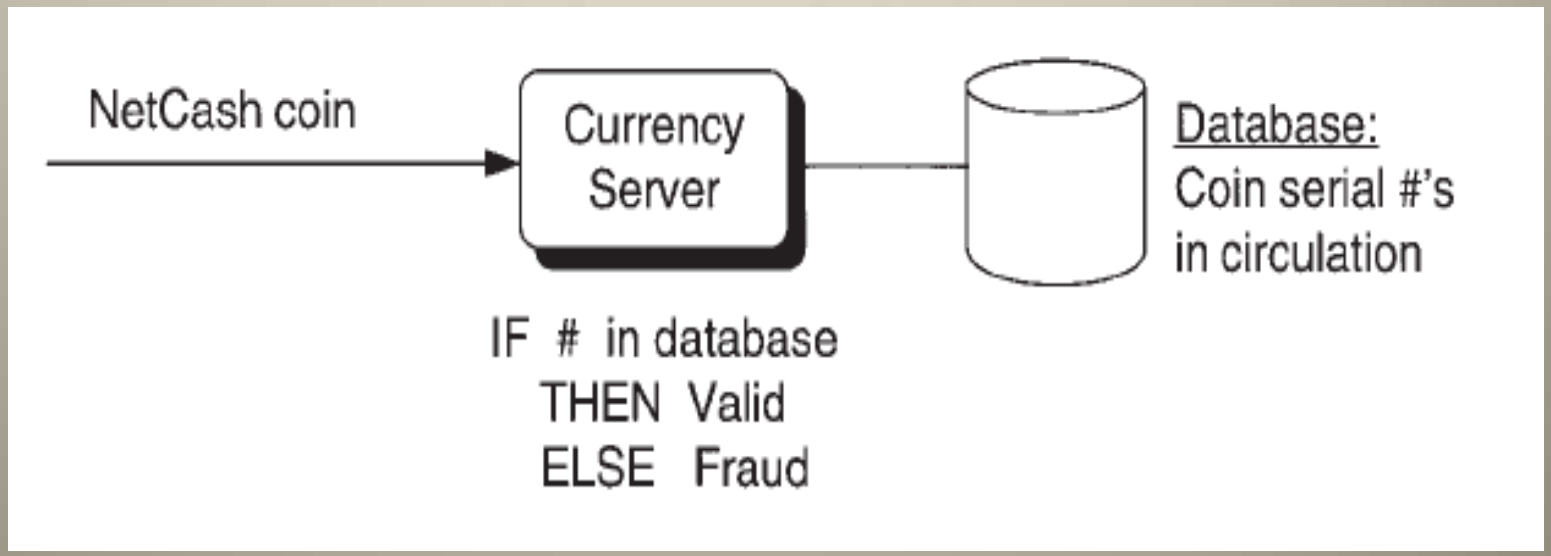
$$\text{Coin} = \{\text{CS\_name, CS\_addr, Expiry, Serial\#, Value}\}SK_{CS}$$

Example:

{CS1, bank.com, 26-July-98,12345678, $1} SK_{CS1}

- cs_name : نام سرور ضرب کننده ی پول
- cs_addr : آدرس شبکه ی سرور ضرب کننده ی پول
- Expiry : تاریخ اعتبار سکه
- Serial # : شماره ی شناسایی یکتای سکه
- Value : ارزش پولی سکه

جلوگیری از خرج مجدد



انتقال سکه

- گواهی بیمه
  - توزیع امن کلید عمومی سرور
  - FIC(Federal Insurance Corporation)
  - یک گواهی بیمه فرم زیر را دارد :

$$Cert = \{Cert\_ID, CS\_name, PK_{CS}, Issue\_date, Expiry\}Sig_{FIC}$$

Cert_ID: شماره شناسایی یکتای گواهی

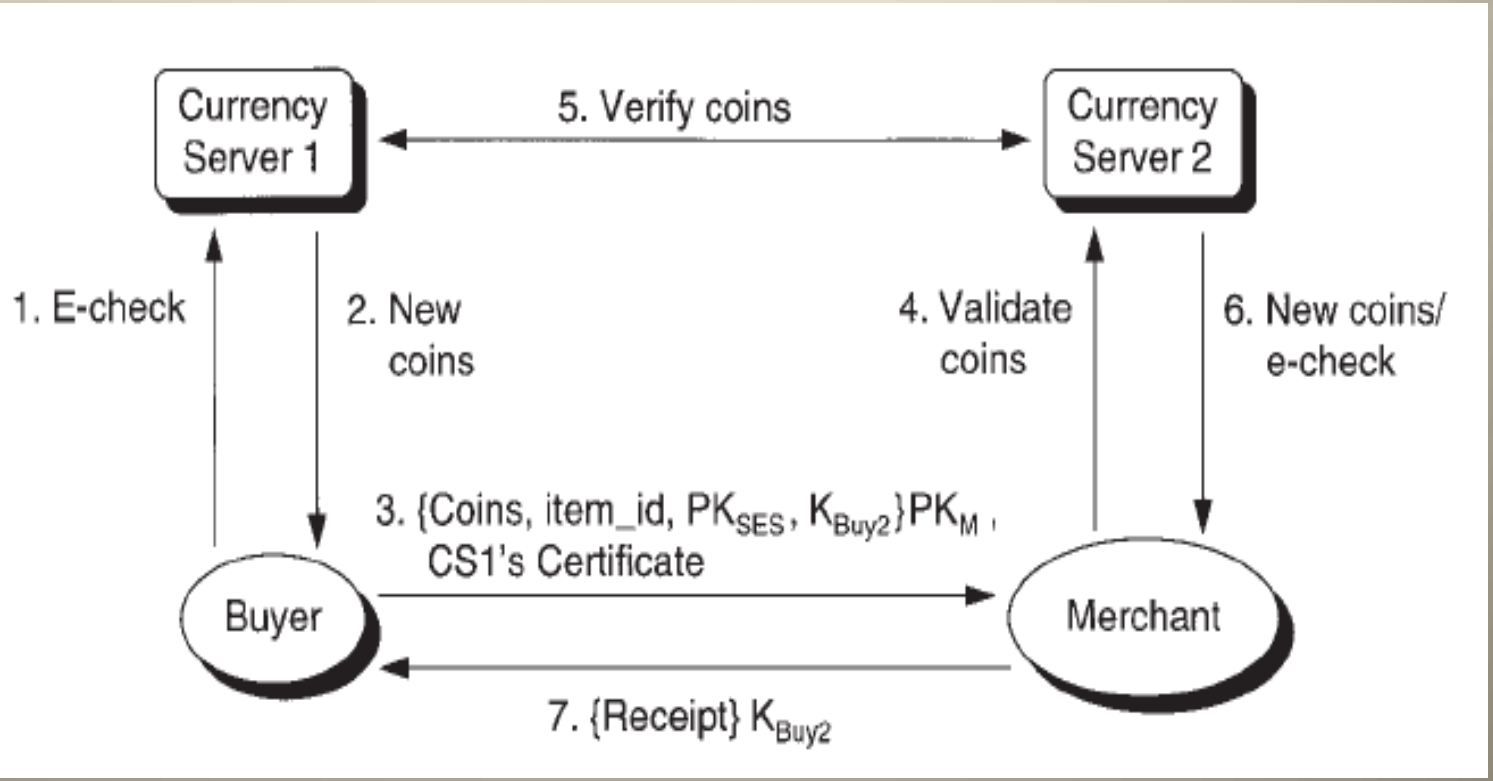
CS_name: نام سرور ضرب کننده ی پول

PK_{CS} : کلید عمومی سرور

Issue_date : تاریخ صدور گواهی

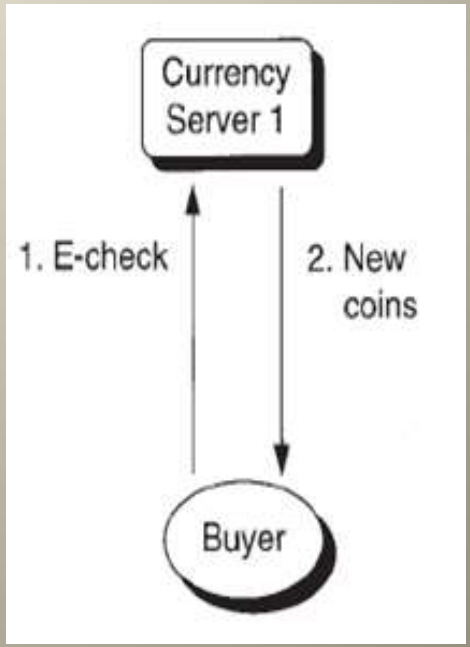
Expiry: تاریخ انقضای گواهی

خرید


Currency Server 1
5. Verify coins
Currency Server 2
1. E-check
2. New coins
4. Validate coins
6. New coins/ e-check
3. {Coins, item_id, PK_{SES}, K_{Buy2}}PK_M , CS1's Certificate
Buyer
Merchant
7. {Receipt} K_{Buy2}

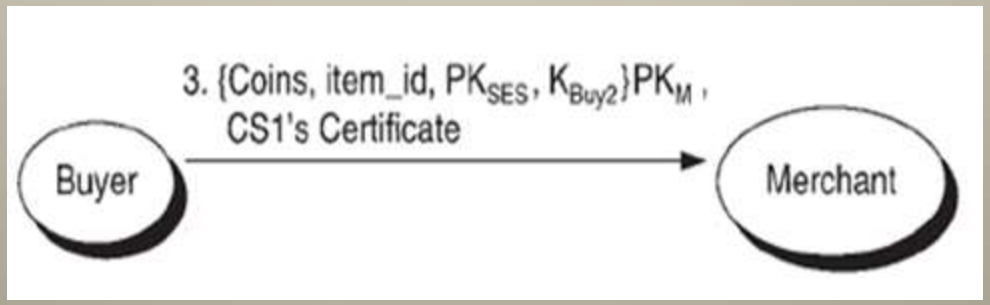
دریافت سکه ها

- B CS1 : $\{\text{E-check}, K_{Buyer}\}PK_{CS1}$
  - ✓ $\overrightarrow{\{\text{Instrument}, K_x, \text{transaction}\}PK_{cs}}$
- CS1 B : $\{\text{New coins}\}K_{buyer}$
  - ✓ $\overrightarrow{\{\text{transaction}\}K_x}$



پرداخت به فروشنده

- {Coins, item_id, PK_{Ses}, K_{Buy2}}PK_M, CS1’s certificate
  - Coins: مبلغ خرید بر حسب سکه های NetCash
  - Item_id: شماره شناسایی اشیا خریداری شده
  - Pkses: کلید نشست عمومی(می تواند کلید عمومی مشتری باشد)برای رمز کردن اقلام خریداری شده
  - K_{Buy2}: کلید نشست متقارن تازه تولید شده برای رمز کردن پاسخ



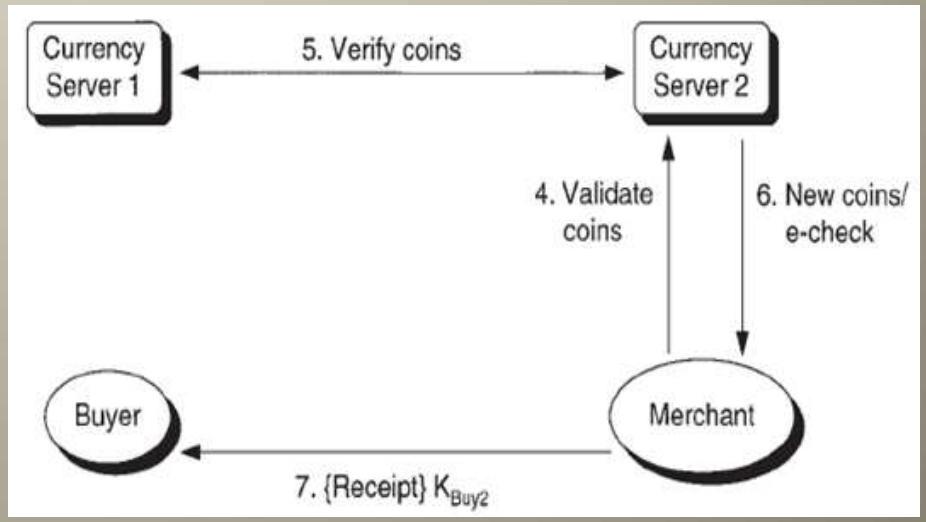
- {PK_M}PK_{Buyer} {PK[illegible]tack}PK_{Buyer}

اعتبار سنجی سکه ها

- M SC2 : $\{Coins, K_M, transaction\}PK_{CS2}$
- SC2 M : $\{New\ coins/check\}K_M$

- M B : $\{receipt\}K_{Buy2}$

Receipt = $\{amount, transaction\_id, date\}Sig_M$



ایجاد گمنامی محدود

- گمنامی فروشنده

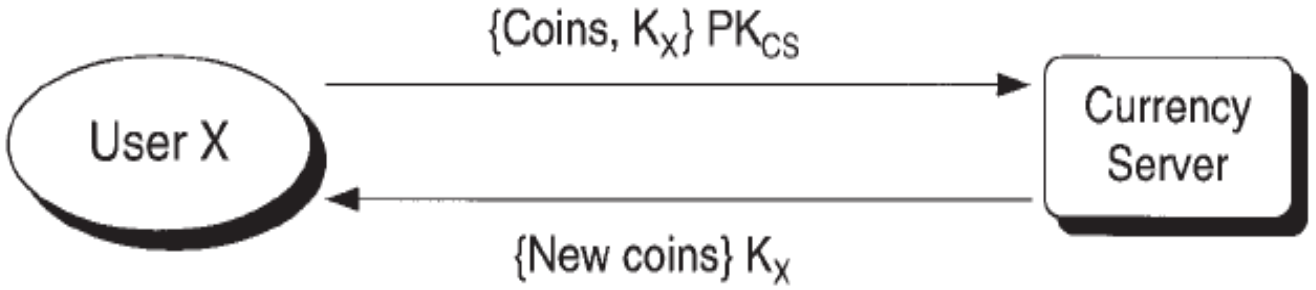
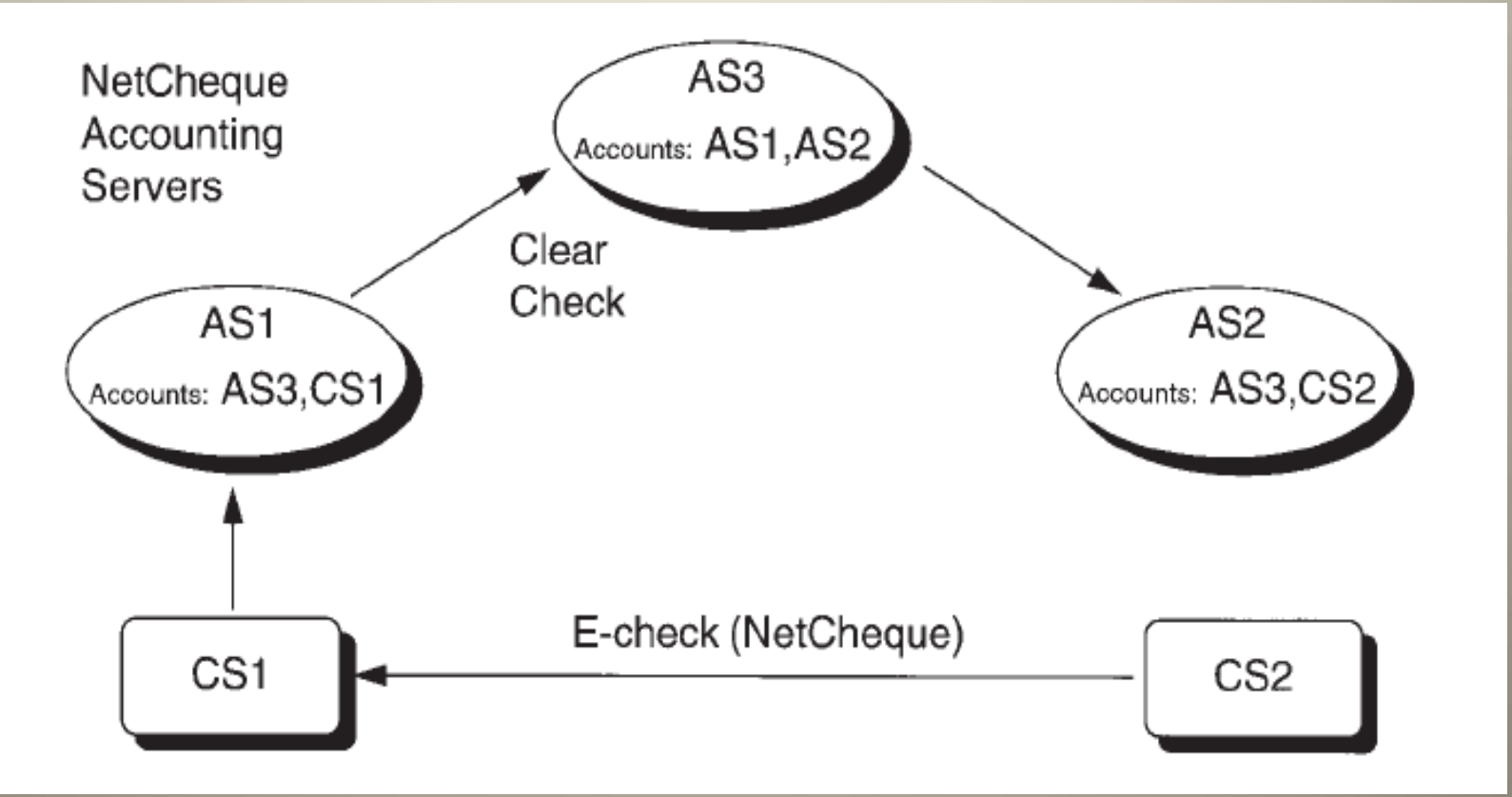


Figure 6.17 Exchanging coins anonymously with a currency server.

نقل و انتقال بانکی(تسویه)



گسترش سیستم

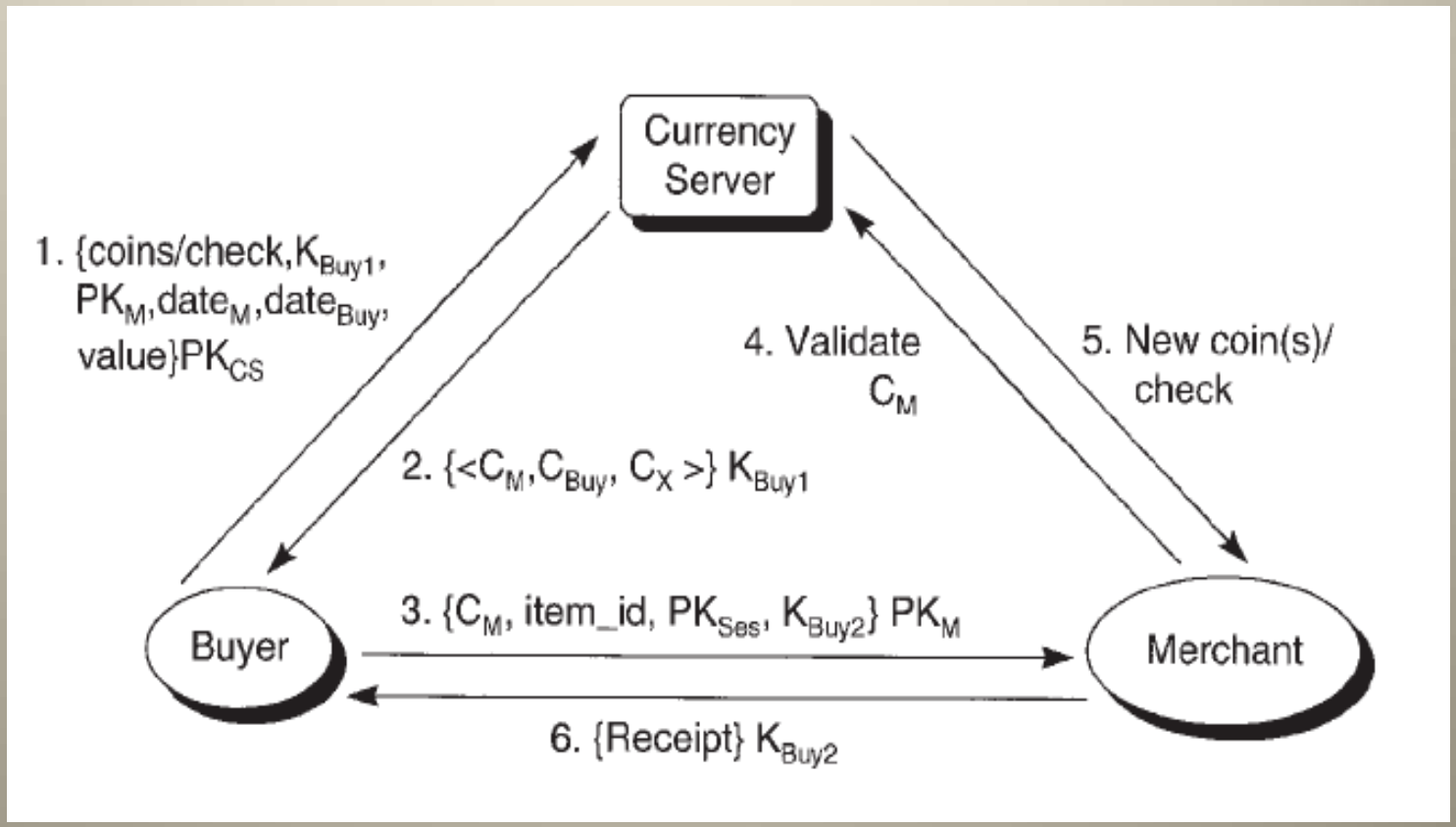
- جلوگیری از تقلب فروشنده
- عملیات off-line

جلوگیری از تقلب فروشنده

- Coin = {C_M, C_{Buy}, C_X}

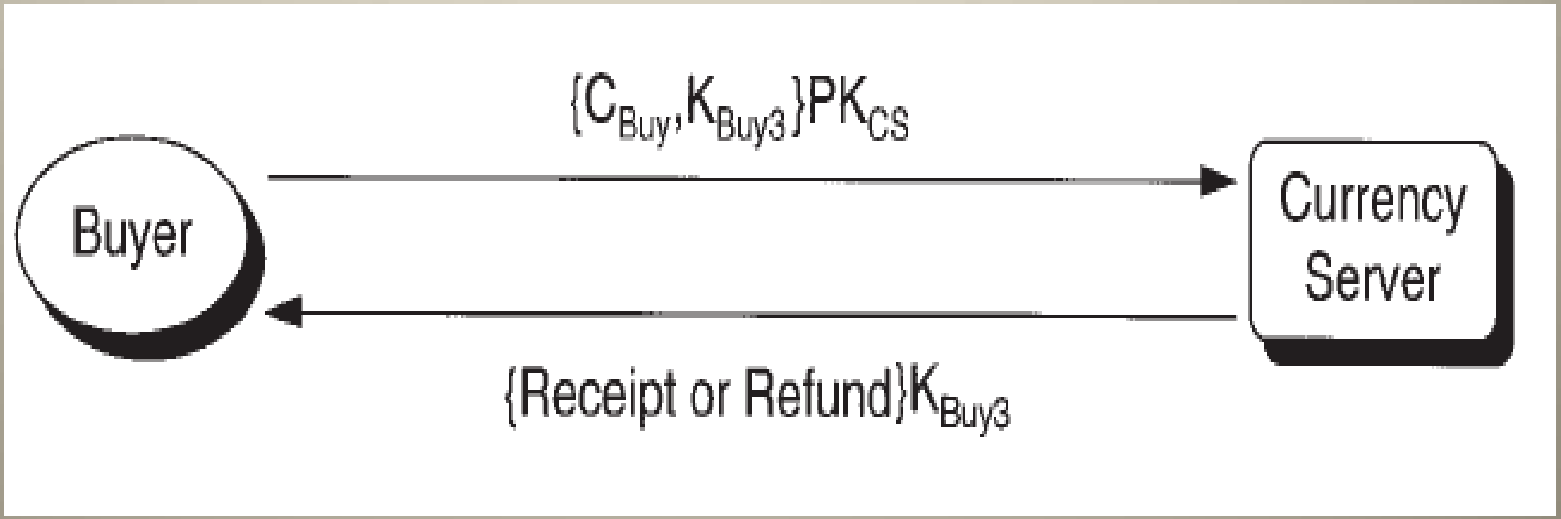
- C_M= {CS_ name, CS_ addr, Serial# , Value, Merchant_ inf o, time_ frame1}SK_{CS}
- C_{BUY}= {CS_ name,CS_ addr, Serial#, Value, Buyer_ info, time_ frame2}SK_{CS}
- C_X = {CS_ name,CS_addr,Serial# , Value, time_ frame3}SK_{CS}

✓ SKM (PKM (Secret)) = Secret



- {Merchant_id, PK_M, amount, date}Sig_{CS}

عمليات off-line



جمع بندی

- امنیت
- گمنامی
- قابلیت پذیرش
- عملیات off-line
- قابلیت انتقال
- Scalability

منابع

- Electronic Payment Systems for E-Commerce, Second Edition, Donal O.Mahony,Michael Peirce and Hitesh Tewari
- Protocols for Secure Electronic Commerce,*Mostafa Hashem Sherif, Ph.D.*
- *NetCash: A design for practical electronic currency on the Internet, Gennady Medvinsky and B.Clifford Neuman*