



9 : Electronic Payment Systems

IT5306 - Principles of Information Security

Level III - Semester 5

List of sub topics

- 9.1. Fundamentals of e-payment
- 9.2. Credit Card Payment Protocols
- 9.3. Digital Cash and other e-payments methods
- 9.4. Cryptocurrency
- 9.5. Blockchain

Fundamentals of e-payment of Payments

Properties :

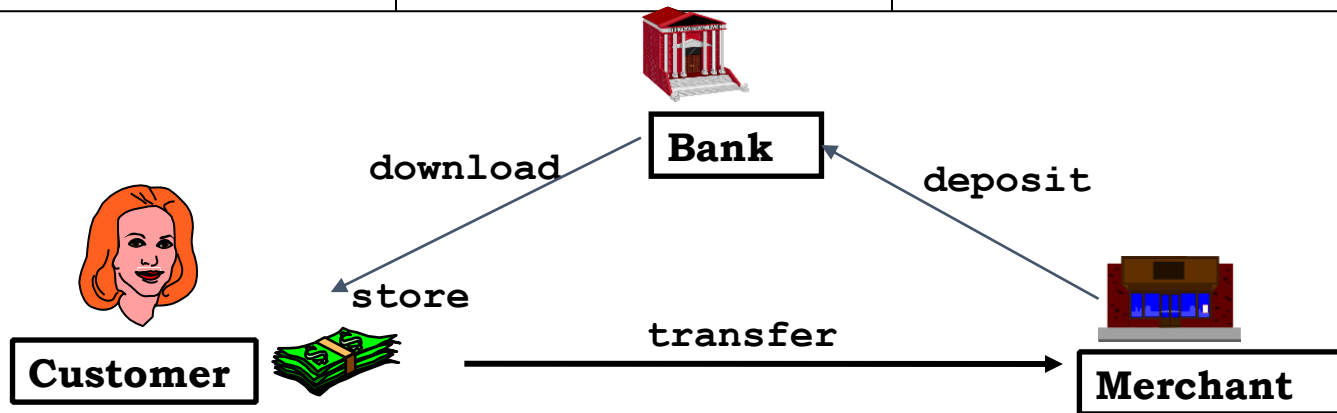
- where is the money (authorization)
- time of payment vs. time of order/shopping

Characteristics of payment methods :

Type of payment	Money	Time
Cash	with Customer	at Purchase
Debit card	in Bank	at Purchase
Credit card	in Bank	after Purchase
Invoice	in Bank	after Purchase
Pre-paid	with Merchant	before Purchase
Subscription	with Merchant	before Purchase

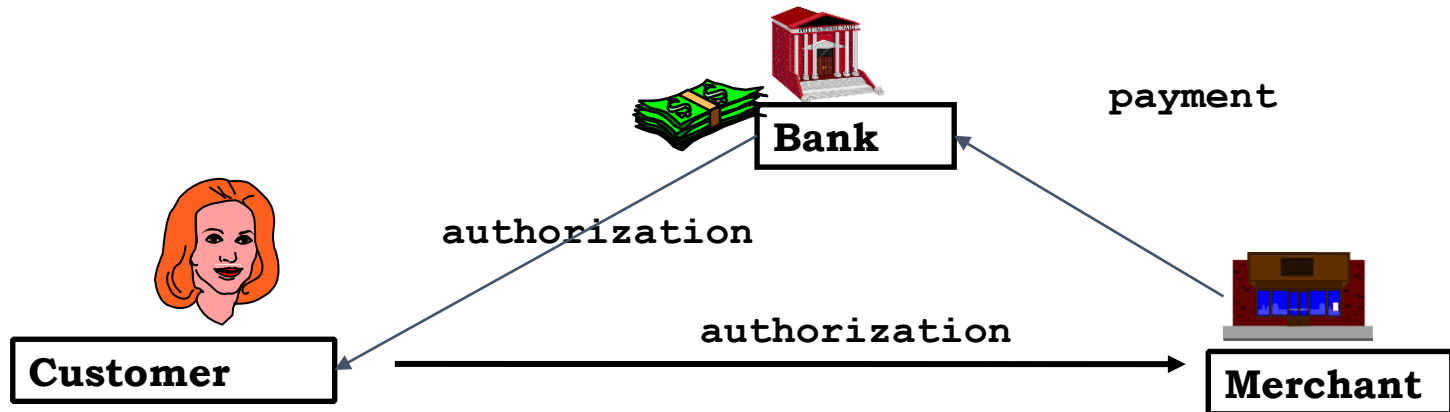
Fundamentals of e-payment of Payments

Type of payment	Money	Time
Cash	<i>with Customer</i>	at Purchase
Debit card	in Bank	at Purchase
Credit card	in Bank	after Purchase
Invoice	in Bank	after Purchase
Pre-paid	with Merchant	before Purchase
Subscription	with Merchant	before Purchase



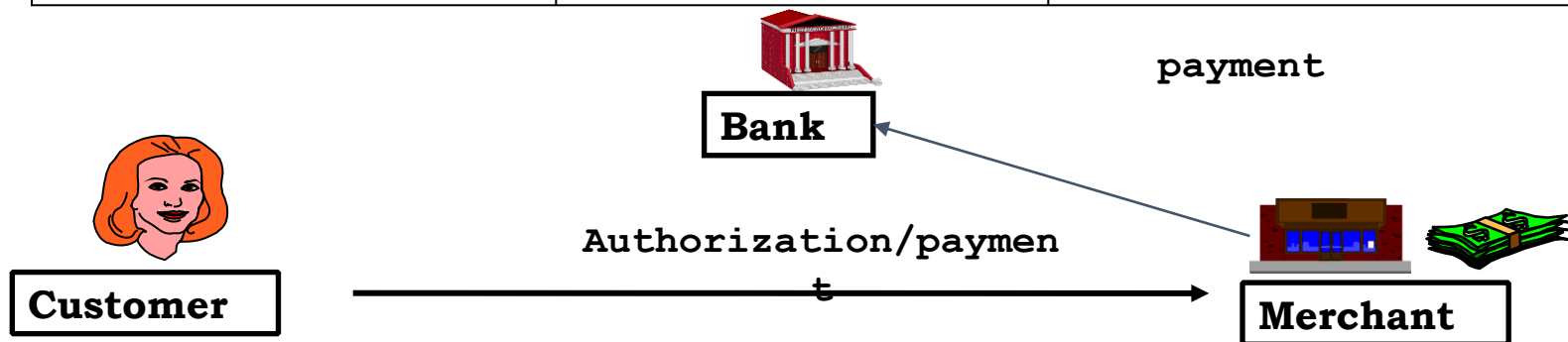
Fundamentals of e-payment of Payments

	Money	Time
Cash	with Customer	at Purchase
Debit card	<i>in Bank</i>	at Purchase
Credit card	<i>in Bank</i>	after Purchase
Invoice	<i>in Bank</i>	after Purchase
Pre-paid	with Merchant	before Purchase
Subscription	with Merchant	before Purchase



Fundamentals of e-payment of Payments

Type of payment	Money	Time
Cash	with Customer	at Purchase
Debit card	in Bank	at Purchase
Credit card	in Bank	after Purchase
Invoice	in Bank	after Purchase
Pre-paid	<i>with Merchant</i>	before Purchase
Subscription	<i>with Merchant</i>	before Purchase



Risk in using Credit cards

- Customer uses a stolen card or account number to fraudulently purchase goods or service online
- Family members use bankcard to order goods/ services online, but have not been authorized to do so.
- Customer falsely claims that he or she did not receive a shipment
- Hackers find the ways into an e-commerce merchant's payment processing system and then issue credits to hacker card account numbers.



Risk in using Credit cards

Extra protection when there's no card

Card-not-present (CNP) merchants must take extra precaution against fraud exposure and associated losses. Anonymous scam artists bet on the fact that many Visa fraud prevention features do not apply in this environment. Follow these recommendations to help prevent fraud in your card-not-present transactions.

Quick steps to ensure against CNP fraud

Obtain an authorization.

Verify the card's legitimacy:

Ask the customer for the card expiration date, and include it in your authorization request.

An invalid or missing expiration date might indicate that the customer does not have the actual card in hand.

Use fraud prevention tools such as Visa's Address Verification Service (AVS), Card Verification Value 2 (CVV2), and Verified by Visa.

Credit Card Protocols

- SSL 1 or 2 parties have private keys
- TLS (Transport Layer Security)
 - IETF version of SSL

VERY IMPORTANT.
USAGE INCREASING

- 3KP (IBM) 3 parties have private keys
- SEPP (Secure Encryption Payment Protocol)
 - MasterCard, IBM, Netscape based on 3KP
- STT (Secure Transaction Technology)
 - VISA, Microsoft

OBSOLETE

- SET (Secure Electronic Transactions)
 - MasterCard, VISA all parties have certificates

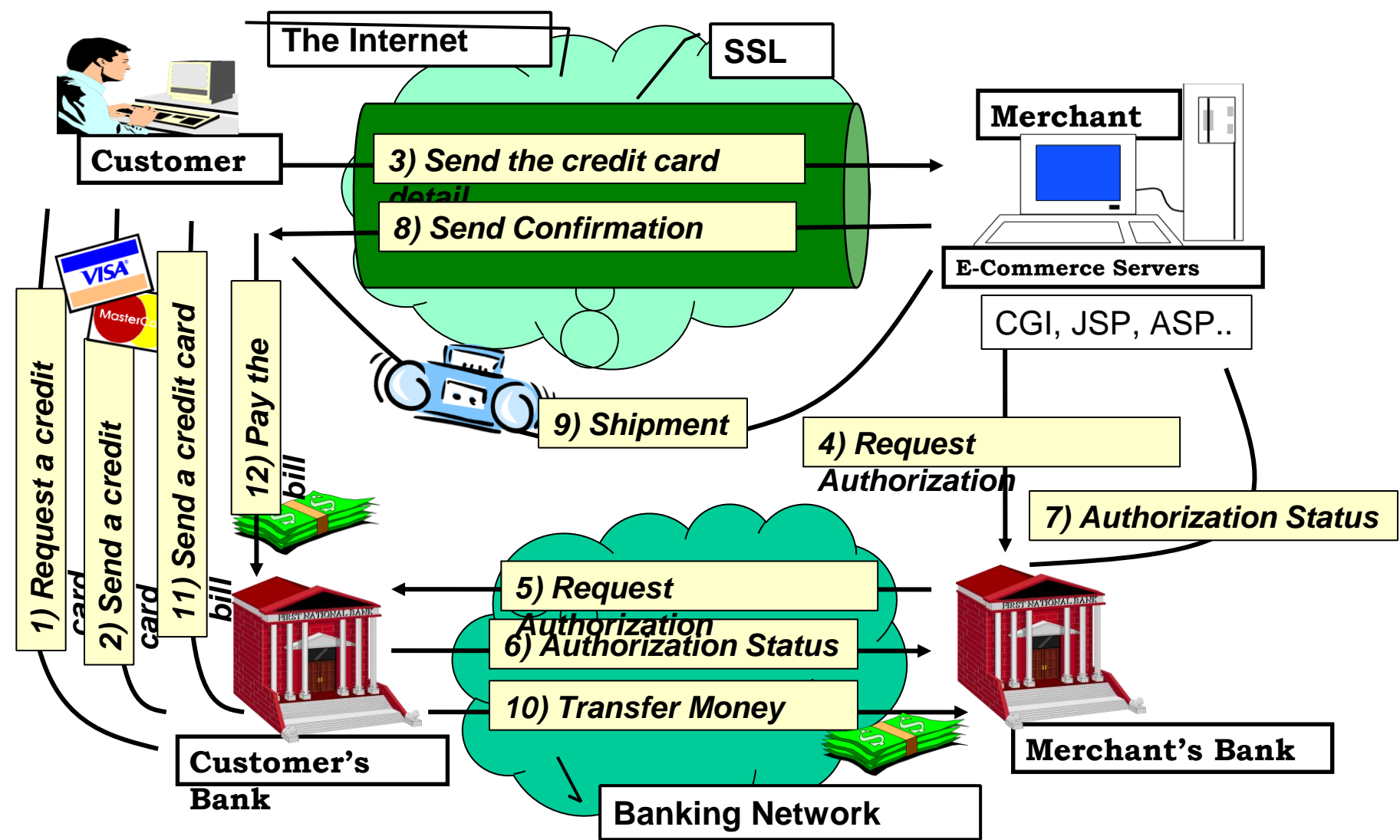
VERY SLOW
ACCEPTANCE

• 3D Secure

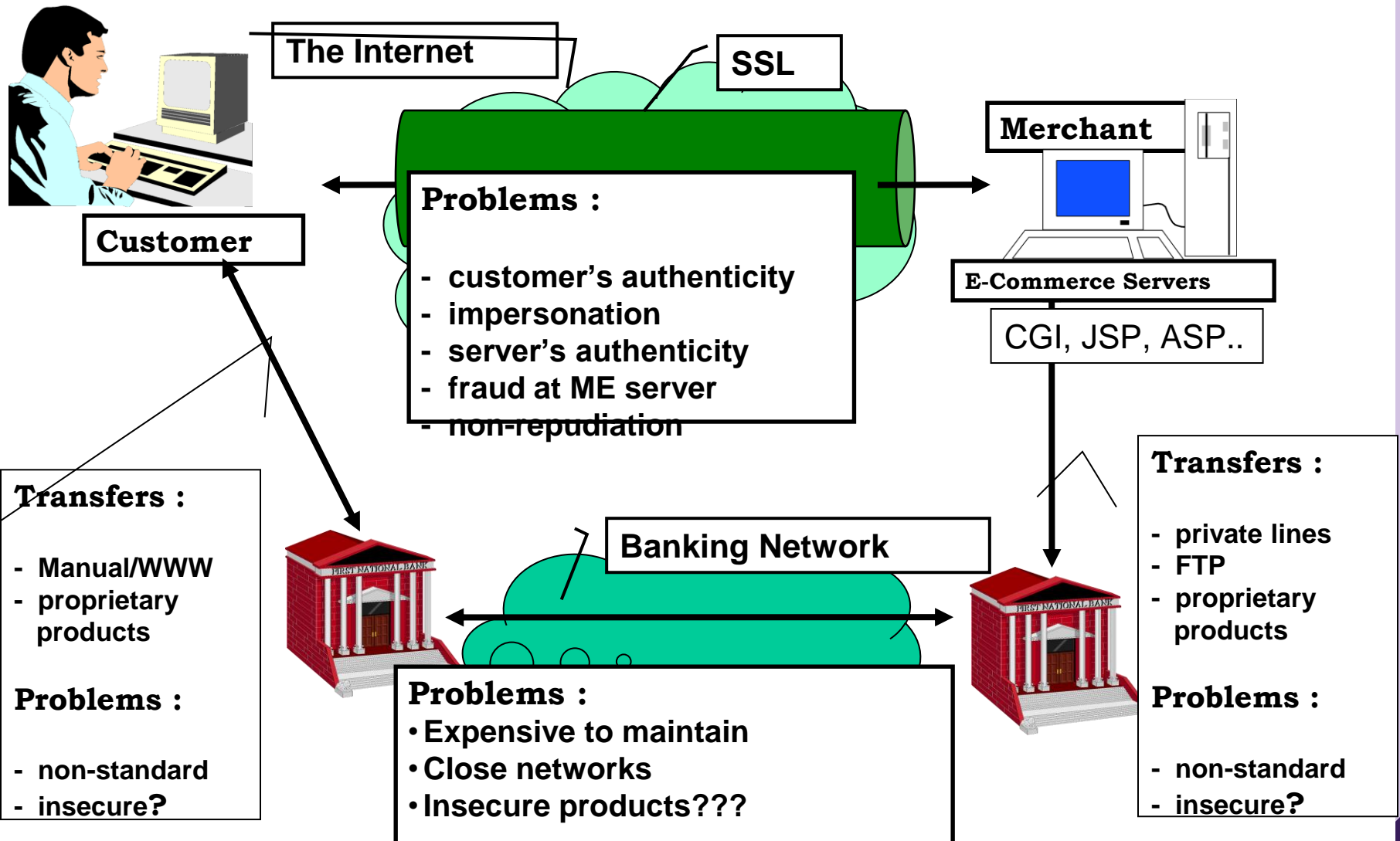
SSL (Secure Sockets Layer)/TLS

- NOT a payment protocol -- can be used for any secure communications, like credit card numbers
- TLS is a secure data exchange protocol providing
 - Privacy between two Internet applications
 - Authentication of server (authentication of browser optional)
- Uses enveloping: RSA used to exchange AES keys
- SSL Handshake Protocol
 - Negotiates symmetric encryption protocol, authenticates
- SSL Record Protocol
 - Packs/unpacks records, performs encryption/decryption
- Does not provide non-repudiation

Internet Transactions (Insecure?)



Secure Credit Card Payments (TLS)



Secure Electronic Transaction (SET)

- Developed by Visa and MasterCard
- Designed to protect credit card transactions
- Confidentiality: all messages encrypted
- Trust: all parties must have digital certificates
- Privacy: information made available only when and where necessary

SET Objectives

- Confidentiality of payment and order information
 - Encryption
- Integrity of all data (digital signatures)
- Authentication of cardholder & account (certificates)
- Authentication of merchant (certificates)
- Interoperability between SET software and network
 - Standardized message formats
- SET is a payment protocol
 - Messages relate to various steps in a credit card transaction

Participants

- Consumer (cardholder)
- Merchant
- **Acquirer**: financial institution acting as transaction clearinghouse for merchant
- **Issuer**: financial institution that issued consumer credit/debit card
- **Association**: Visa or Mastercard

SET Overhead

Simple purchase transaction:

- Four messages between merchant and customer
- Two messages between merchant and payment gateway
- 6 digital signatures
- 9 RSA encryption/decryption cycles
- 4 DES encryption/decryption cycles
- 4 certificate verifications

Scaling:

- Multiple servers need copies of all certificates

SET Advantages/Disadvantages

Advantages :

- strong cryptography
- strong / complete security services
- complete system (all parties involved)
- full functionality (payments, authorizations, captures, credits, inquiries, batches, etc.)
- “standardized”
- scalable (certification infrastructure)

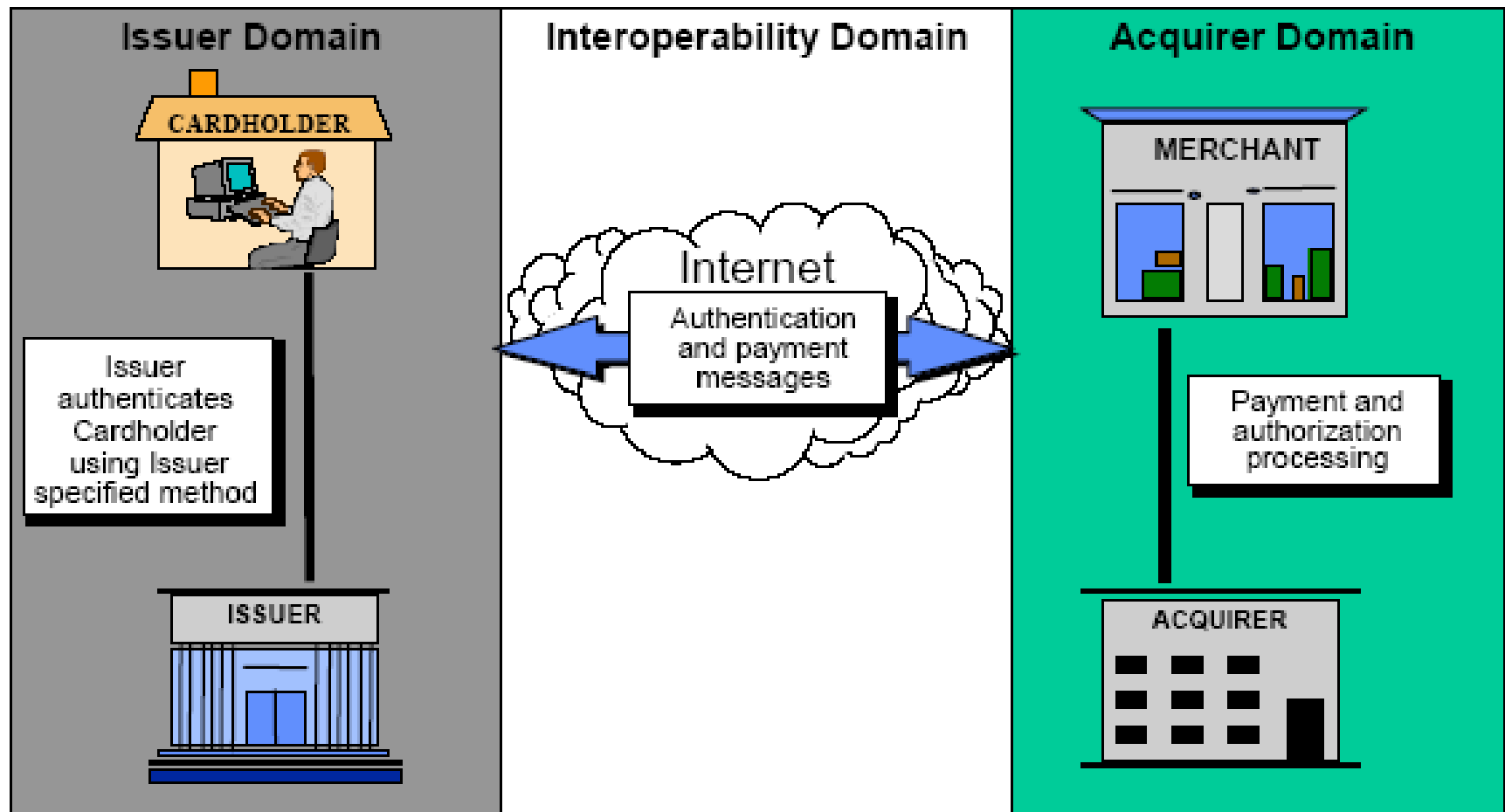
Disadvantages :

- global system (“all-or-nothing”)
- “heavy-weight” components
- “privately” owned (VISA, MasterCard)
- credit cards payments only
- early implementations complicated
- “ahead of time” (user requirements, problems)

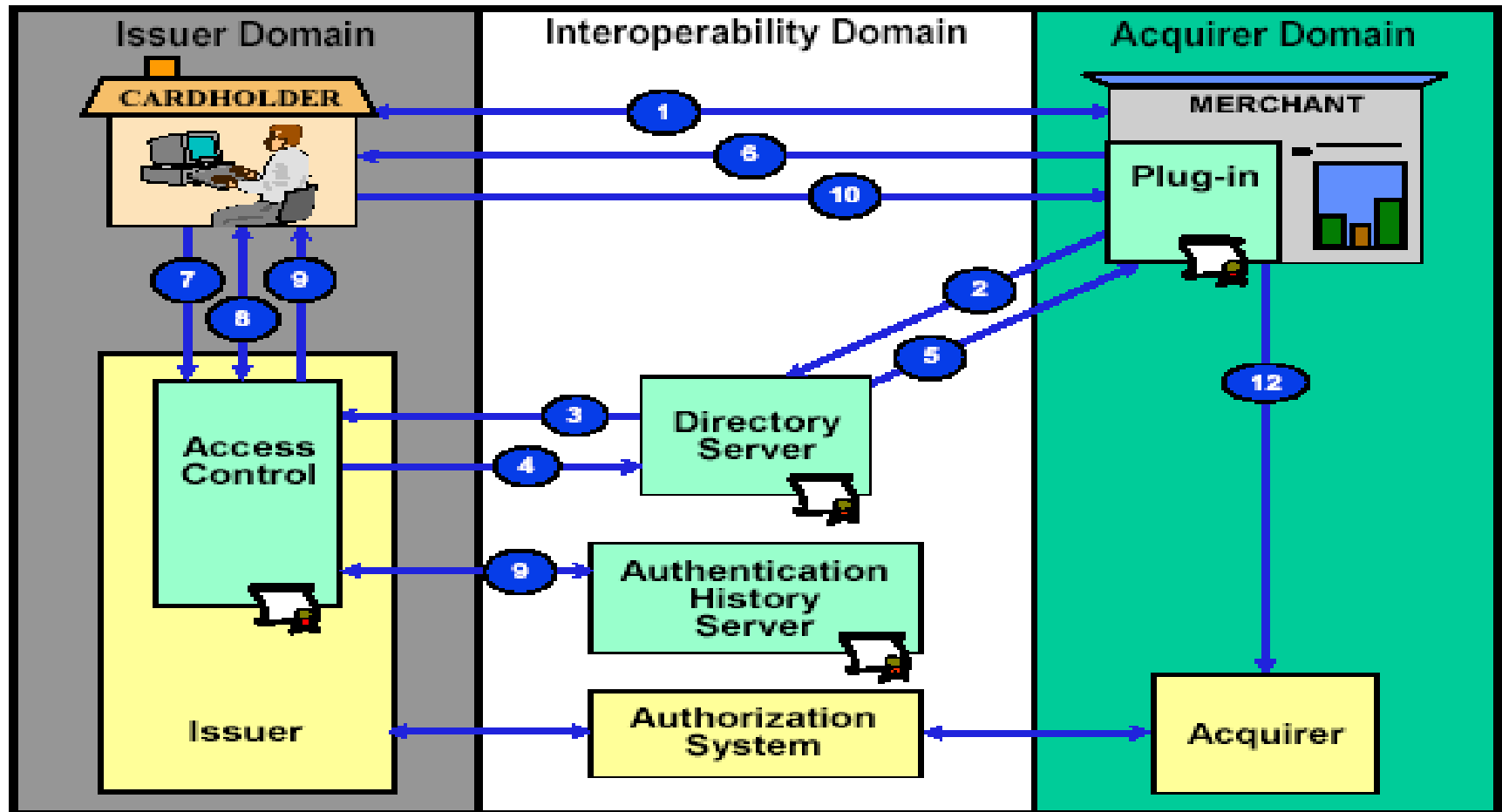
3-D Secure

- Idea: authenticate user without a certificate
- Requires the user to answer a challenge in real-time
- Challenge comes from the issuing bank, not the merchant
- Issuing bank confirms user identity to merchant

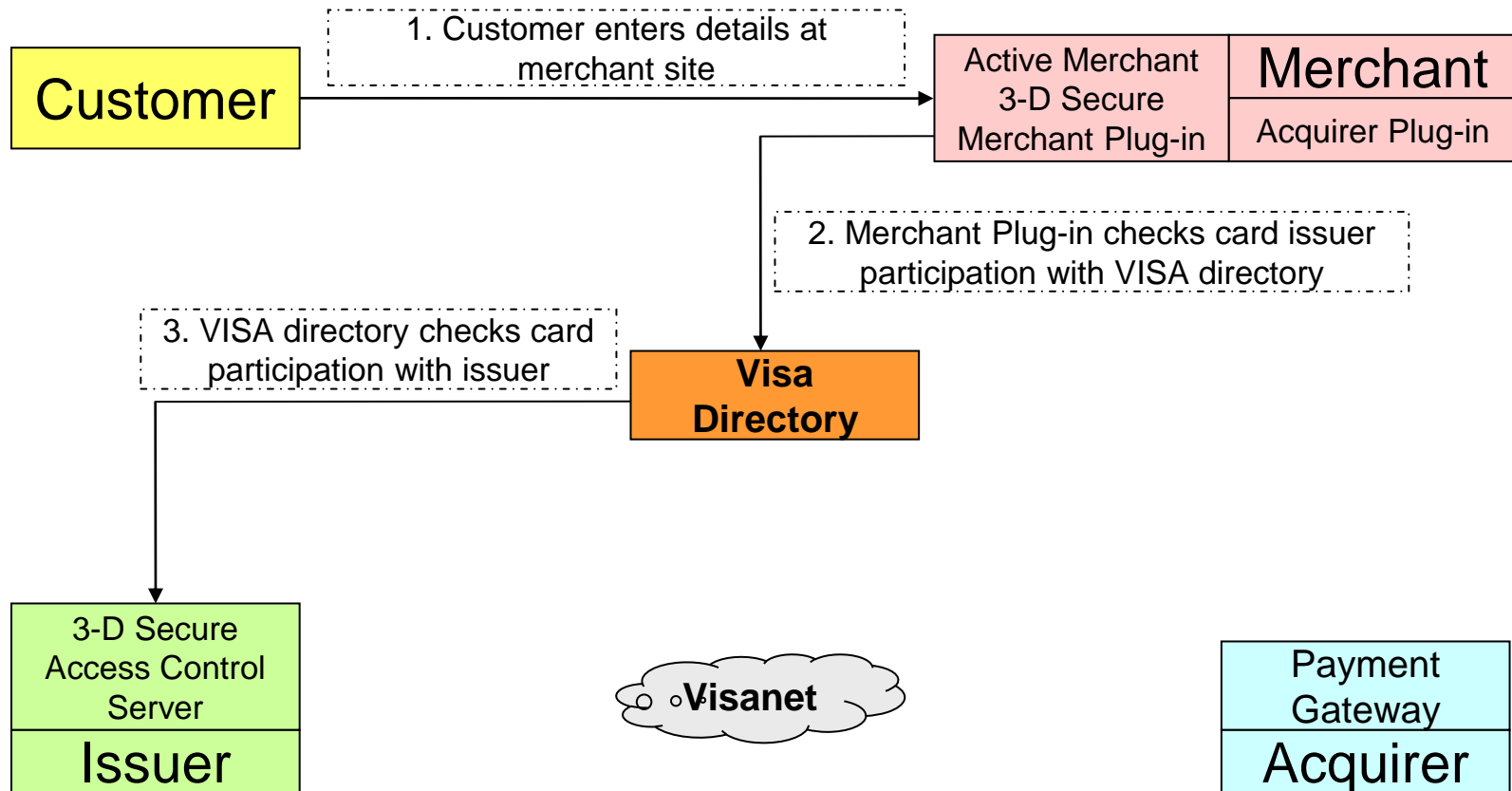
Overview of 3-D Secure



How Does 3-D Secure Work

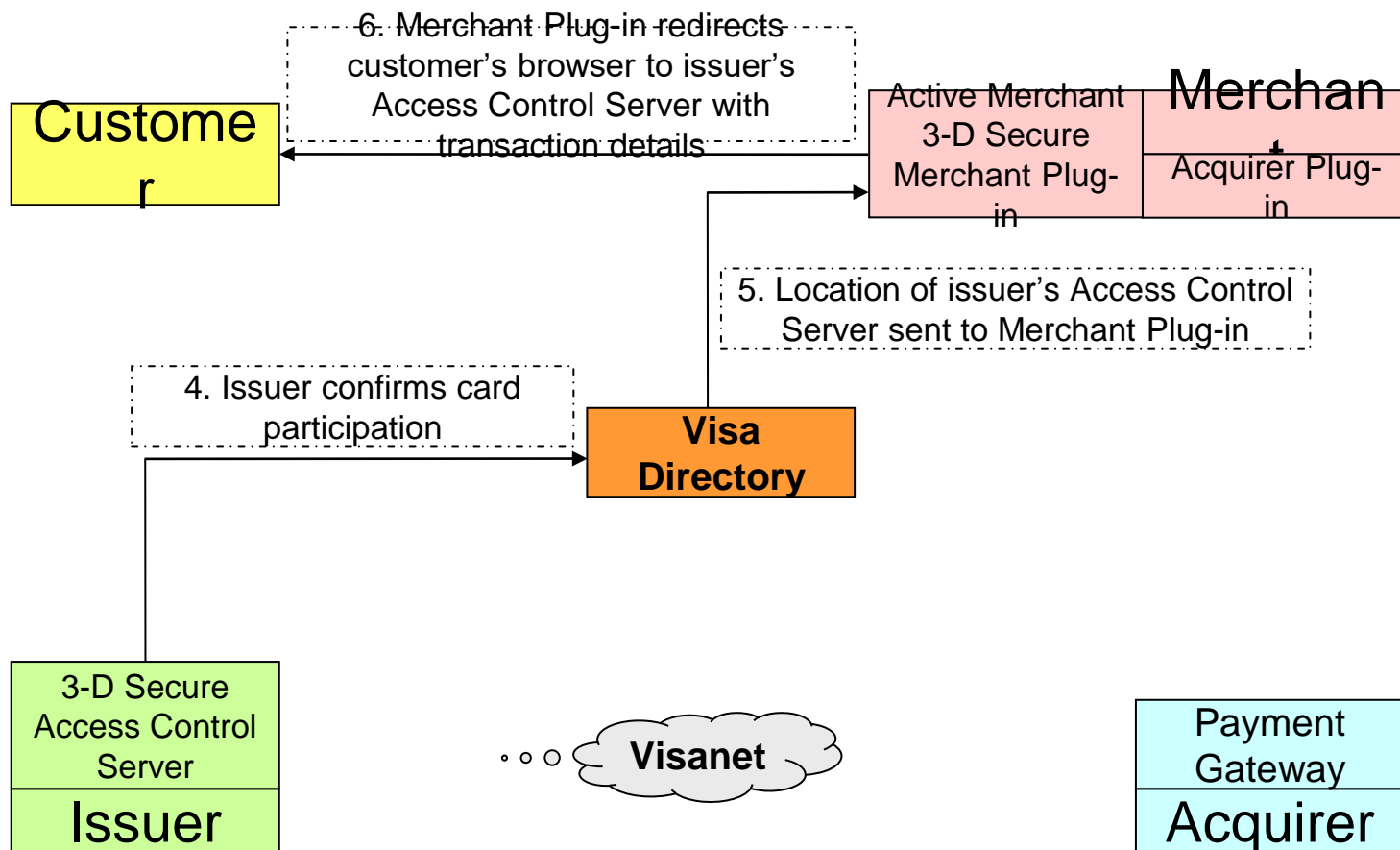


3-D Secure (1)



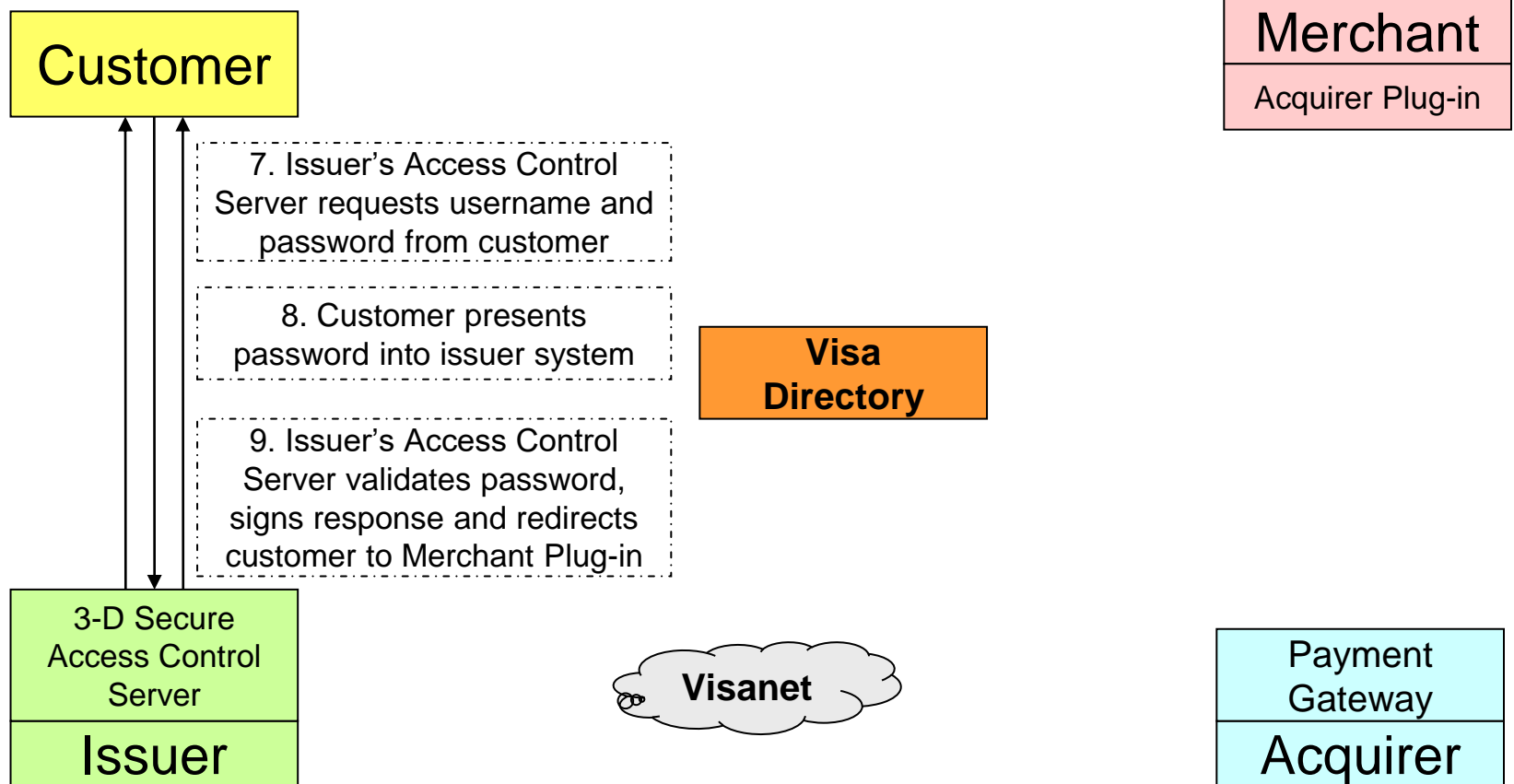
SOURCE:
[KMIS](#)

3-D Secure (2)



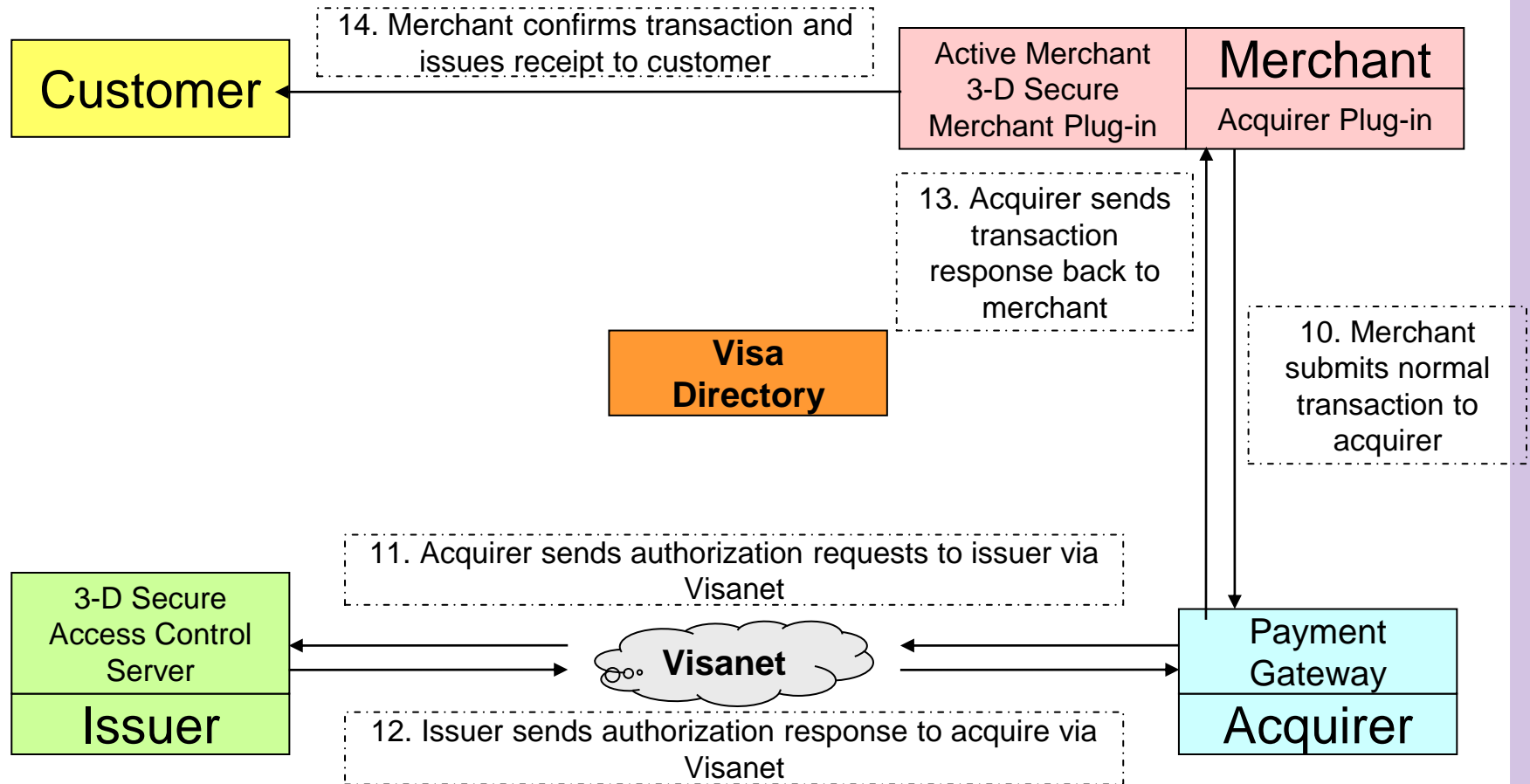
SOURCE:
[KMIS](#)

3-D Secure (3)



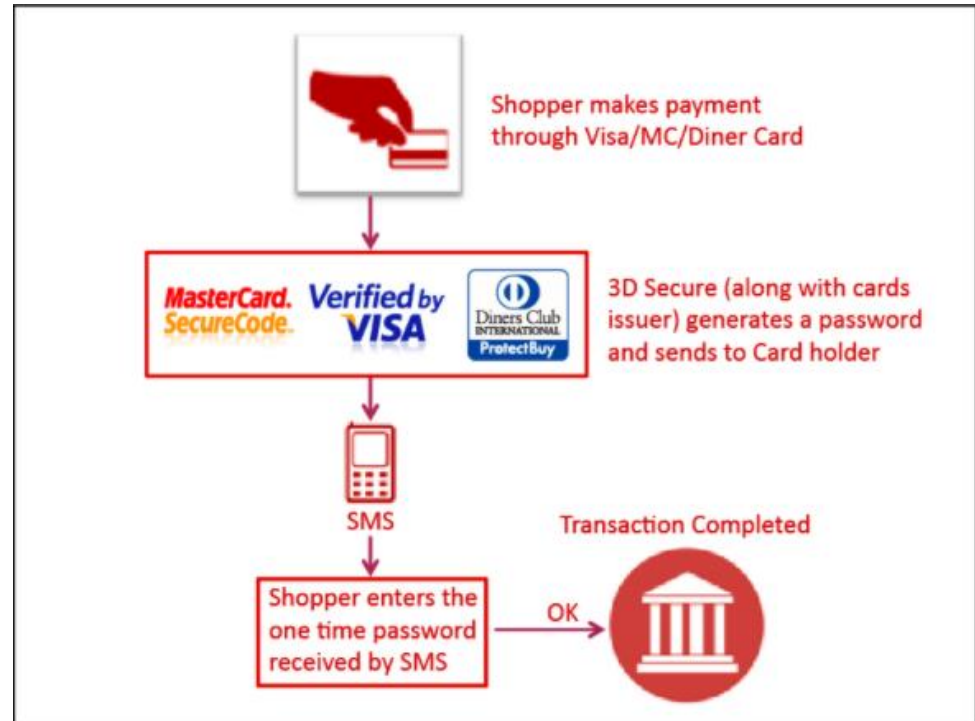
SOURCE:
[KMIS](#)

3-D Secure (4)



3-D Secure with OTP

- **Step 1** – Make an online purchase.
- **Step 2** – Enter your card details in the Payment section.
- **Step 3** – An SMS with a one-time password (OTP) will be sent to your registered mobile device.
- **Step 4** – Enter the one-time password (OTP) and complete your transaction.



Features of 3-D secure

- **Payment Authentication**
 - Issuers to verify that the person involved in e-commerce is a authorized cardholder.
 - Improved transaction performance to benefit all participants
 - Increase consumer confidence
- **Support variety of Internet access devices**
 - Personal Computer
 - Mobile Phones
 - Personal Digital Assistants



Benefit of 3-D Secure

- **Benefit for Cardholder**
 - Increased Customer confidence
 - No Application software is needed
 - Easy to use
- **Benefit for Merchants**
 - Ease of integration into merchant system
 - Reduce risk of fraudulent transaction
 - Decrease in disputed transactions



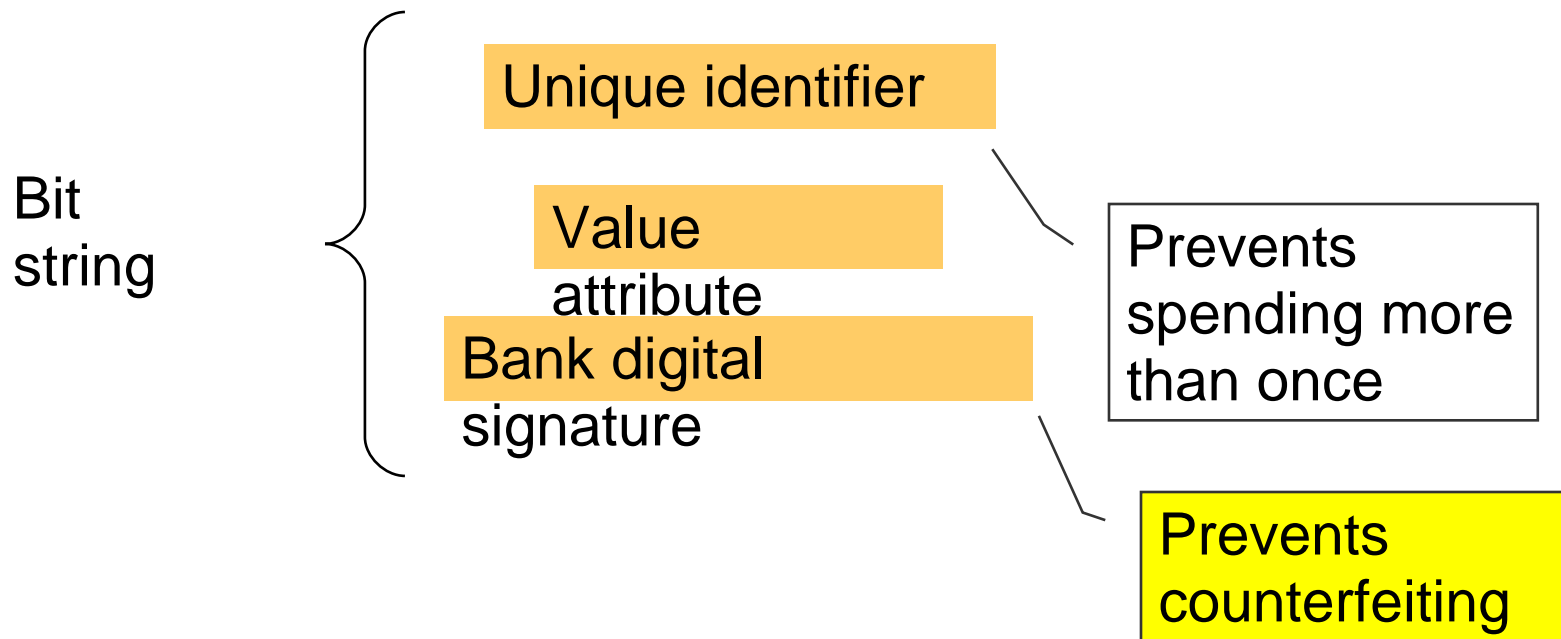
Digital Cash

01011010110101011101011010
10110101101010110101101010
11010101101010110111101011
11101101000000011010101011
0101

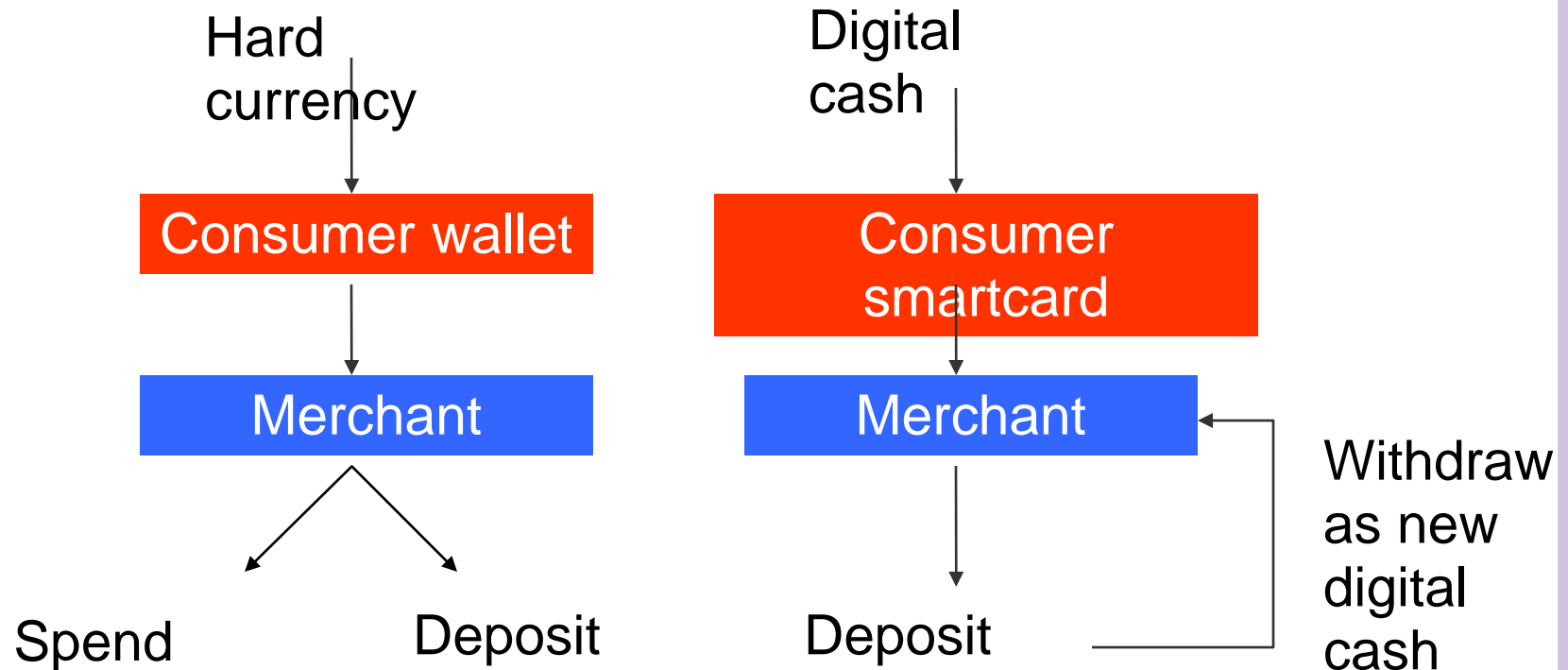
Since digital cash is represented by data, it is easily replicated. How do we prevent:

- Counterfeiting?
- Multiple spending?

What is a digital cash token?



Digital cash must be deposited



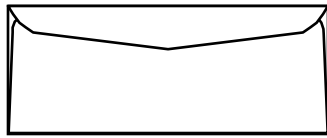
Possible Characteristics of Digital Cash

- Anonymity of consumer
 - Merchant knows who paid, but that information is not inherent to the digital cash itself
 - Financial institution knows what merchant deposited
- Attribution of cheating
 - Double spending
- Authorized traces

Blind Signature

Carbon
Token

Consumer gets bank to sign cash token without observing contents



Put token and carbon in envelope



Present to bank for embossing



Remove token from envelope

Spending Anonymity

Create \$\$,
including

Repeat n times



Cut and choose one



If the consumer's software creates the digital cash, and the bank signs it blindly, the bank will not see the identifier. The cut and choose protocol assures the bank the \$\$ is proper.

The Failure of Digital Cash

- There have been several proposals for digital money. All had failed.
- No gain over existing systems:
 - Still need a central point of trust
 - Privacy: Who monitors the system?
 - Can we entrust a bank with managing an entire currency?

Digital Cash vs Digital Currency

- **Digital cash:** Electronic version of existing currency (USD)
- **Digital currency:** Entirely new currency (i.e. Bitcoin)

Making Money Digital

- Why not create a currency based on cryptography?
- Design goals should be a currency with the following properties:
 - 1. Secure transfer in computer networks
 - 2. Cannot be copied and reused
 - 3. Anonymity
 - 4. Offline transactions
 - 5. Can be transferred to others
 - 6. Can be subdivided

Bitcoin

- The Bitcoin protocol was proposed in 2008 by **Nakamoto**
- Takes care of:
 - Creation of new currency
 - Secure transactions
 - Protection against double-spending
 - Anybody can be a “merchant” or a “customer”.
 - Pseudo-anonymity



The Advent of Bitcoin

- 2009: **Bitcoin announced** by Satoshi Nakamoto
 - *Pseudonym for person or group of person*
- 2009-2011: slow start...
- 2011-2013: Silk Road and Dread Pirate Roberts
- End 2013: **Bitcoin price skyrockets**
 - *and the world notices!*

We will now create Bitcoin from scratch

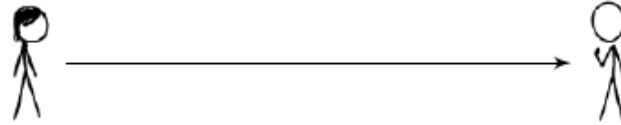
- Step by step, we create a peer-to-peer currency.
- In each step we discuss strengths and weaknesses.
- Let's call one unit of currency "BitKasi".
- BitKasi = the protocol
- bitKasi = the currency

BitKasi version 1: Public, signed transactions

- Kasun publishes a signed message: “I, Kasun, send one bitkasi to Chamath”
- **Good stuff:**
 - Chamath can verify the signature as being from Kasun.
 - The transaction cannot be undone
- **Bad stuff:**
 - No account balances
 - Infinite number of bitKasi
 - Very incomplete. . .



BitKasi version 2: Serial numbers



- “I, Kasun, send bitkasi no. 856034 to Chamath”
- Duplicate transactions are easily spotted.
- How are the serial numbers created?
- The (too) easy solution: Serial numbers generated by a trusted source, like a bank.

No Central Point of Trust, Instead a Blockchain

- We remove the central point of trust.
- Instead, we establish a list of all transactions ever made.
- Computing an account balance is done by summing over all previous transactions for that account.
- This list is called the **blockchain** and is shared by all users.

BitKasi Version 3: The blockchain



- Chamath checks his blockchain before accepting the transaction
- If he sees that the bitkasi in question is owned by Kasun, he accepts it.
- After the transaction is complete, Chamath broadcasts his acceptance.
- As soon as the other peers hear this broadcast, they will not allow double-spending.

Double-spending is Still Possible



- Kasun can perform a double-spend before the acceptance broadcast is heard by enough peers
- To solve this problem, we make Chamath ask everybody else if a transaction is valid.
- Double-spending will be noticed before payment is accepted.

Asking the Network about the Transaction

- How many answers should Chamath require? How can the answers be trusted?
- A “majority vote” is impossible, what if Kasun spams Chamath with false confirmations?
- There is no way to perform traditional authentication.
- But BitKasi won't work if transactions can't be reliably verified. . .

BitKasi version 4 (final): Proof of work

- The finished BitKasi protocol uses Proof of Work (PoW).
- Basic idea: We only trust solutions that are accompanied by a proof of someone having committed a large amount of resources to a problem.
- That is, we don't authenticate a user, but we authenticate the fact that time/money/energy/etc. has been spent.
- In order for Kasun to make a double-spend, he first has to spend energy before Chamath trusts him.
- Even better: We turn proof-of-work into a competition.

Constructing the PoW Challenge

- We want a problem that. . .
 - is difficult to solve
 - has solution(s) that are easy to verify
 - has scalable difficulty (will be discussed later)
- Remember one-way hash function $h(x)$ has the
- following properties:
 - Easy to calculate $h(x)$ from x
 - Given $h(x)$, it is hard to find x_0 so that $h(x_0) = h(x)$.
 - Finding preimages is the perfect proof of work!

The Verifications are Done by Miners

- Kasun's transaction message m is broadcast:
- “I, Kasun, transfer bitkasi no. 3869303 to Chamath”.
- A miner selects a random k and computes $h(m + k)$.
- If $h(m + k) > T$ the miner chooses a new k and tries again.
- After a long time we get $h(m + k) < T$ and the miner broadcasts k .
- Chamath receives k and checks that $h(m + k) < T$.
- We will talk more about T in a minute.

A simple example of Proof of Work

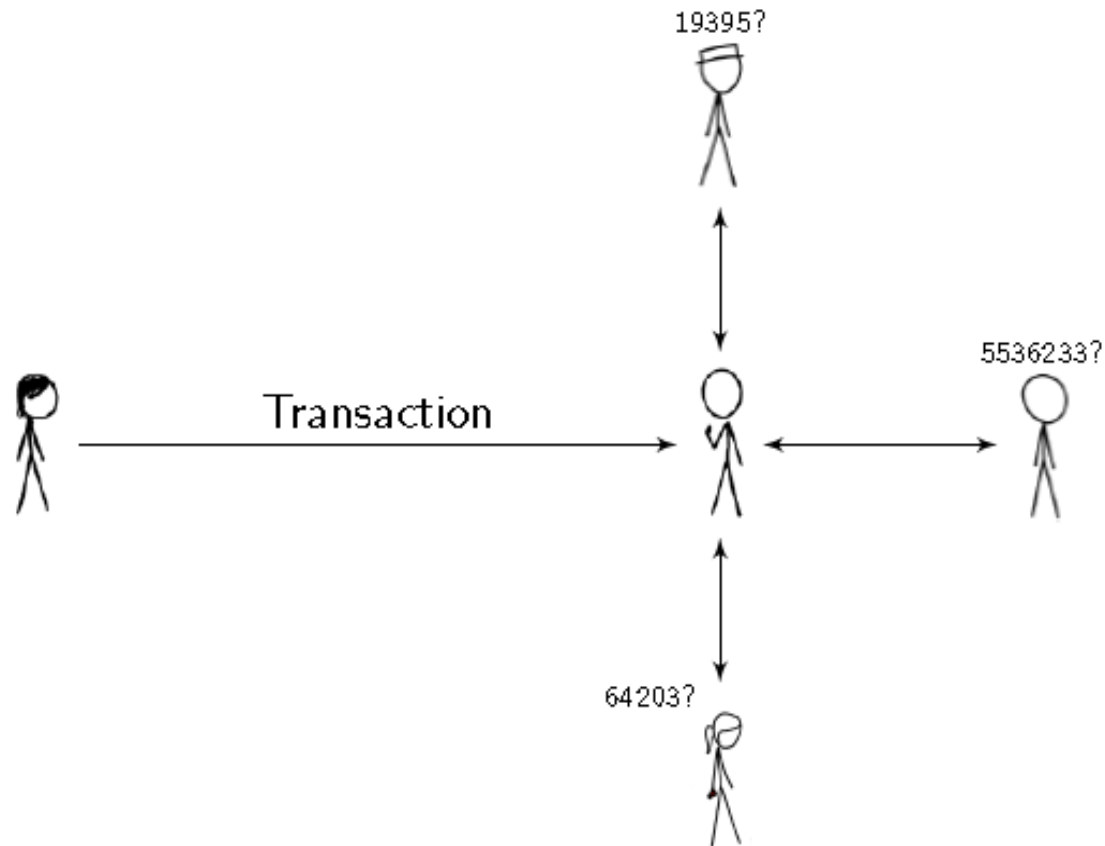
- Let the threshold T be so that the hash value $h(m + k)$ needs five leading zeros and let $m = \text{"AAA"}$.

$m + k$	$h(k + m)$
AAA0	802dbe2e69...
AAA1	bbfce0d522...
AAA2	7bb4db476f...
...	...
AAA770239	00000921ac...

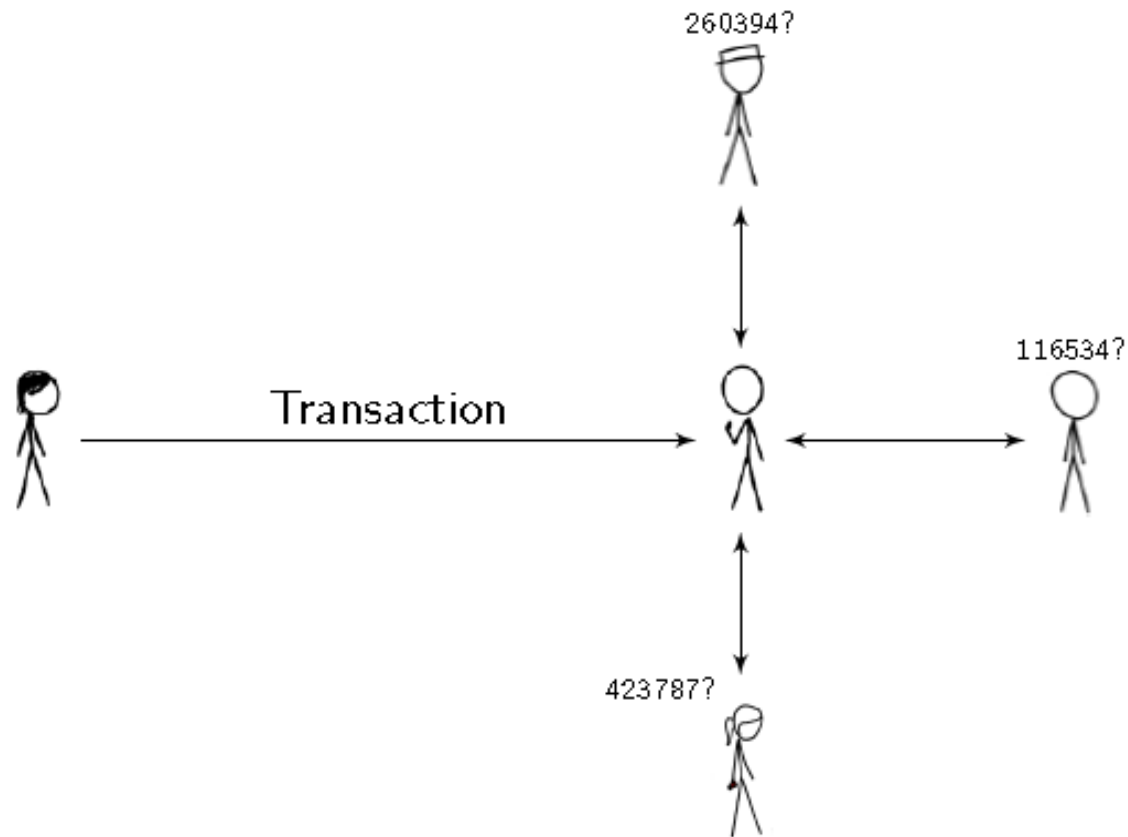
$k = 770239$ is a valid solution

- Note that in the normal case, k is chosen randomly.
- There are several solutions k to the problem $h(m + k) < T$

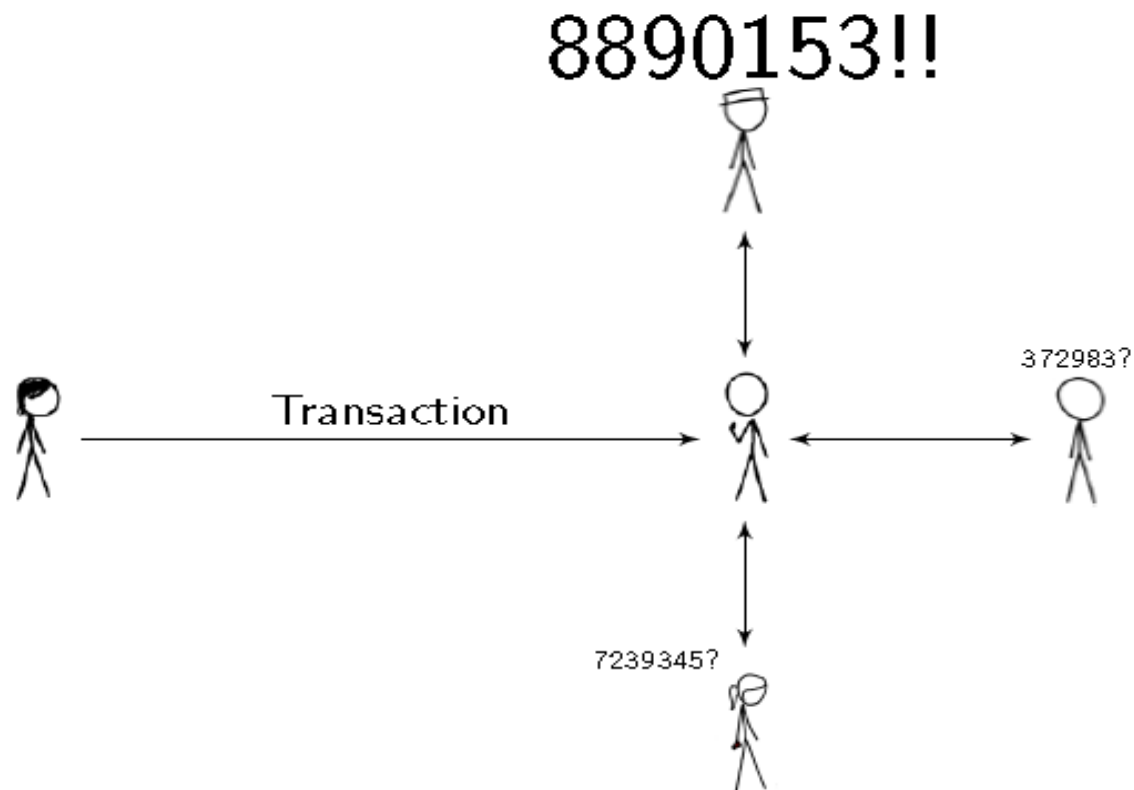
Mining is a Competition to Find a Solution



Mining is a Competition to Find a Solution

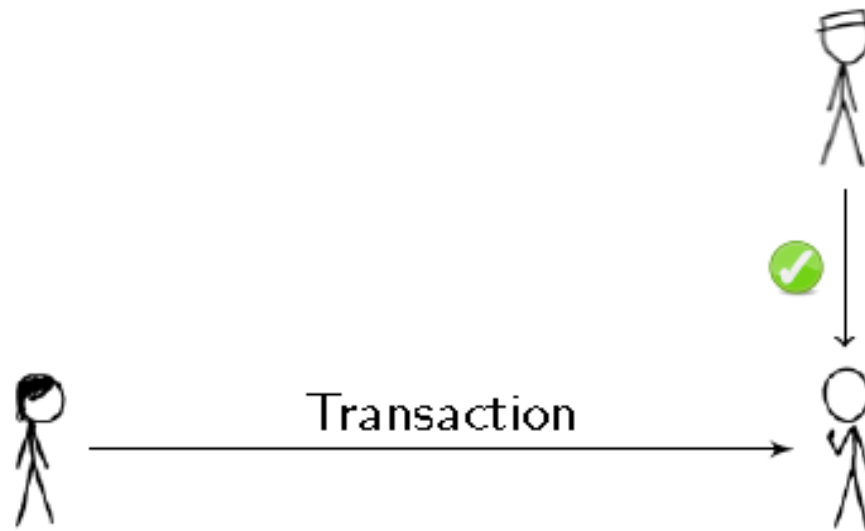


Mining is a Competition to Find a Solution



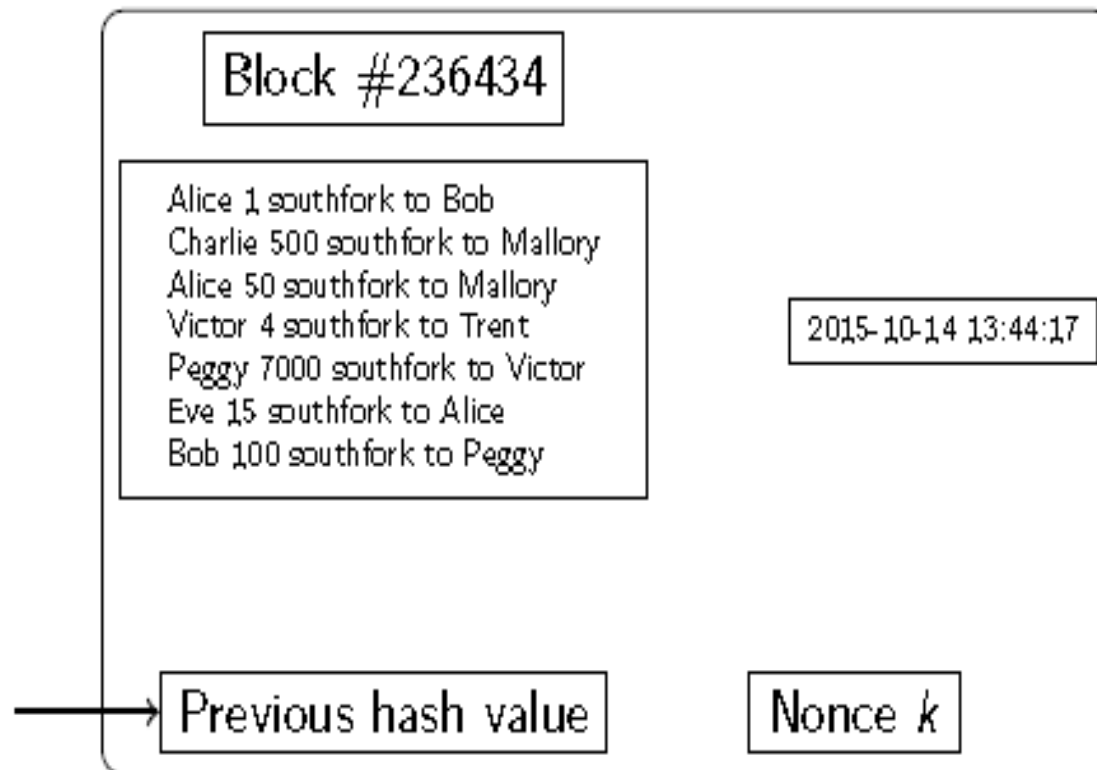
Charlie is the lucky winner

Mining is a Competition to Find a Solution



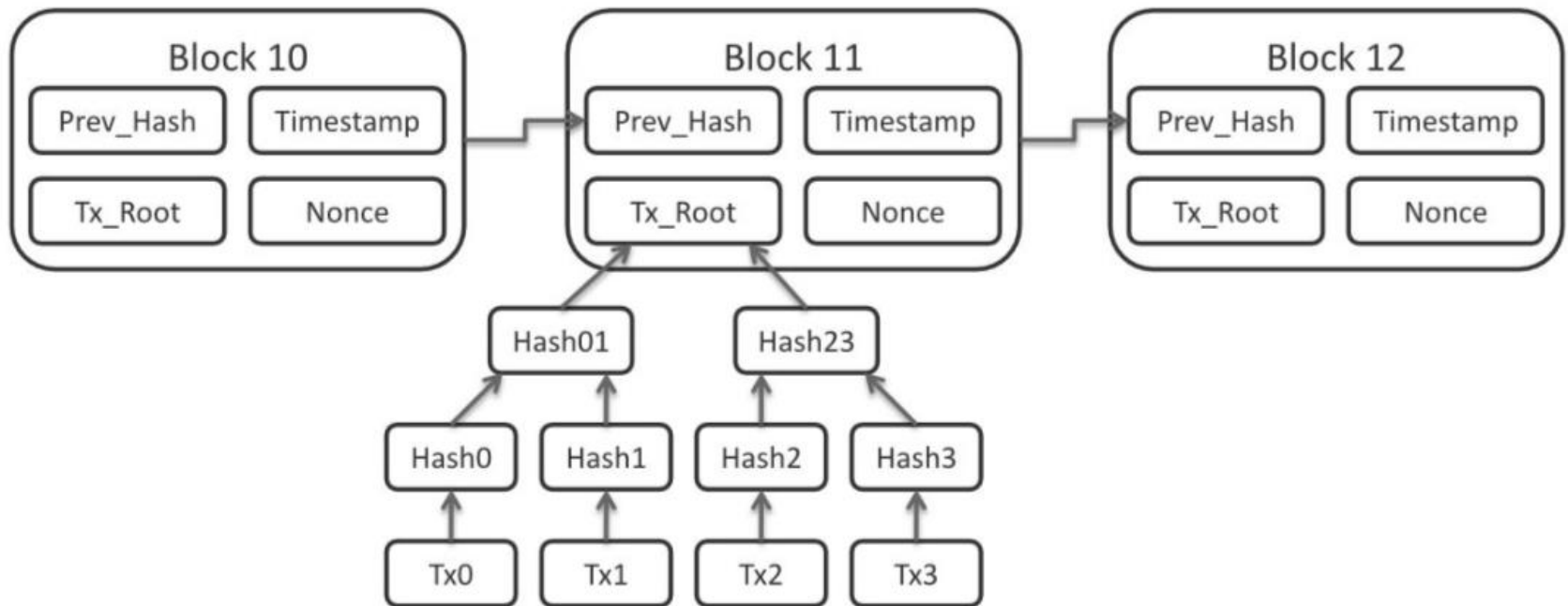
- Chamath can trust the acknowledgment from Charlie.

A Block is a Large Number of Transactions



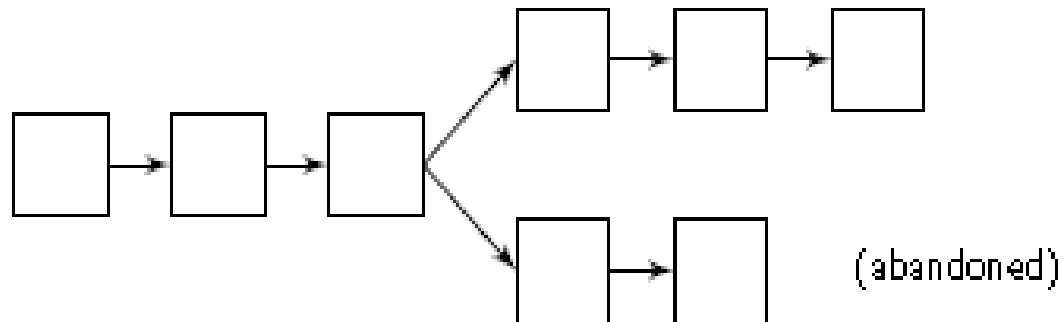
A block is only valid if its hash value is less than T .

Merkle Hash



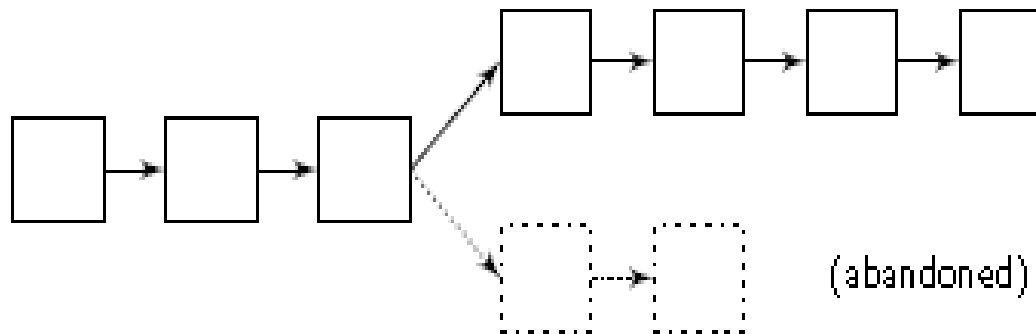
Transactions are Verified by Miners

- The process of turning transactions into blocks is mining.
- The blocks are numbered and form a long chain, blockchain

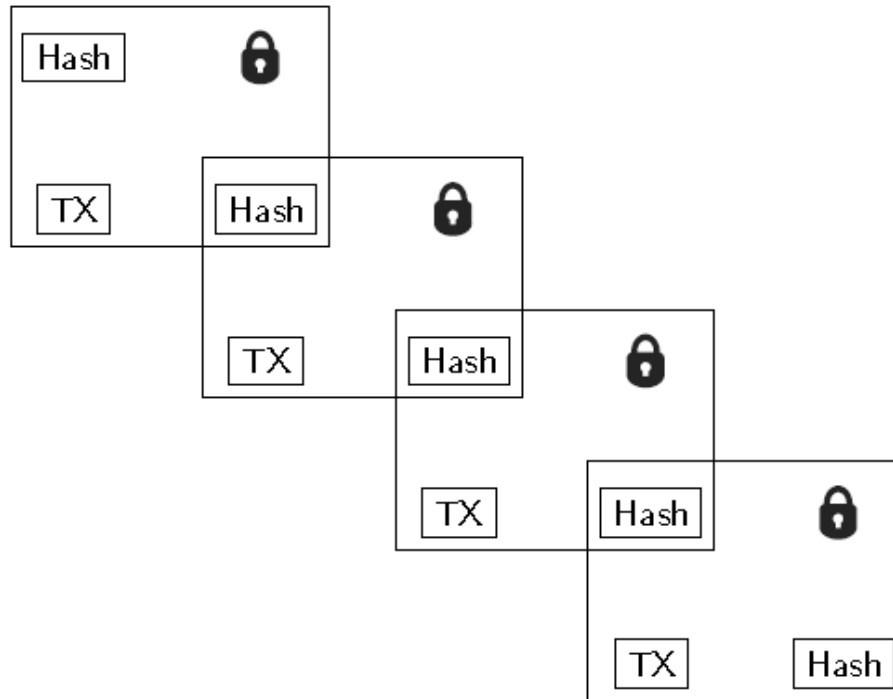


Transactions are verified by miners

If two miners find a valid block simultaneously, the resolution strategy is to randomize and then work on the longest chain.



Each Block Gives Security to the Previous Ones

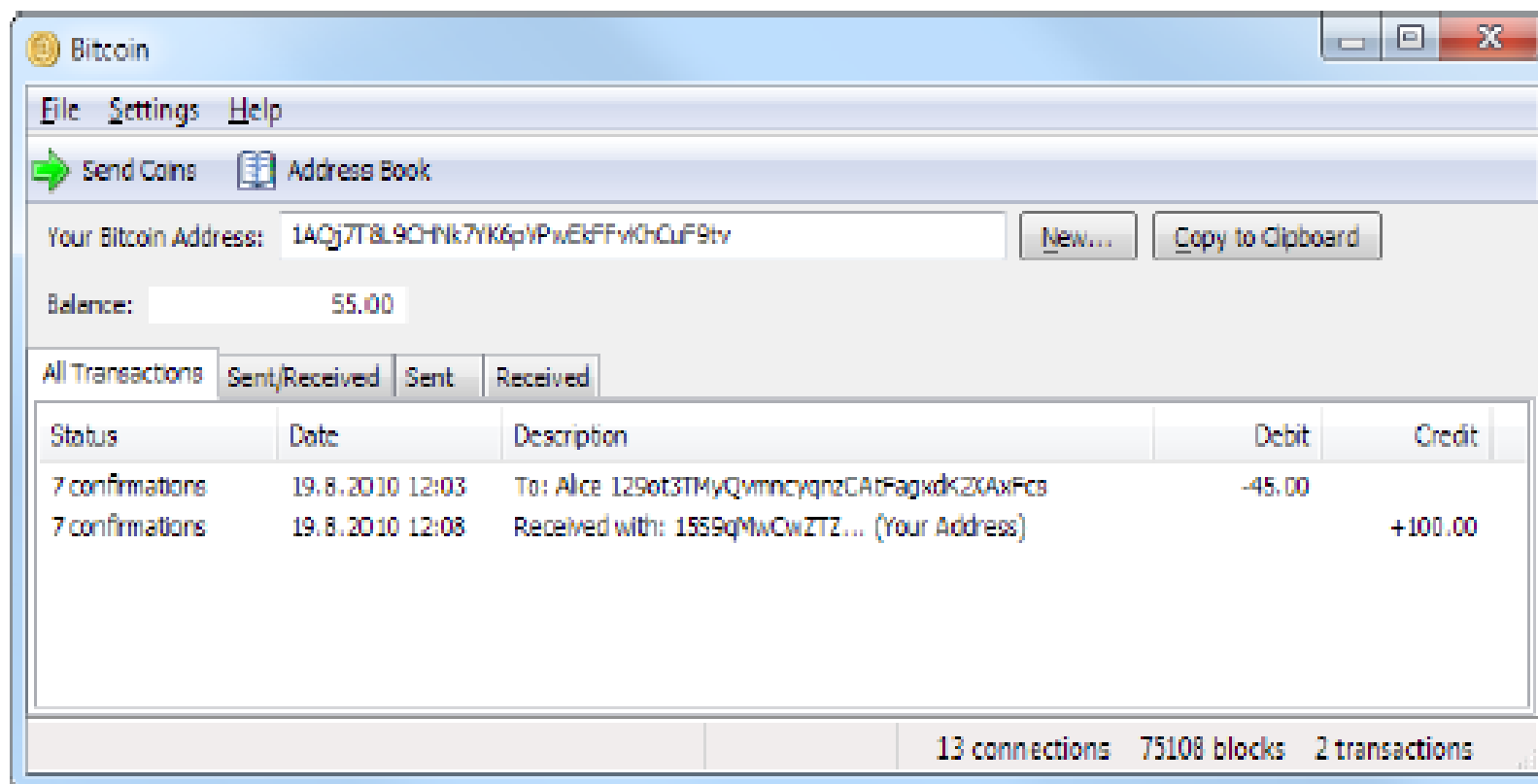


Chamath waits a number of blocks before accepting Kasun's transaction

This is how Bitcoin works!

- BitKasi now essentially works like Bitcoin.
- Digital signatures initiate the transaction
- Miners verify the transactions
- Chamath accepts the transaction after six successive blocks (takes one hour).
- New currency is created by rewarding miners.
- All transactions are in the blockchain.
- Anybody can see all transactions
- Today, the blockchain takes up more than 140 gigabyte

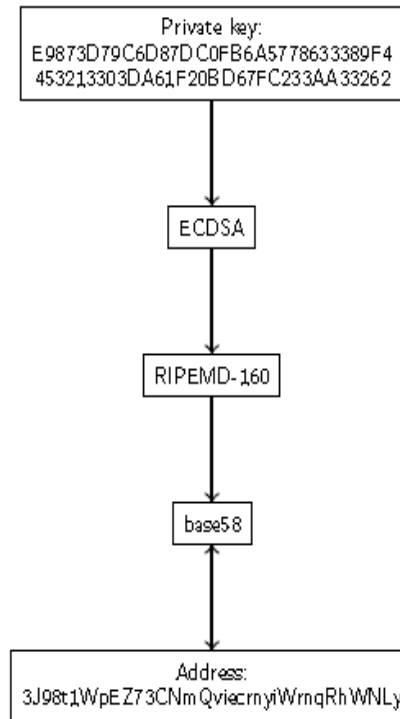
Sending and Receiving Bitcoin



A bitcoin wallet

Sending and Receiving Bitcoin

- Bitcoin uses cryptographic addresses.



How to transfer money

(Digital) Signatures


- Only you can sign
- Everyone can verify
- You cannot deny



1025

DATE _____

PAY TO THE ORDER OF Give coin 3 to Chamath \$

_____ DOLLARS  Security Features Included. Details on Back.

MEMO kasun

⑈0000000000⑈ ⑈0000000000⑈ 1025

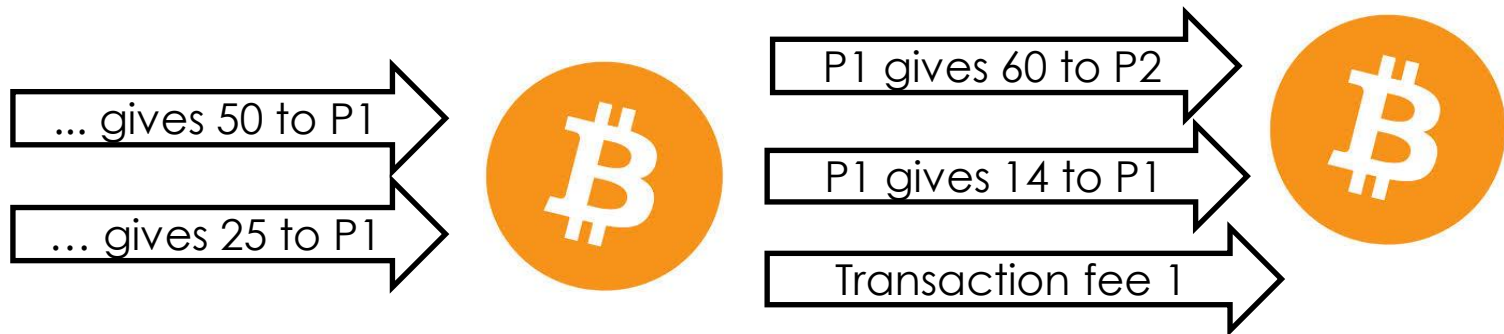
Transactions

- What makes a transaction valid?
 - **Proof of ownership** (a signature)
 - Available funds
 - No other transactions using the same funds

Instead of accounts like one might expect, Bitcoin uses an **Unspent Transaction Output (UTXO)** model to ensure that funds are used only once.

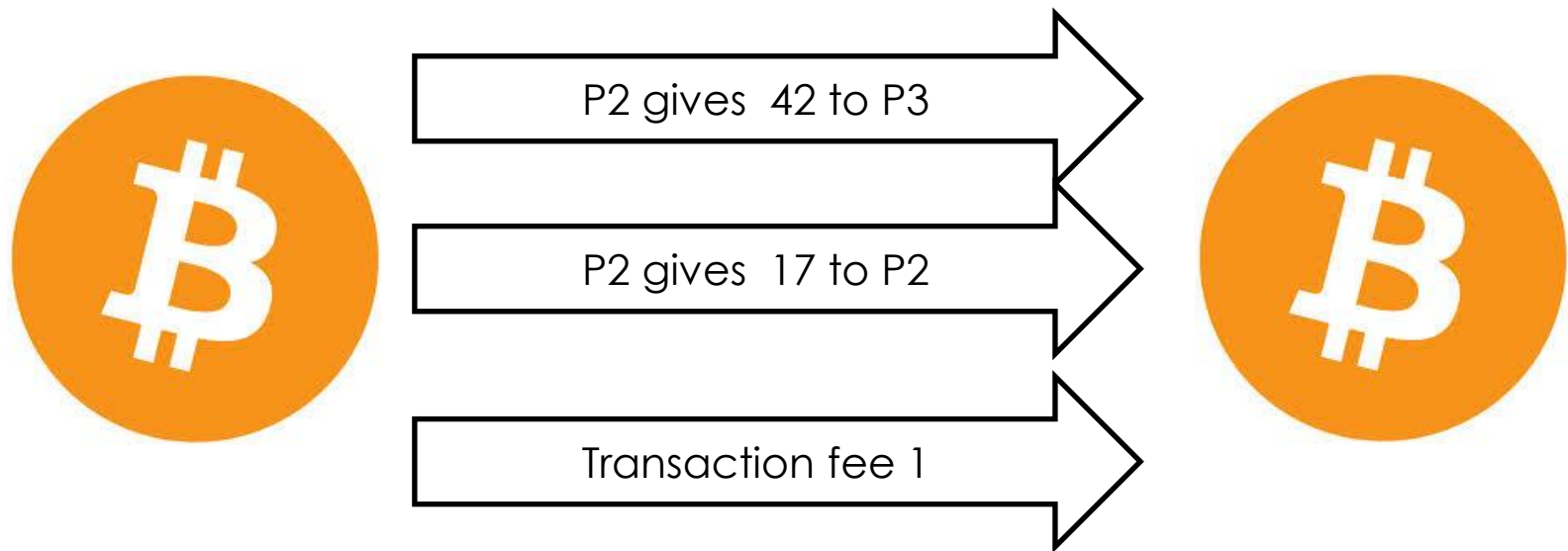
How is money transferred in Bitcoin?

Example: P1 wants to give 60 to P2



How is money transferred in Bitcoin?

Example: P2 wants to give 42 to P3

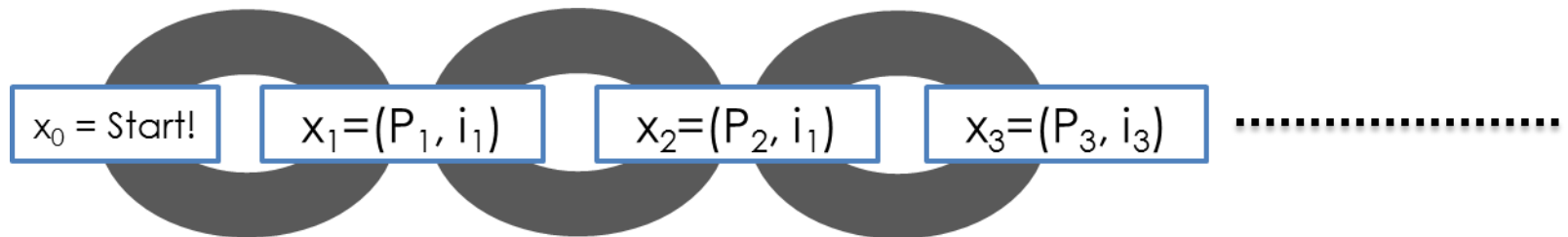


How to store money



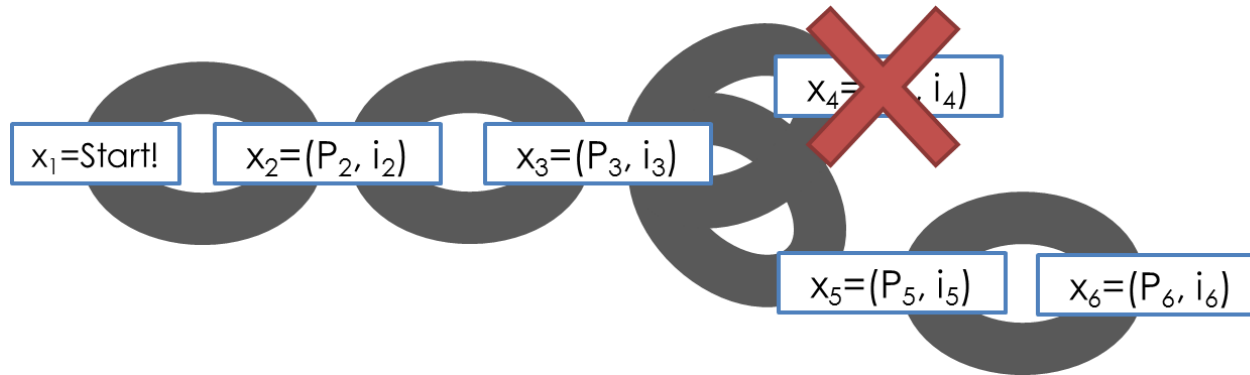
Main Idea:

Record every **transfers** in the **blockchain**



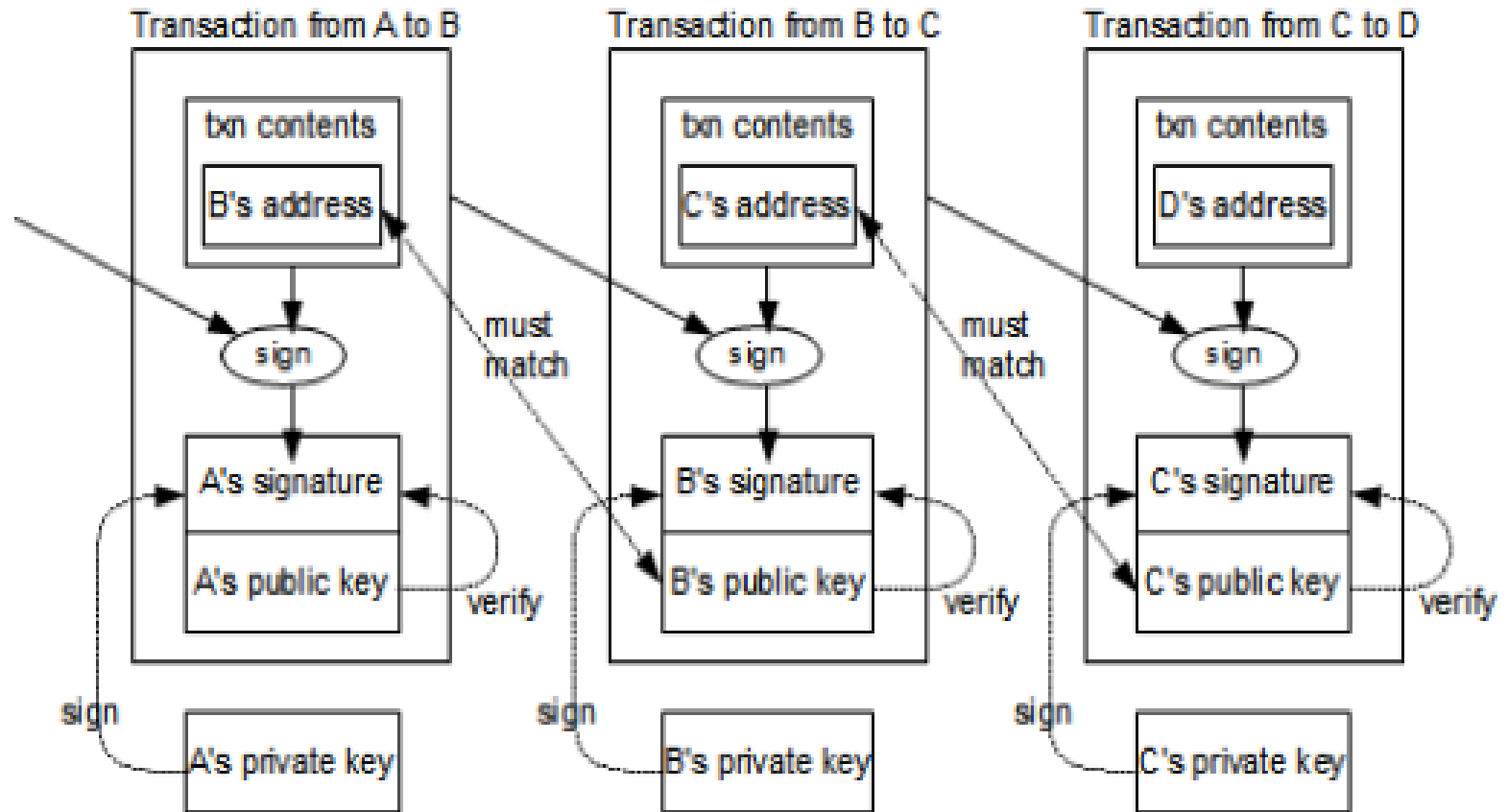
How is money stored in Bitcoin?

- Transaction in **orphaned blocks** are invalid
 - **Wait 6 blocks** (~1 hour) before accepting transaction.
 - **Checkpoints** to prevent complete history rollback.



- All transaction** are stored in the blockchain
 - (Currently ~150 GB)

Detailed view of a transaction



How is money created in Bitcoin?

- Miners use special software to solve math problems (Bitcoin algorithm), and upon completing the task they receive certain amount of coins.
- They are created each time a user discovers new block (Initial 50 BTC, 25 BTC, 12.5 BTC).
- Software is creating new units until it reaches amount of 21 million unites (currency with Finite Supply).
- The rate of block creation is approximately consistant over time (6 per hour) with 50 % reduction every four years.
- Halving (in theory) continues until 2110-2140 when 21 million BTC have been issued.

Bitcoin mining has scalable difficulty

- Bitcoin dynamically scales the mining difficulty.
- The goal is one mined block per 10 minutes, globally.
- Smaller T gives higher difficulty.
- Currently, you need hash values beginning with 16 (!) zeros.
- 0000000000000000000000001093a79b7a3a5939f7b032b7e6927799eed667149dc71007

Bitcoin and trust

- In Bitcoin, the users only need to trust the algorithm, nothing else.
- In contrast, with traditional currency trust in the central bank,
- The Bitcoin protocol is a system without inherent trust.
- You don't even need to trust the initial creator, Nakamoto

Pros and cons of using Bitcoin

PROS



- Independent currency (account cannot be frozen)
- Little to no transaction fees (perfect for sending money overseas or travelling)
- Secure transactions (encrypted)
- Unlimited transfers and amount can be sent
- It's essentially anonymous*

CONS

- Unstable value (bitcoin currency can increase or decrease drastically)
- Volatile market (unpredictable)
- Not widely accepted (for now...)
- Payments are irreversible (no money back guarantee!)

Comparison to US Dollar

US Dollar (Cash)

- Backed by United States?
- Controlled by US
- Primarily US-only
- Created by government
- Supply controlled by politics
- Easy to steal by muggers
- Hard to steal by hackers
- Hard to transmit
- Hard to trace
- Non-refundable
- Used for crime

Bitcoin

- Backed only by other users
- Controlled by users
- International
- Created based on work done
- Fixed number issued
- Hard to steal by muggers
- Easier to steal by hackers
- Easy to transmit
- Hard to trace
- Non-refundable
- Used for crime

The Challenges

- As a currency, bitcoin is very young.
- Transactions are safe, storage is not.
- If Alice loses her key, she loses her money.
- If Eve finds Alice's key, she can take her money and gets away with it.
- Many questions remain: Taxation? Volatility? Illicit trade?

Thank You

