

Bachelor of Computer Science

SCS2214 - Information System Security

Handout 9 - ePayment Protocols

Kasun de Zoysa
kasun@ucsc.cmb.ac.lk



UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING



Characteristics of Payments

Properties :

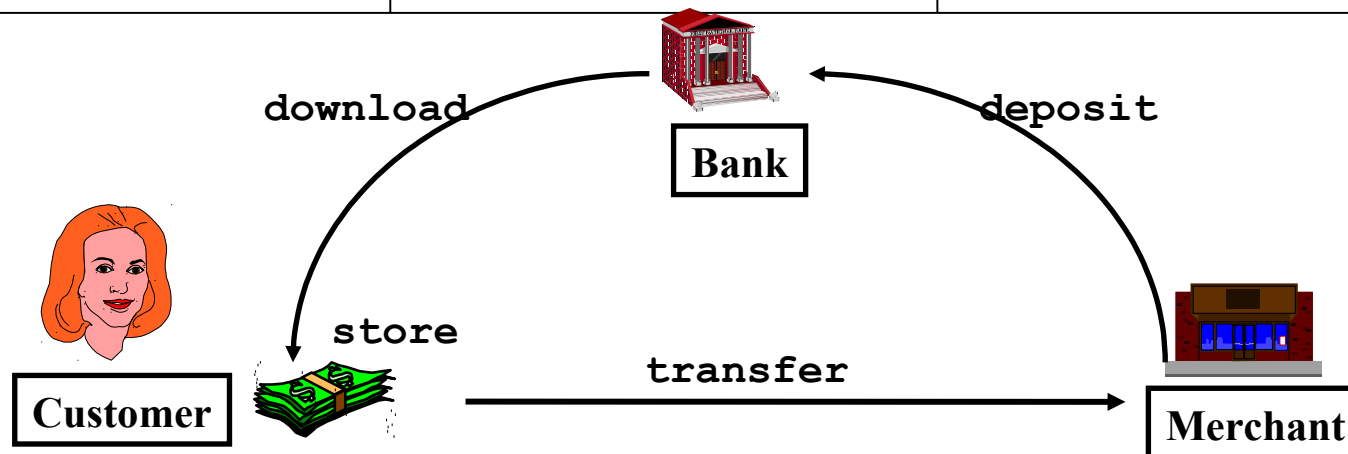
- where is the money (authorization)
- time of payment vs. time of order/shopping

Characteristics of payment methods :

	Money	Time
Type of payment 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

Internet transactions

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



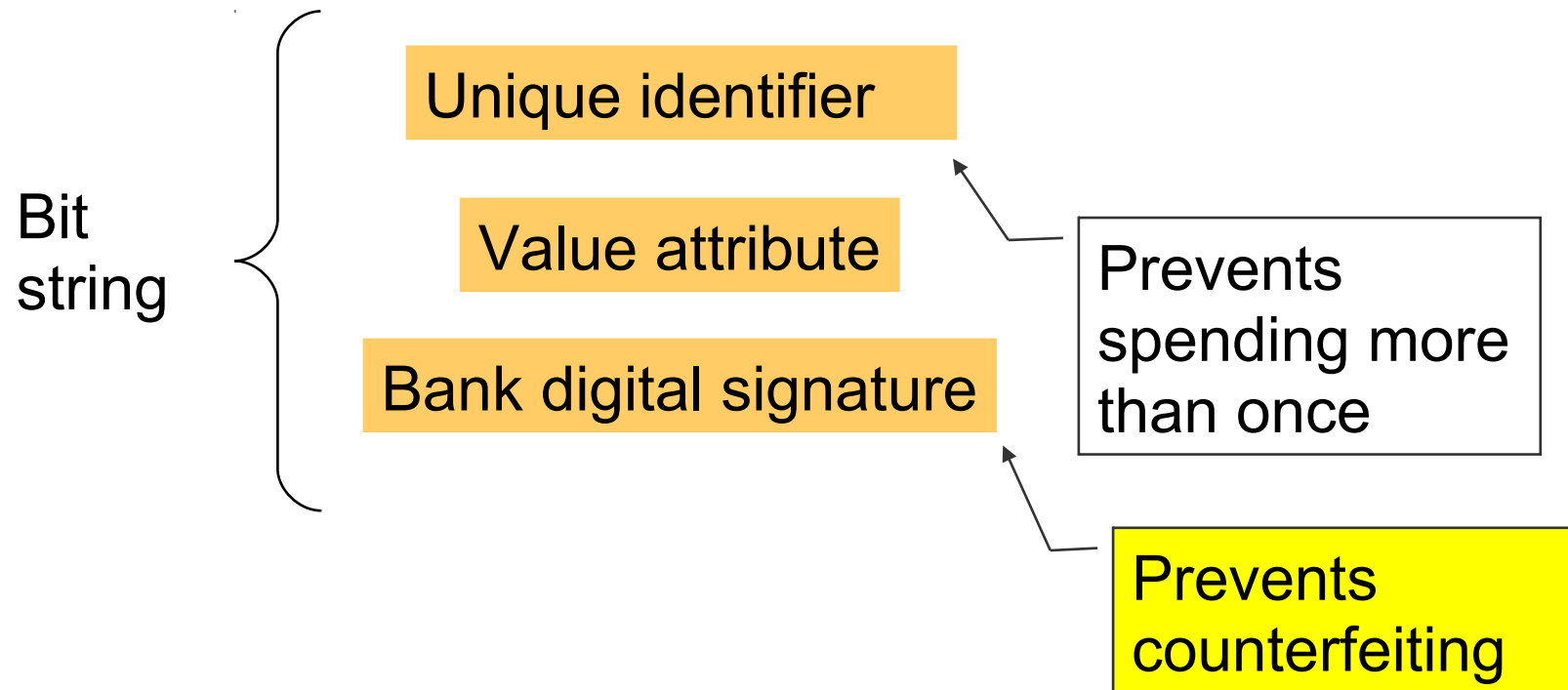
Digital cash

```
010110101101010111010110101  
011010110101011010110101011  
010101101010110111101011111  
011010000000110101010110101
```

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

- Counterfeiting?
- Multiple spending?

What is a digital cash token?

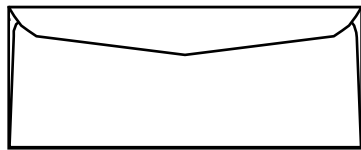


Blind signature analogy

Carbon

Token

Consumer gets bank to sign cash token without observing contents



Put token and carbon in envelope

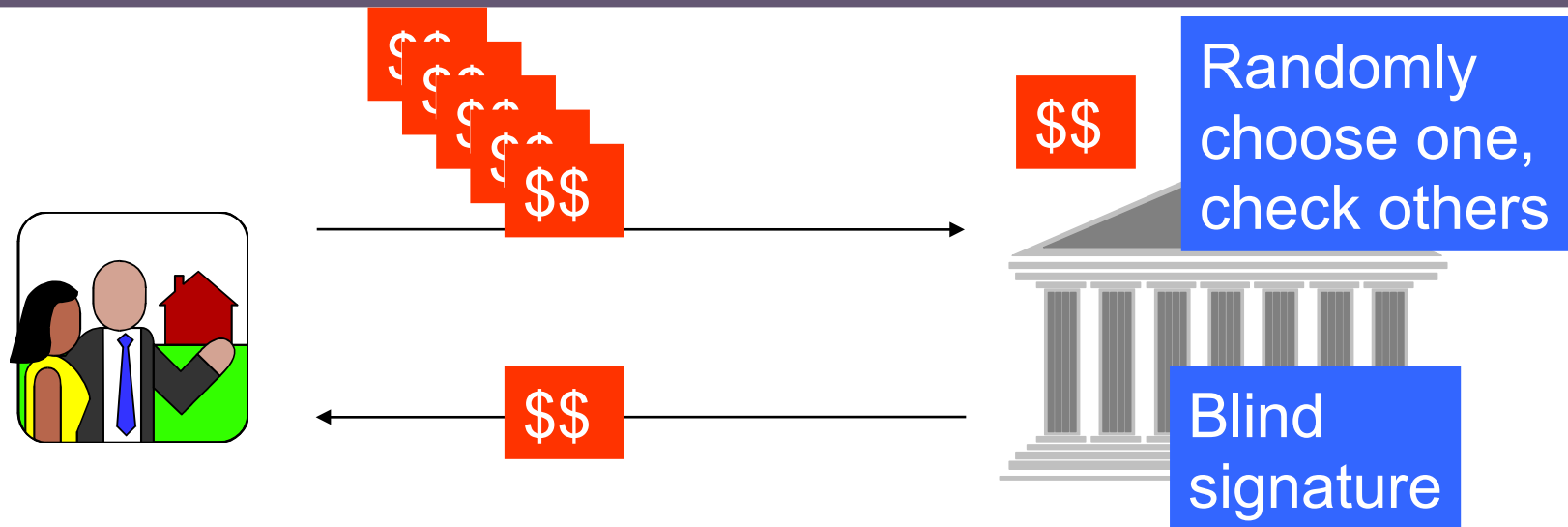


Present to bank for embossing



Remove token from envelope

Cut and choose protocol



Although the bank can't see what it is signing, with the cut and choose the incentive for the consumer is to generate legitimate instances of digital cash.

Chaum's anonymous e-cash

anonymous

secure (no double-spending)

only **transfer** (no creation/storage)



...and **bankrupted** in 1999

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

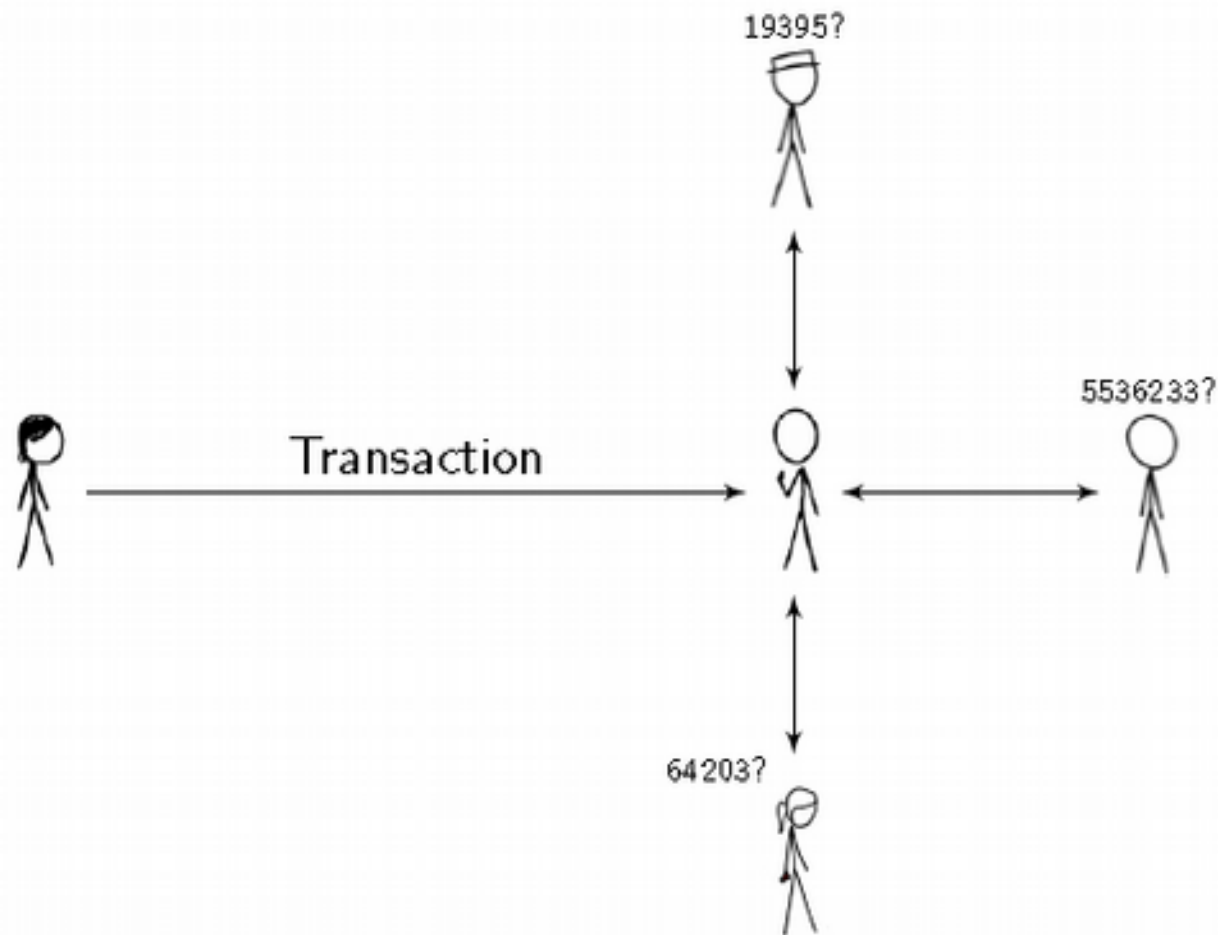
Let the threshold T be so that the hash value $h(m + k)$ needs five leading zeros and let $m = \text{"AAA"}$.

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

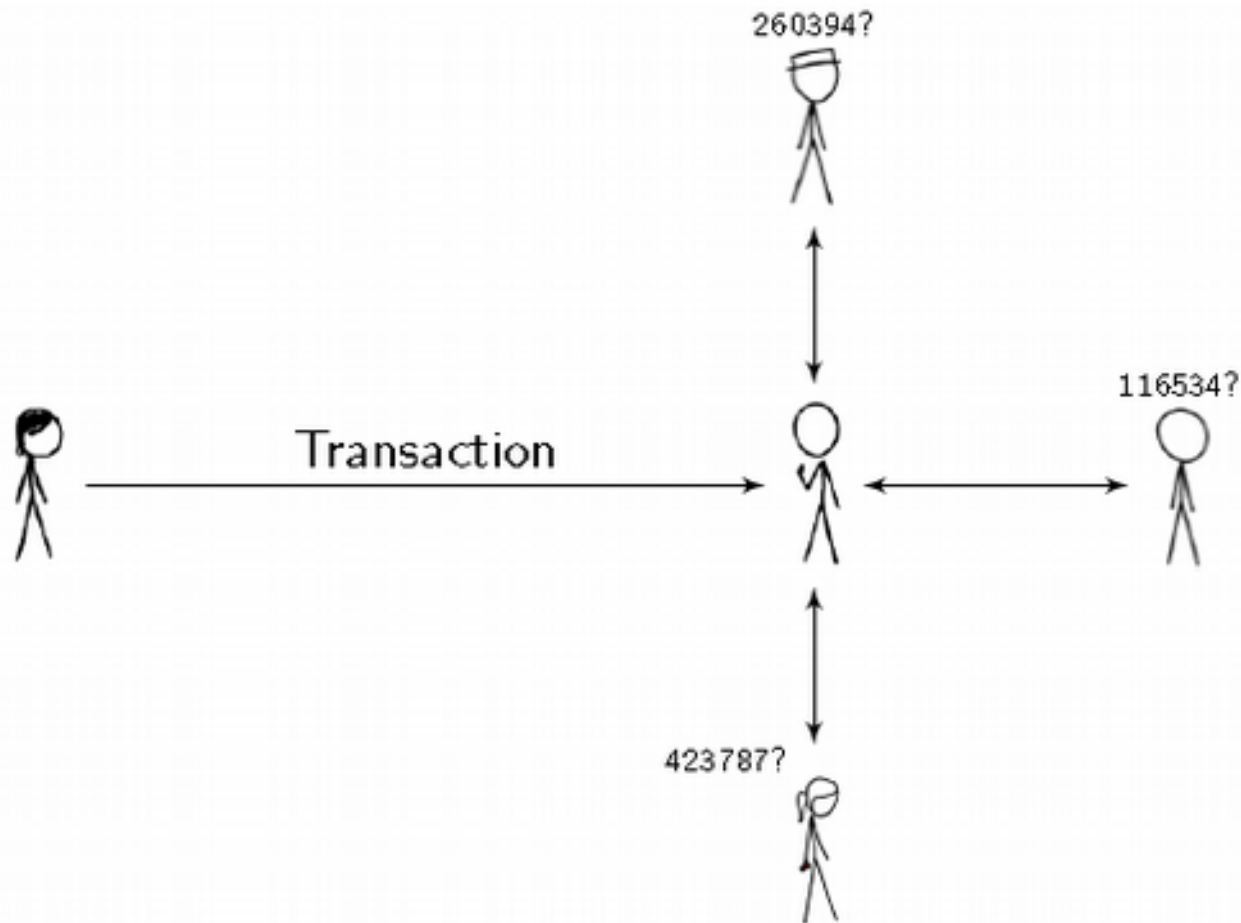
$k = 770239$ is a valid solution

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

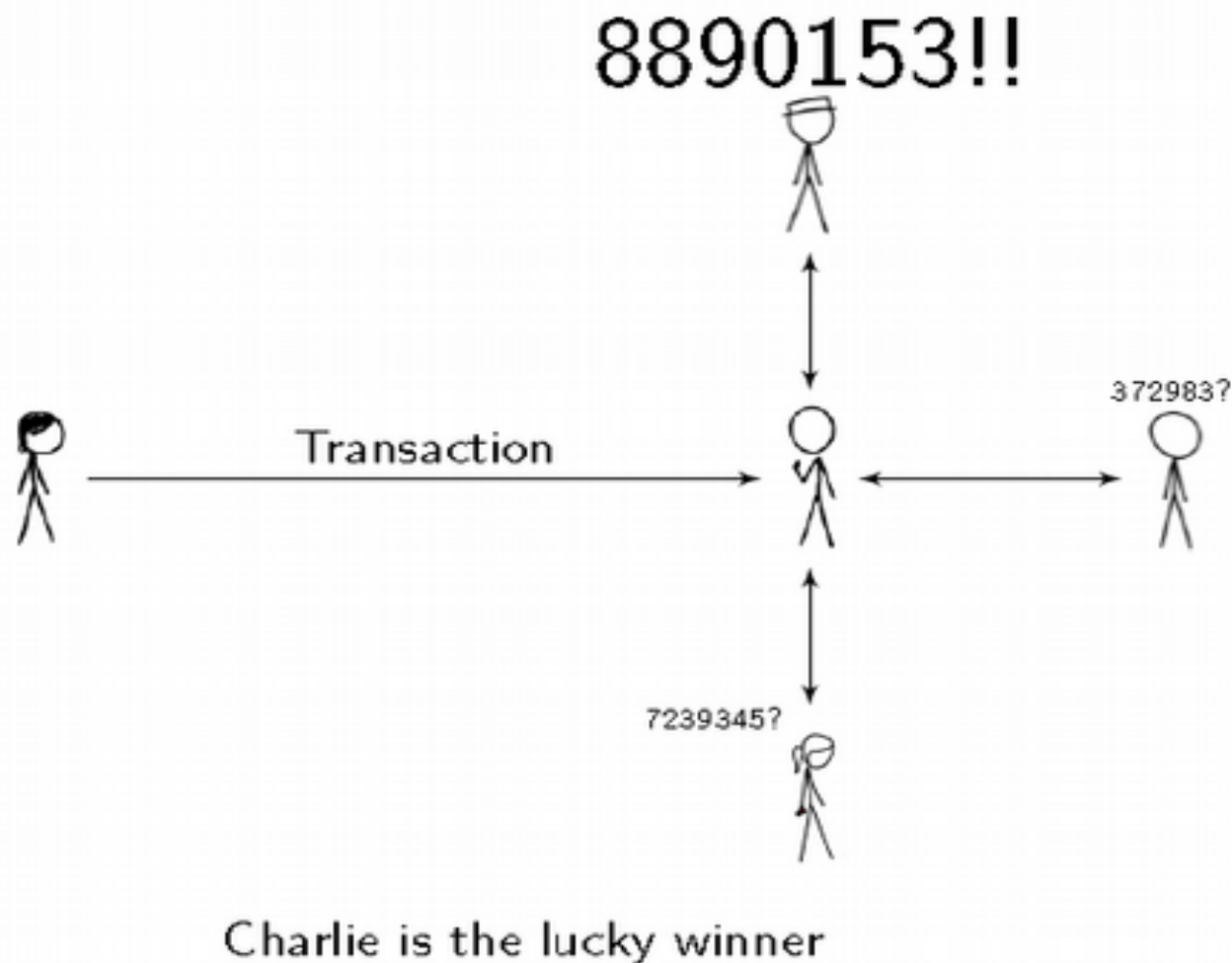
Mining is a competition to find a solution



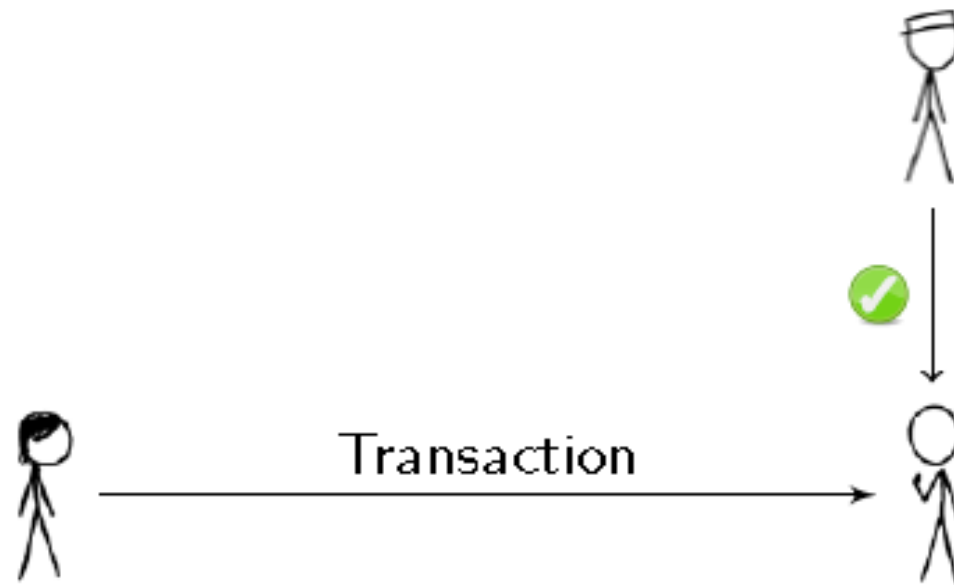
Mining is a competition to find a solution



Mining is a competition to find a solution

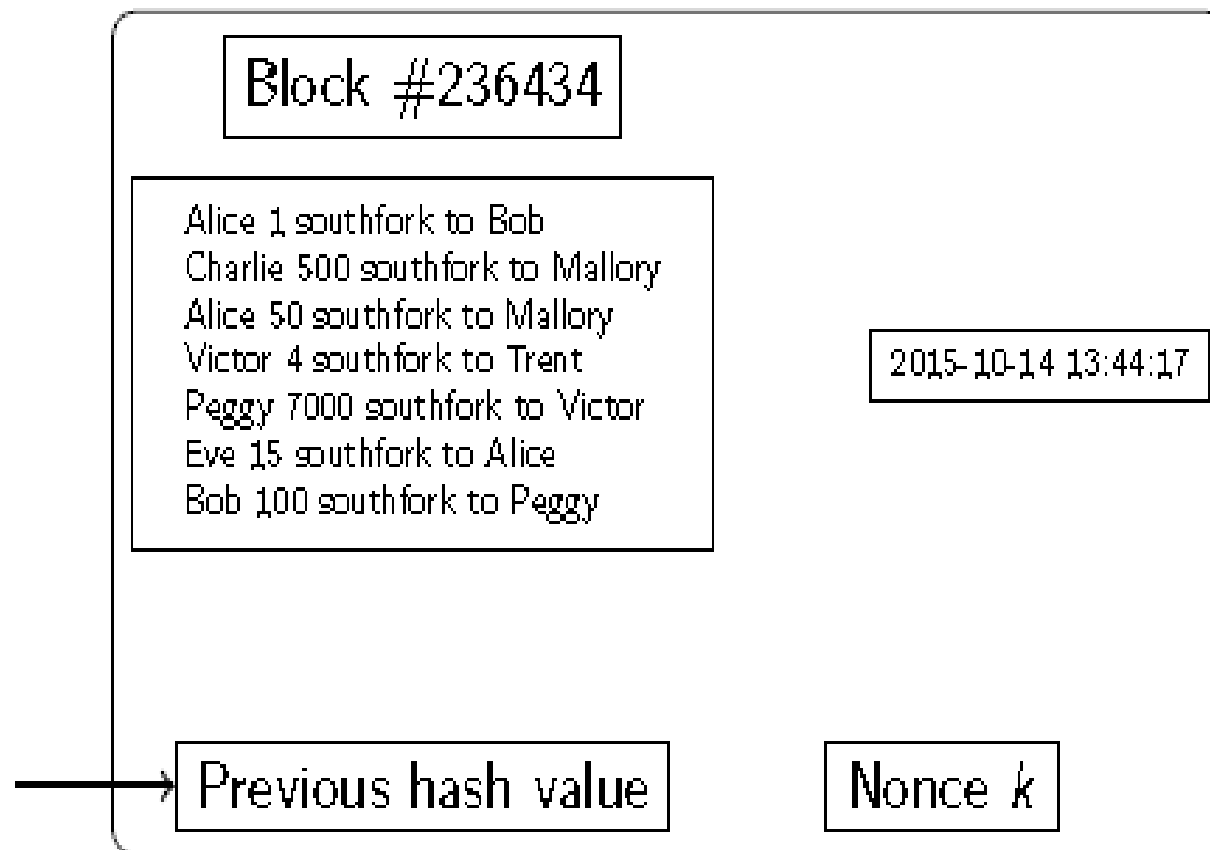


Mining is a competition to find a solution



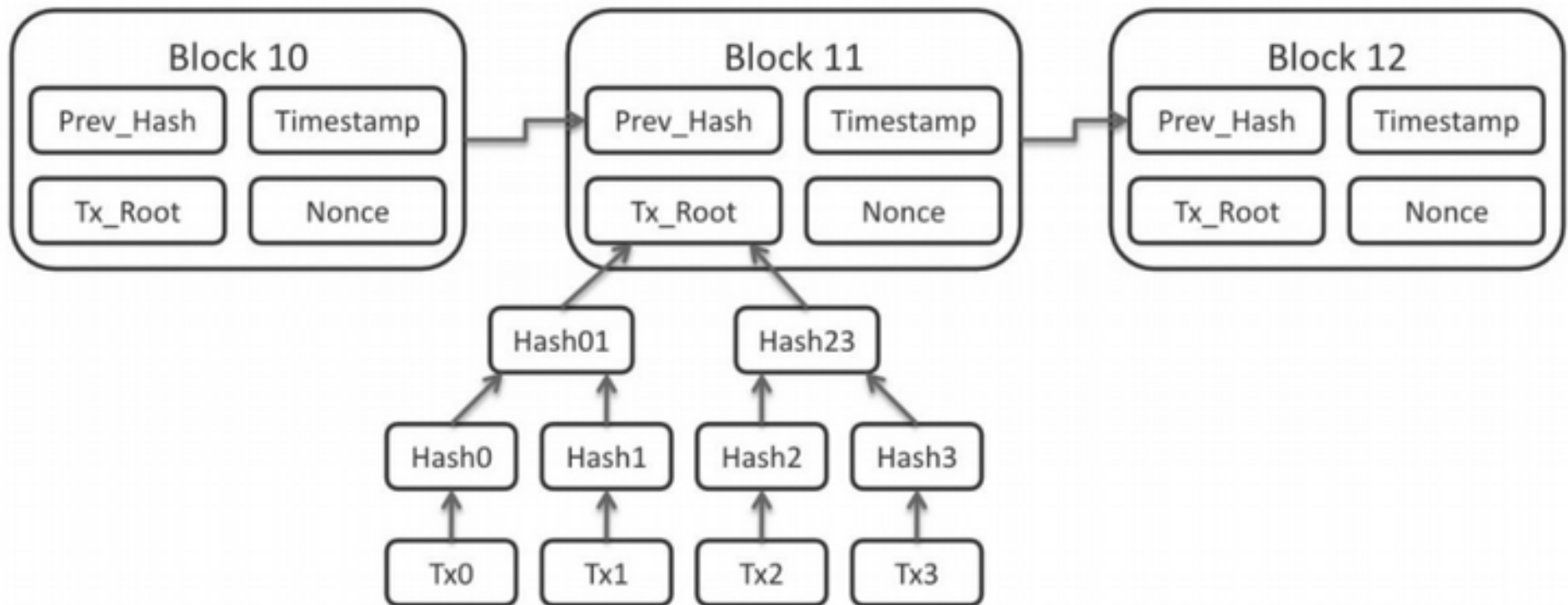
Chamath can trust the acknowledgment from Charlie.

A block is a large number of transactions



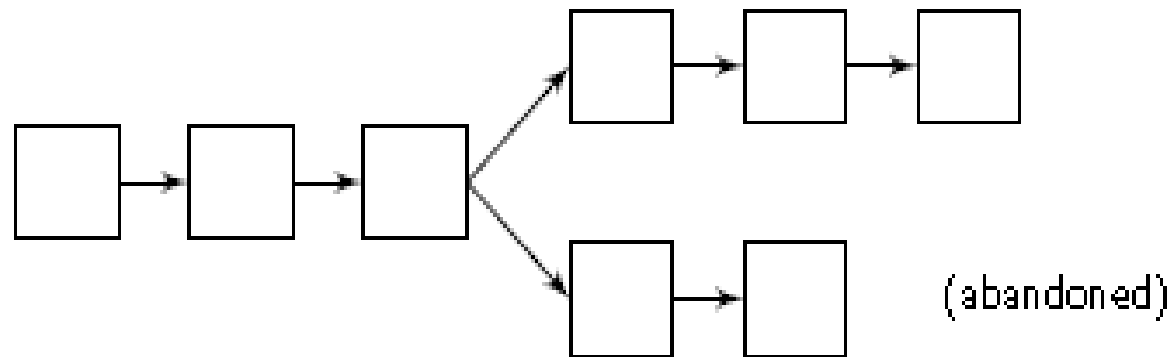
A block is only valid if its hash value is less than T .

Merkle Hash



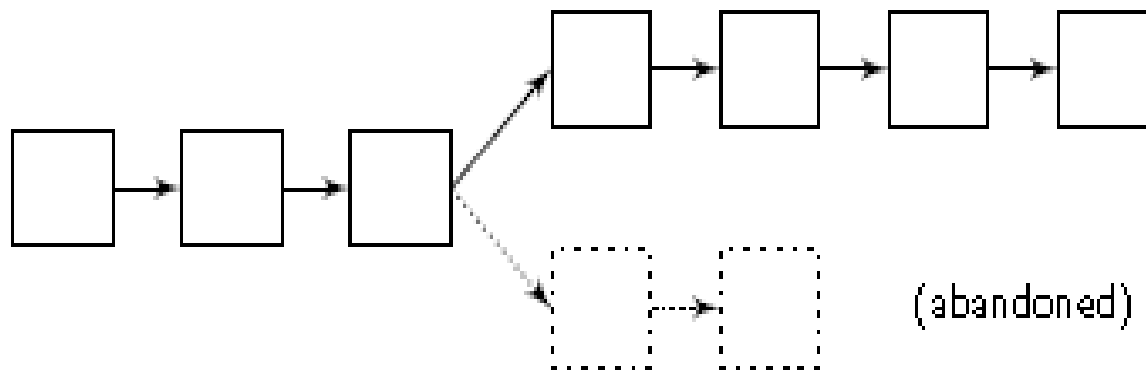
Transactions are verified by miners

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

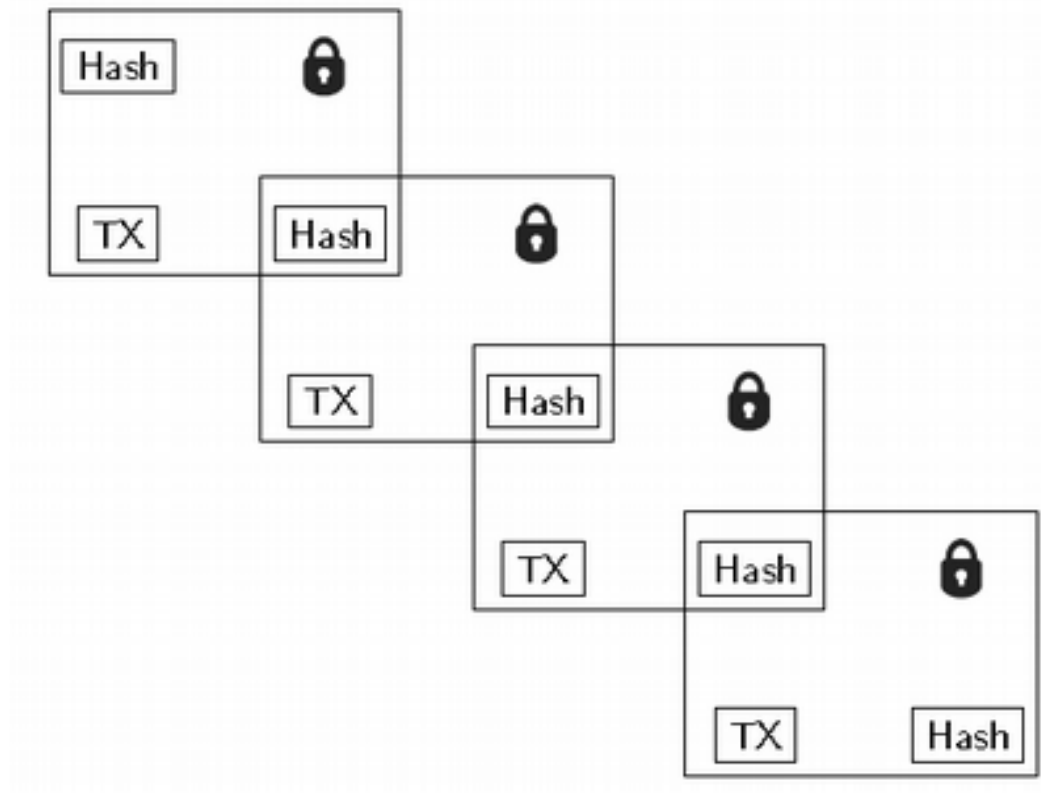


Transactions are verified by miners

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



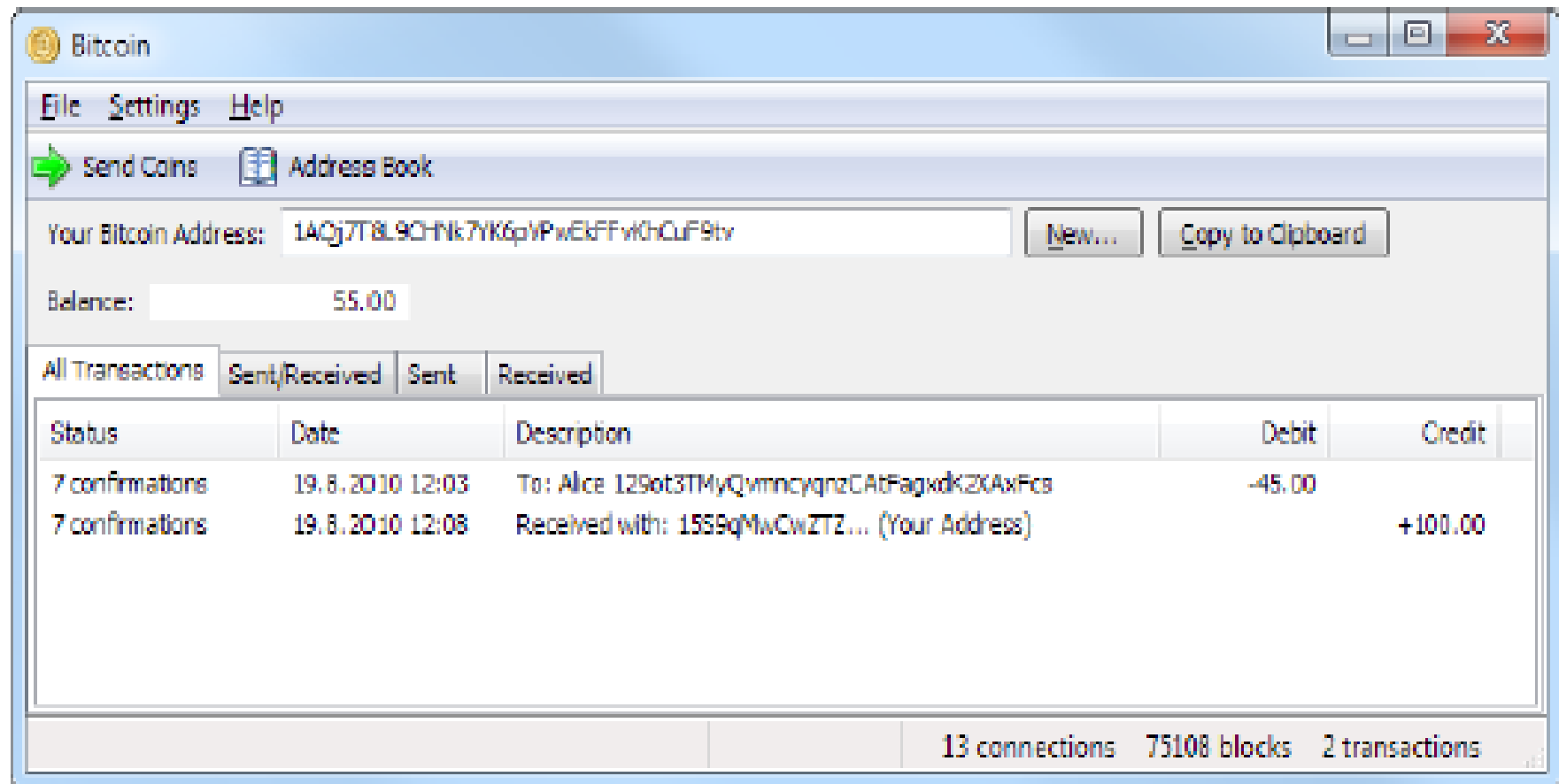
Each block gives security to the previous ones



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

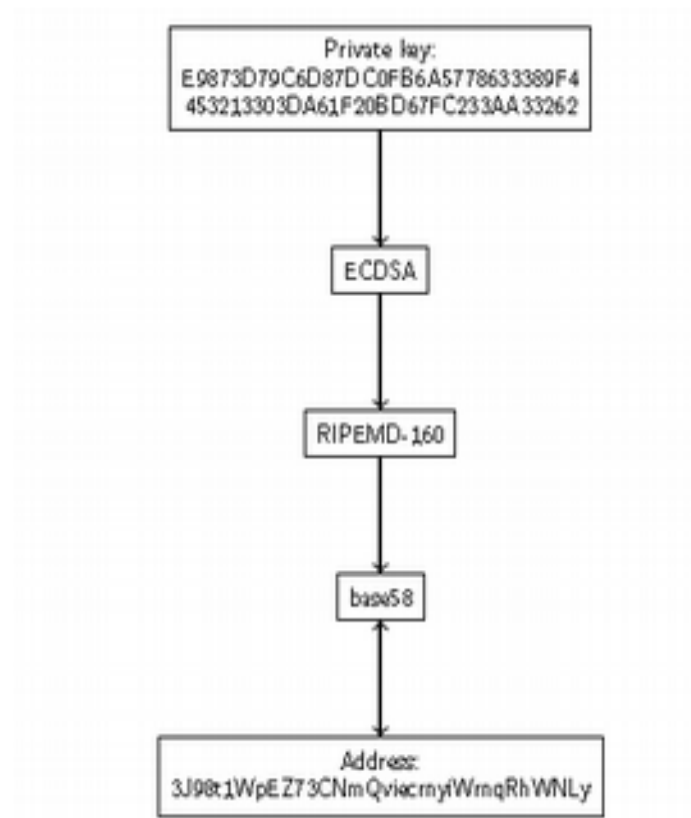
Sending and receiving bitcoin



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	\$ <input type="text"/>
<i>Give coin 3 to Chamath</i>	
_____ DOLLARS  Security Features Included. Details on Back.	
MEMO _____	
<i>kasun</i>	
⑈0000000000⑈ ⑈0000000000⑈ 1025	

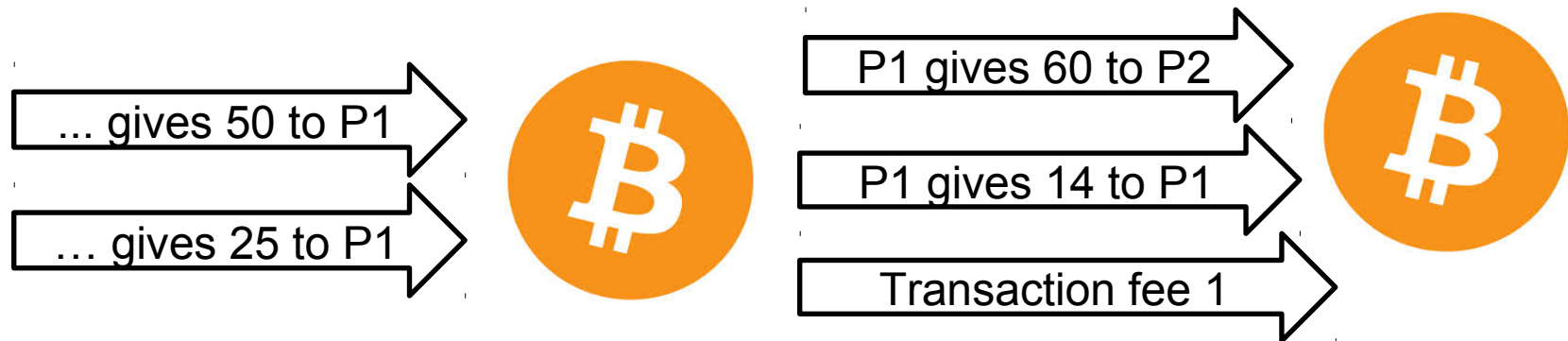
TRANSACTIONS

- 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.

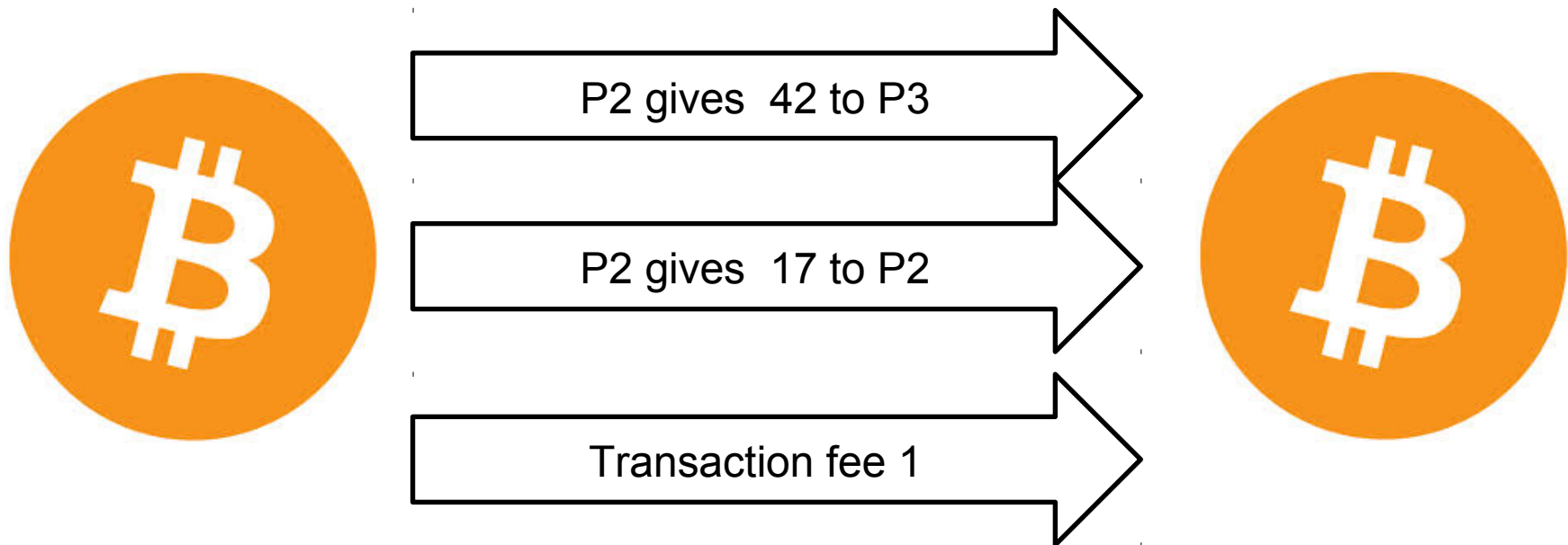
How is money transferred in Bitcoin?

Example: P1 wants to give 60 to P2



How is money transferred in Bitcoin?

Example: P2 wants to give 42 to P3

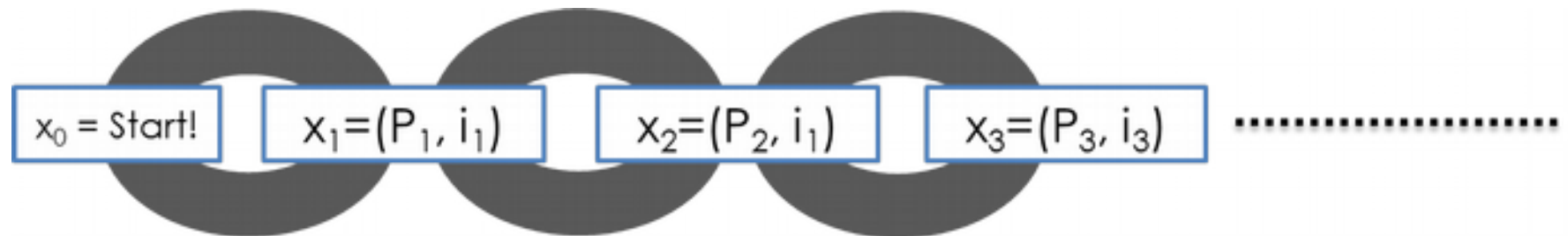


How to store money



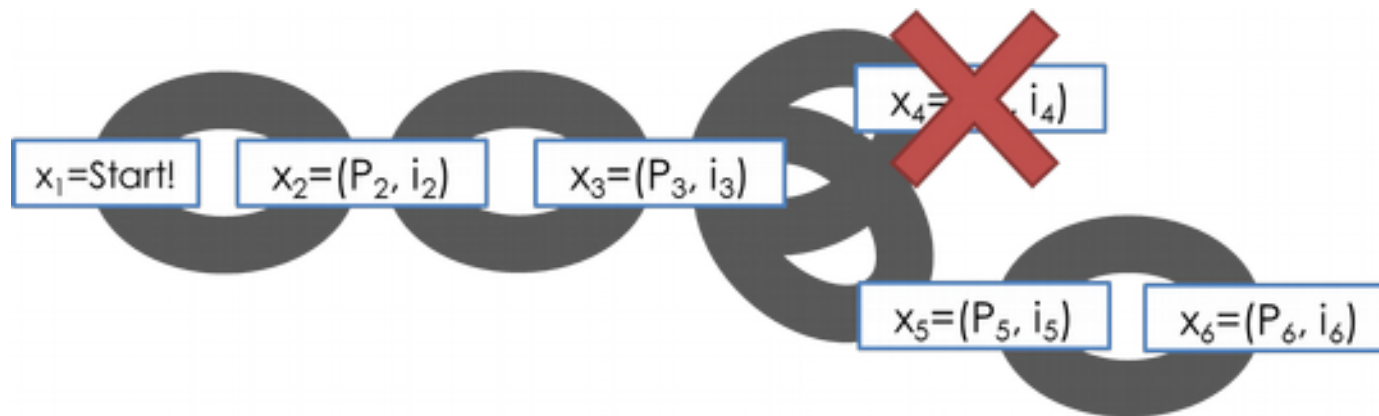
Main Idea:

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



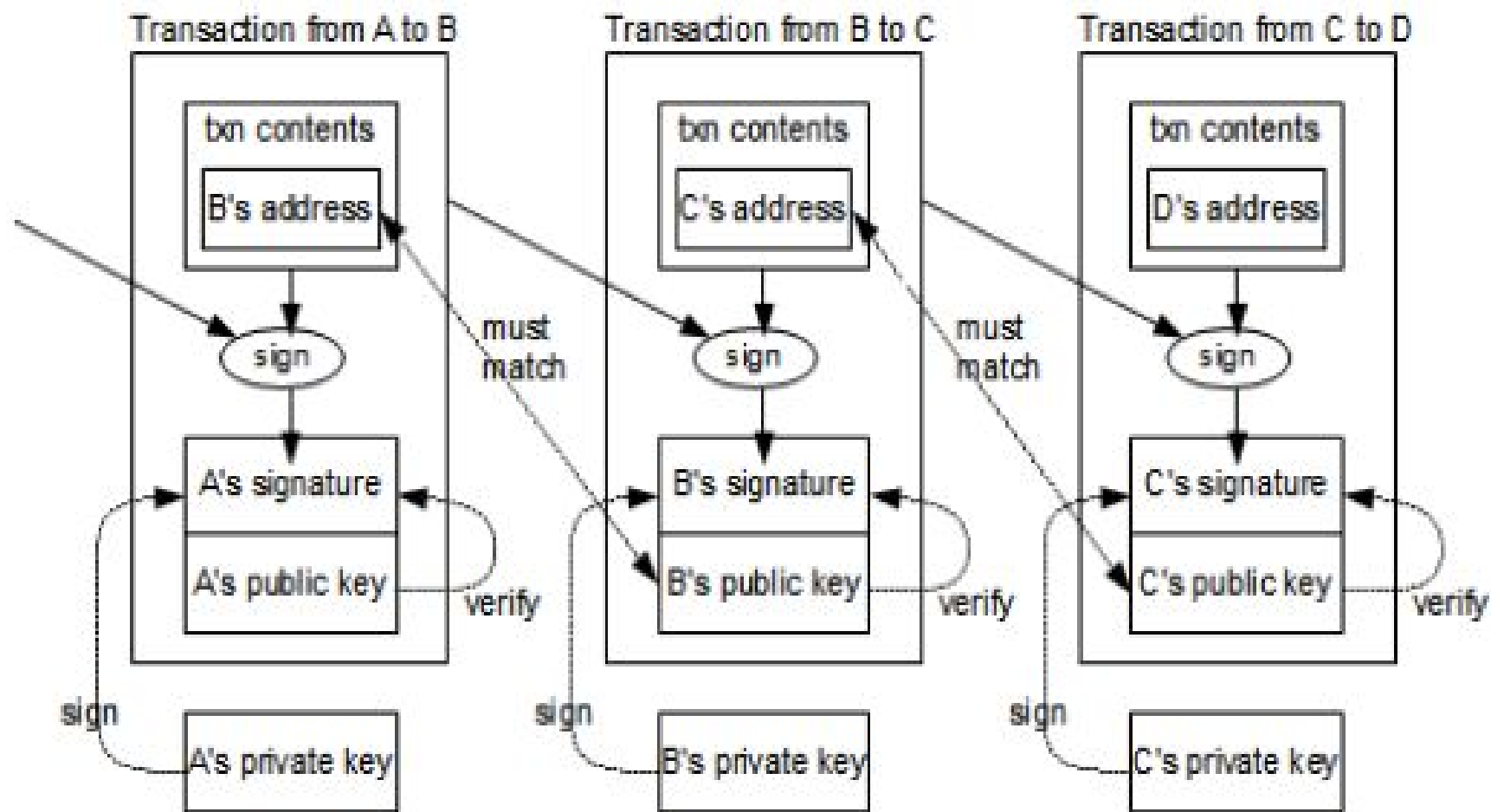
How is money stored in Bitcoin?

- 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)

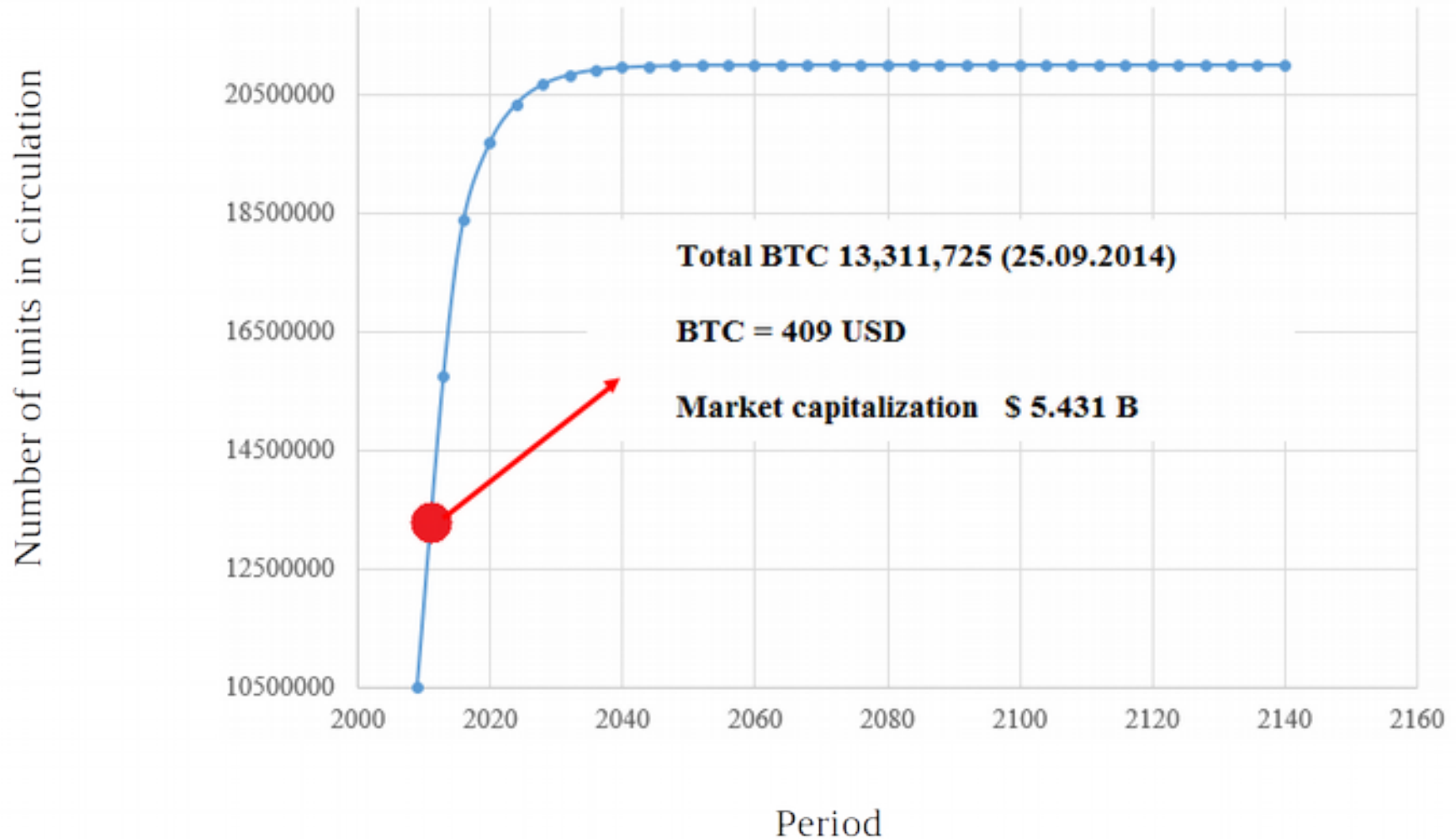
Detailed view of a transaction



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.

Total bitcoin unit supply over time (Projection)

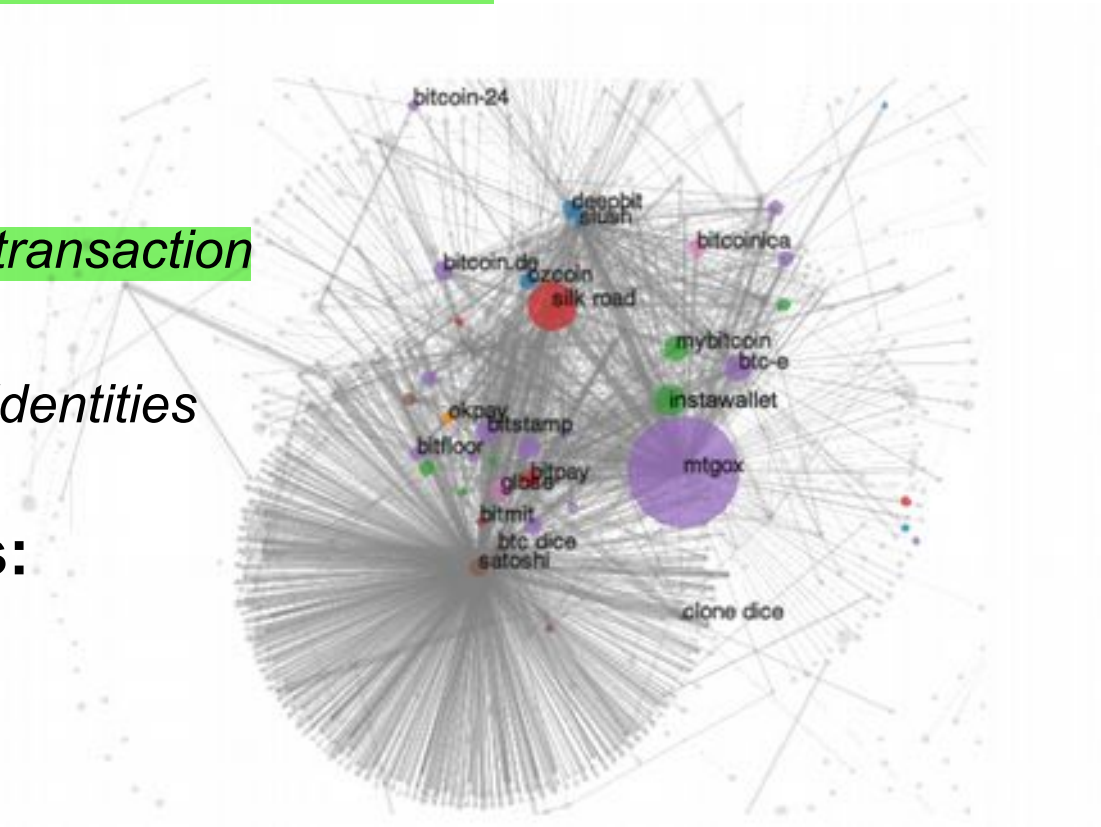


Security Analysis

- The only way for Kasun to cheat is the following:
 1. Buy a supercomputer
 2. Save up money for the electric bill
 3. Broadcast an invalid transaction m to Chamath
 4. Let the supercomputer search for a block containing m .
 5. The computer must be faster than everybody else's, combined.
 6. Even if she manages to solve an “illegal” block, no other miner will accept it.

Anonymity?

- **Problem:**
 - *Every transaction ever made is **recorded forever***
- **Solution?**
 - *Use **new identity** for each transaction*
- **But:**
 - *Heuristics allow to **cluster** identities*
- **Anonymous alternatives:**
 - *Zerocoin, Zerocash...*



Bitcoin mining is big business

Whenever a miner finds a valid block, he or she is rewarded.



Industrial-scale mining. Photo from KnC Miner

Bitcoin mining is big business



The Swedish miner KnC Neptune costs thousands of dollars and performs 3×10^6 hashes per second. Today, that gives roughly 160 USD per month (expenses not included).







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

coinmarketcap.com

1	 Bitcoin	\$113,244,946,217	\$6,549.77	\$4,514,066,930	17,289,900 BTC	2.32%		...
2	 Ethereum	\$22,531,824,888	\$220.46	\$1,829,973,838	102,202,939 ETH	4.77%		...
3	 XRP	\$21,415,644,800	\$0.537125	\$2,168,179,938	39,870,907,279 XRP *	18.85%		... %



CoinMarketCap

Rankings ▾

Trending ▾

Tools ▾

Services ▾

47	 Augur	\$143,749,968	\$13.07	\$3,601,671	11,000,000 REP *	3.21%		...
48	 Golem	\$134,070,648	\$0.139767	\$2,180,133	959,242,000 GNT *	2.24%		...
49	 Holo	\$132,654,886	\$0.000896	\$4,198,854	133,214,575,156 HOT *	1.26%		...

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?

More reading if you are interested

- The Bitcoin whitepaper: Read it!
<https://bitcoin.org/bitcoin.pdf>
- More detailed explanation of transaction and keys:
<http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html>
- CRYPTOCURRENCY - සයිබර් කාසි
<http://kasun.scorelab.org/2018/04/cryptocurrency.html>

A final word...

**Distributed currencies:
for the **good guys** or the **bad guys**?**

- *Crime is bad! Tax evasion is bad!*
- *But sometimes governments are bad too!*

Discussion

