Høgskolen på Vestlandet

DAT159
Module3 – Blockchain technology

L14 - Introduction to Blockchain and Bitcoin

Lars-Petter Helland, 08.10.2018

Module content

From the course description:

- Construction and structure of blockchains
- Distributed trust and consensus
- Proof of Work
- Block content and transactions
- Examples of blockchains (e.g. Bitcoin and Ethereum)
- Smart contracts
- Ecosystems and infrastructure
- Application areas.

Plan for the module

- L14 - Introduction to Blockchain and Bitcoin
- L15 - Consensus, PoW, Whitepaper, ...
- Lab1 - Writing a simple blockchain in Java

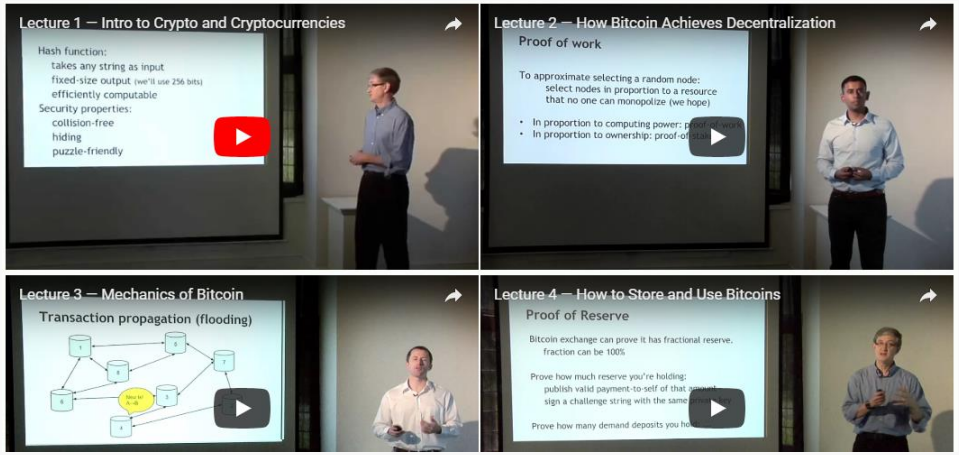
- L16 - A closer look at Bitcoin 1 (blocks, hashes, inputs/outputs, ...)
- L17 - A closer look at Bitcoin 2 (+ coding a little bit)
- Lab2 - Writing a bitcoin-like blockchain in Java

- L18 - Applications, altcoins and ecosystem
- L19 - Smart contracts?
- Lab3 - ??? Oblig3 ???

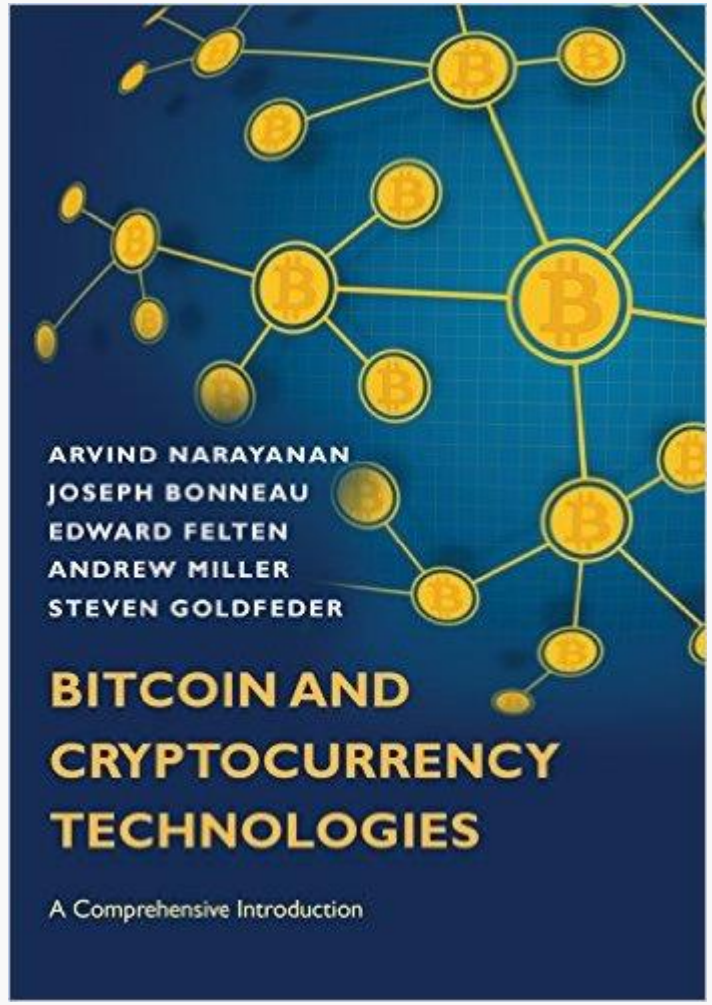
Learning resources, I

http://bitcoinbook.cs.princeton.edu/

with accompanying (YouTube) video lectures

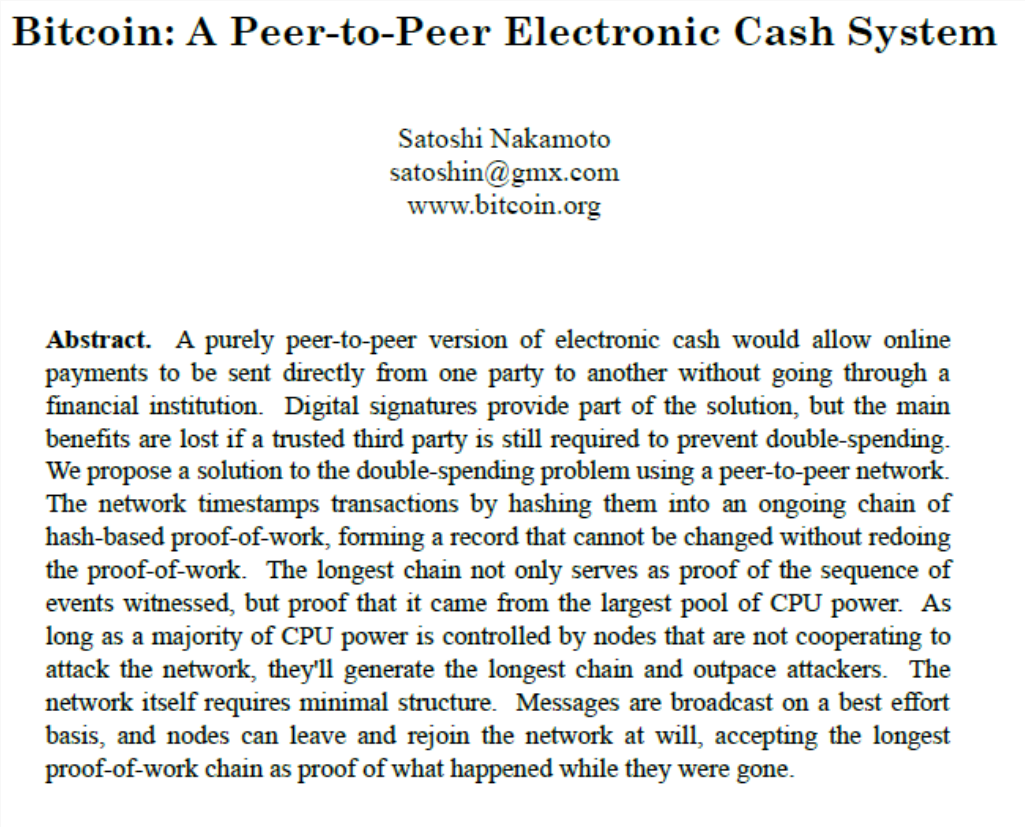


Free draft copy of book @ https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf



Learning resources, II

The Bicoin whitepaper by Satoshi Nakamoto can be found @ https://bitcoin.org/bitcoin.pdf



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

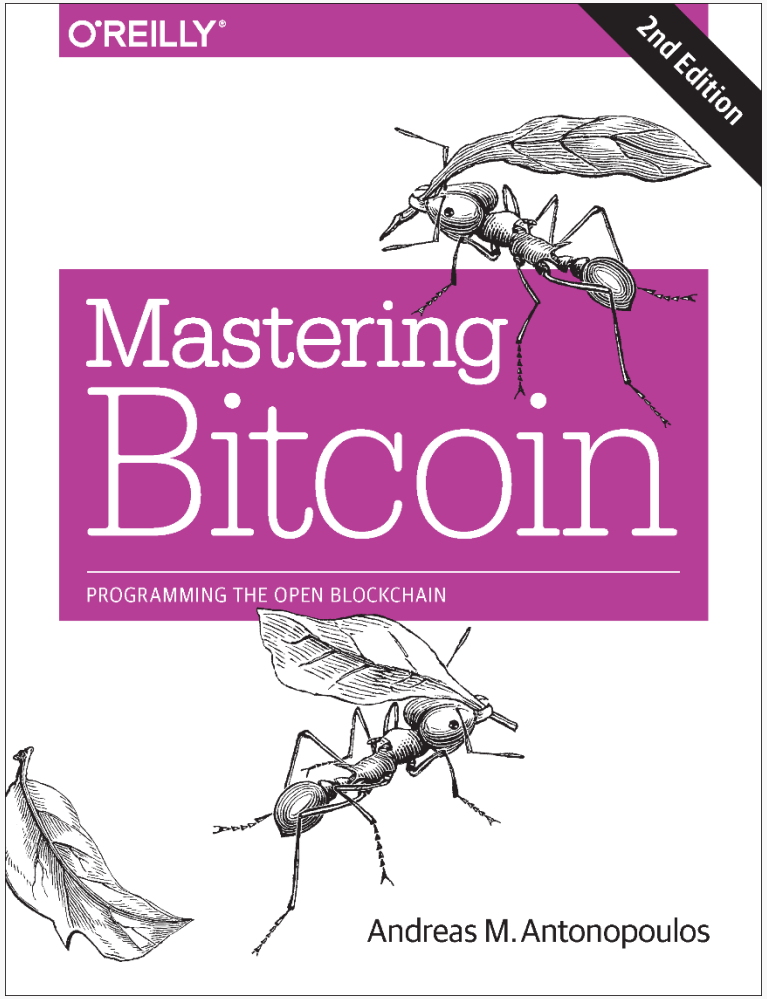
Learning resources, III (cursory)

https://github.com/bitcoinbook/bitcoinbook

Free draft copy of book @

https://github.com/bitcoinbook/bitcoinbook/releases/tag/second_edition_print2

Use Chrome-extension "Asciidoctor.js Live Preview“ (or similar) to read properly formatted text.



Learning resources, IV

To be determined …

I will try to find articles, videos and code examples to support the learning outcomes.

You are also encouraged to suggest topics and resources.

Today

- We will examine many of the key concepts, illustrated by a live demo using the Bitcoin network to transfer bitcoin from one address to another.
- We will look at the core structure of a blockchain
- We will look briefly at the Bitcoin white paper

- Reading material:
  - **[NA Ch1]** - Introduction to Cryptography and Cryptocurrencies
  - **[SN]** - Bitcoin: A Peer-to-Peer Electronic Cash System


Introduction
To Bitcoin

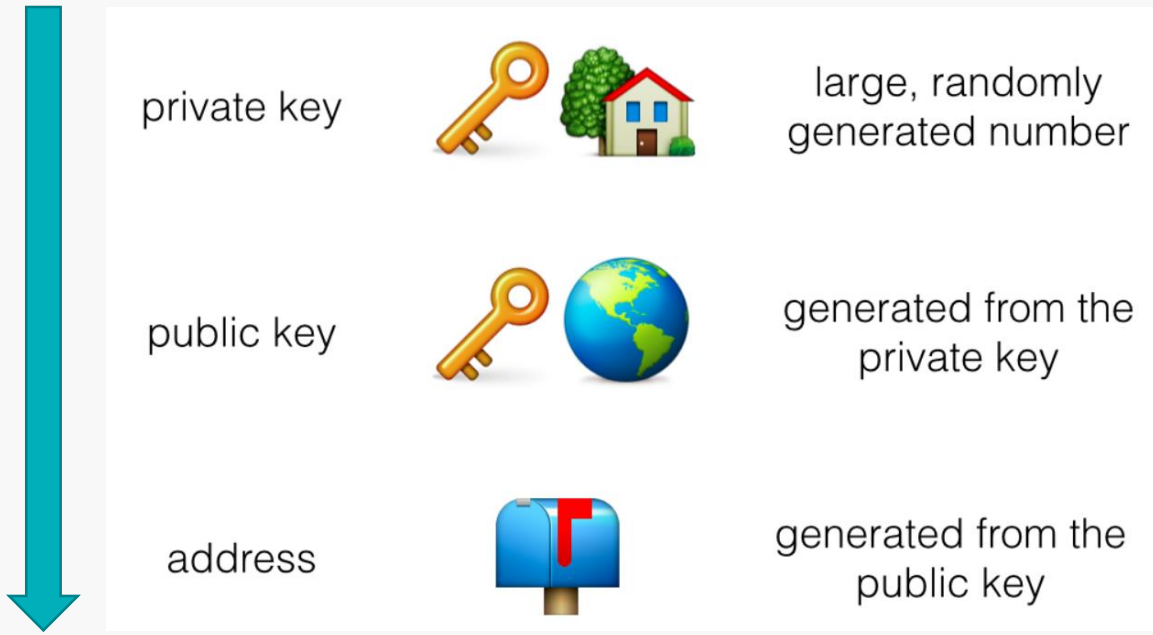
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of

Keys, addresses and signatures

- A bitcoin amount is always associated with **a bitcoin address**. Think of the address as an **account number**. The address is a hash of a **public key**.
- When we transfer (spend) bitcoin, it "moves" from one address to another.
- To spend bitcoin, you have to provide the private key for the sender address to prove that you "own" this address. Think of the **private key** as a **password**.
- A key-pair is created, **from a random number**, according to the Elliptic Curve Digital Signature Algorithm (ECDSA).



Key creation

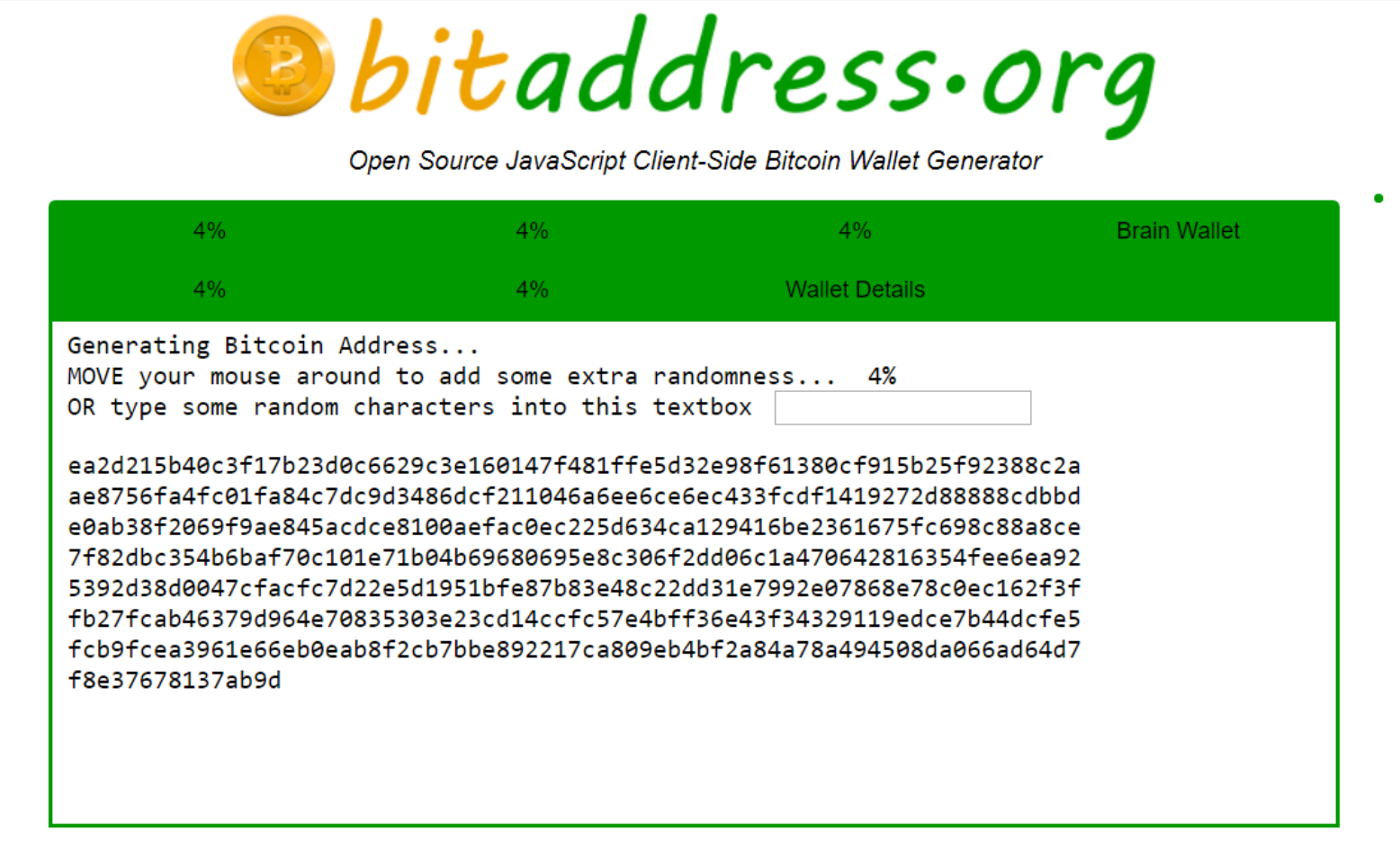
- In Bitcoin, a private key is a 256-bit number
- Nearly every 256-bit number is a valid ECDSA private key
- => The number of keys is $2^{256} \sim 10^{77}$ ~ number of atoms in the universe

- So if you create a truly random private key, there is **~ zero chance that someone else can guess or create the same key**. Even with much computing power, it is really hard to brute force a guess of your key. (In practice, there are more private keys than addresses (2^{160}), but still ...)

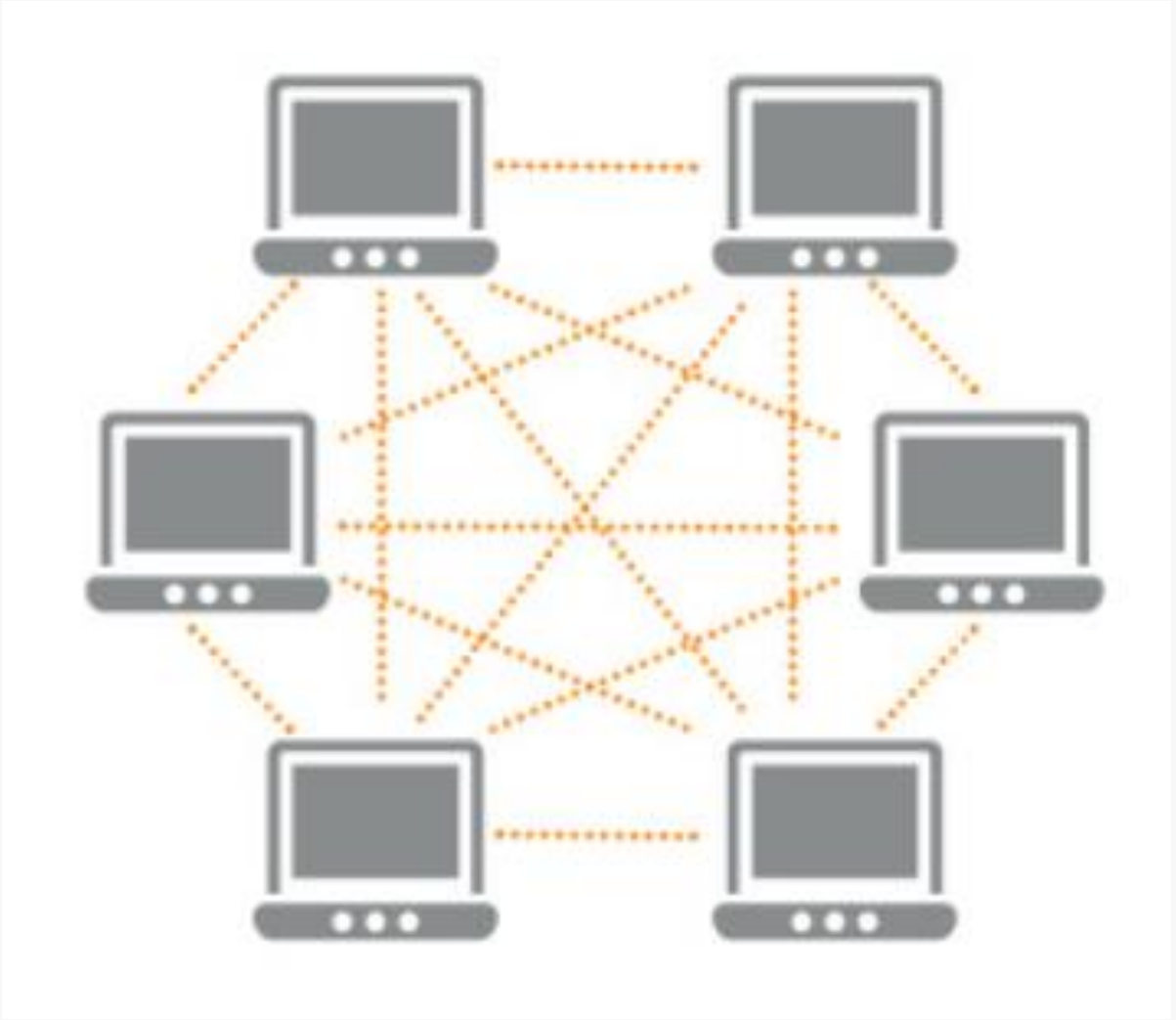
- See: https://lbc.cryptoguru.org/about and https://lbc.cryptoguru.org/man/theory

```
1AAAAAAAAAAAAAAAAAAAAAAAAAAAGZJFqF (4200000000), Time elapsed: 13 seconds
```

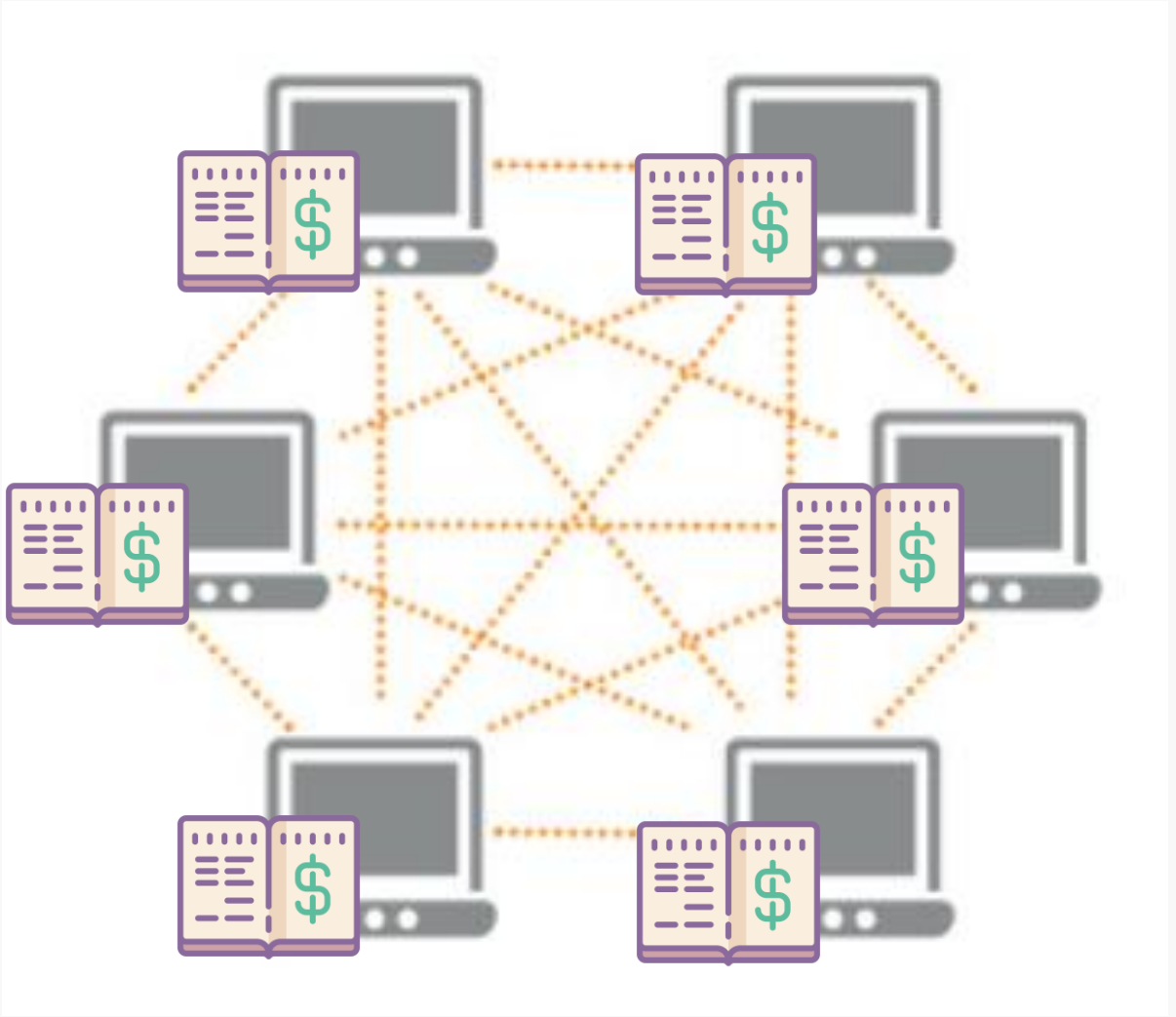
Let's illustrate the process by creating a "wallet"



The Bitcoin network



The Bitcoin network - A distributed ledger



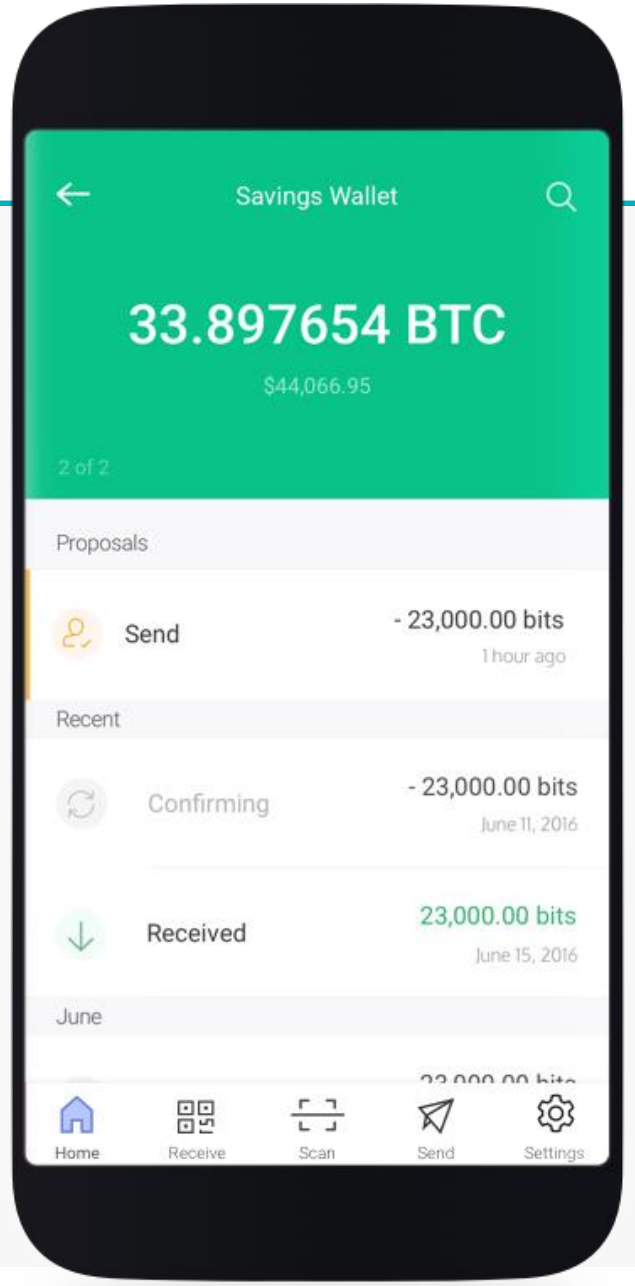
The Bitcoin network - ... with a Block Explorer

Block Explorers

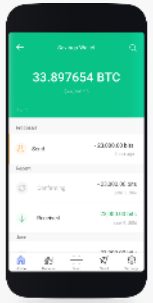
- The data in the Bitcoin blockchain is publicly available
- But the format is not human understandable
- There are a lot of applications that shows / visualizes / gives read-access to the data in the blockchain
- These are called block explorers
- One example is https://live.blockcypher.com/

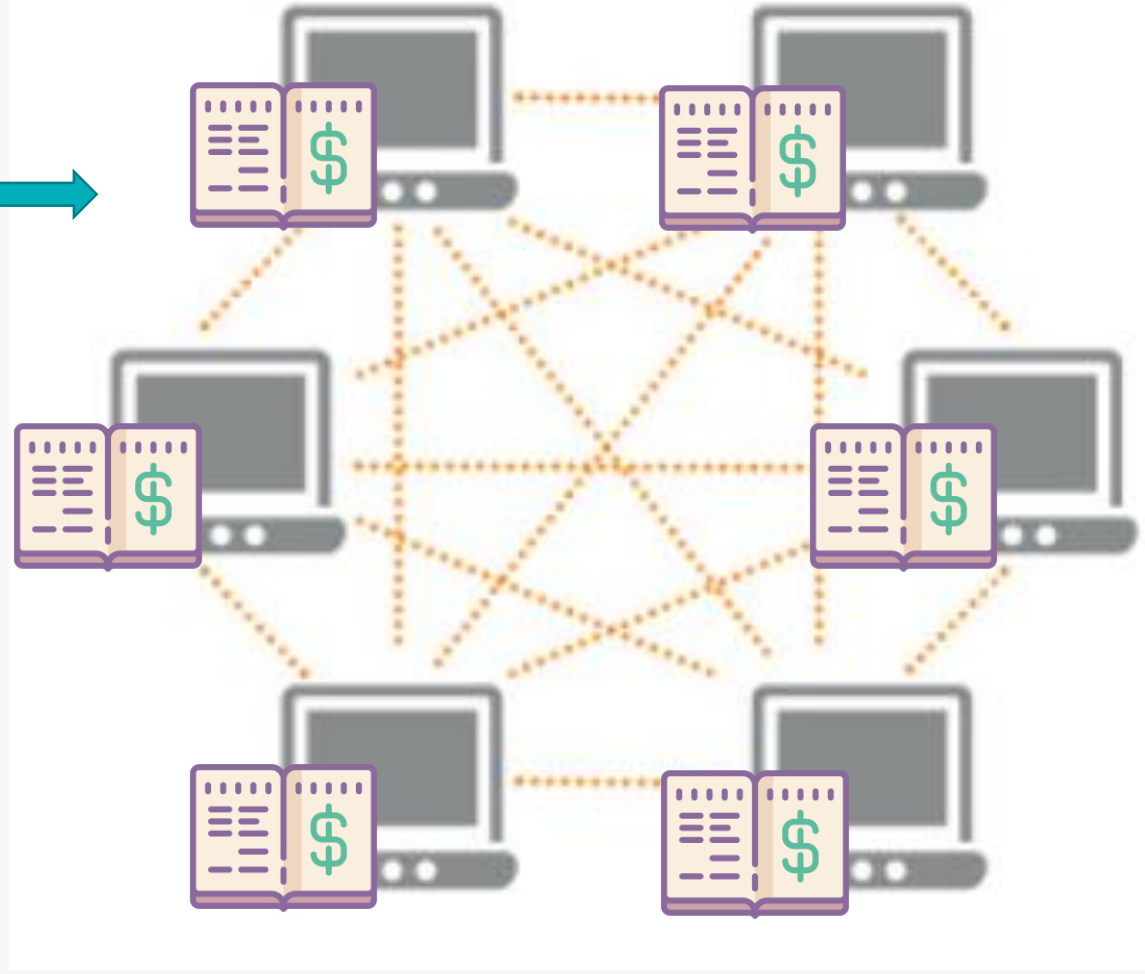
Bitcoin Wallet software

- We have created a key-pair, but in order to send bitcoin we need software to create, sign and send a transaction.
- One example of such software is a Mobile Wallet.
- Wallet software handle your key(s), shows your balance, and enables you to send bitcoin.

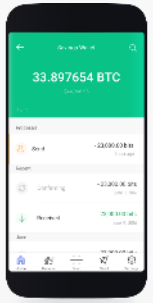


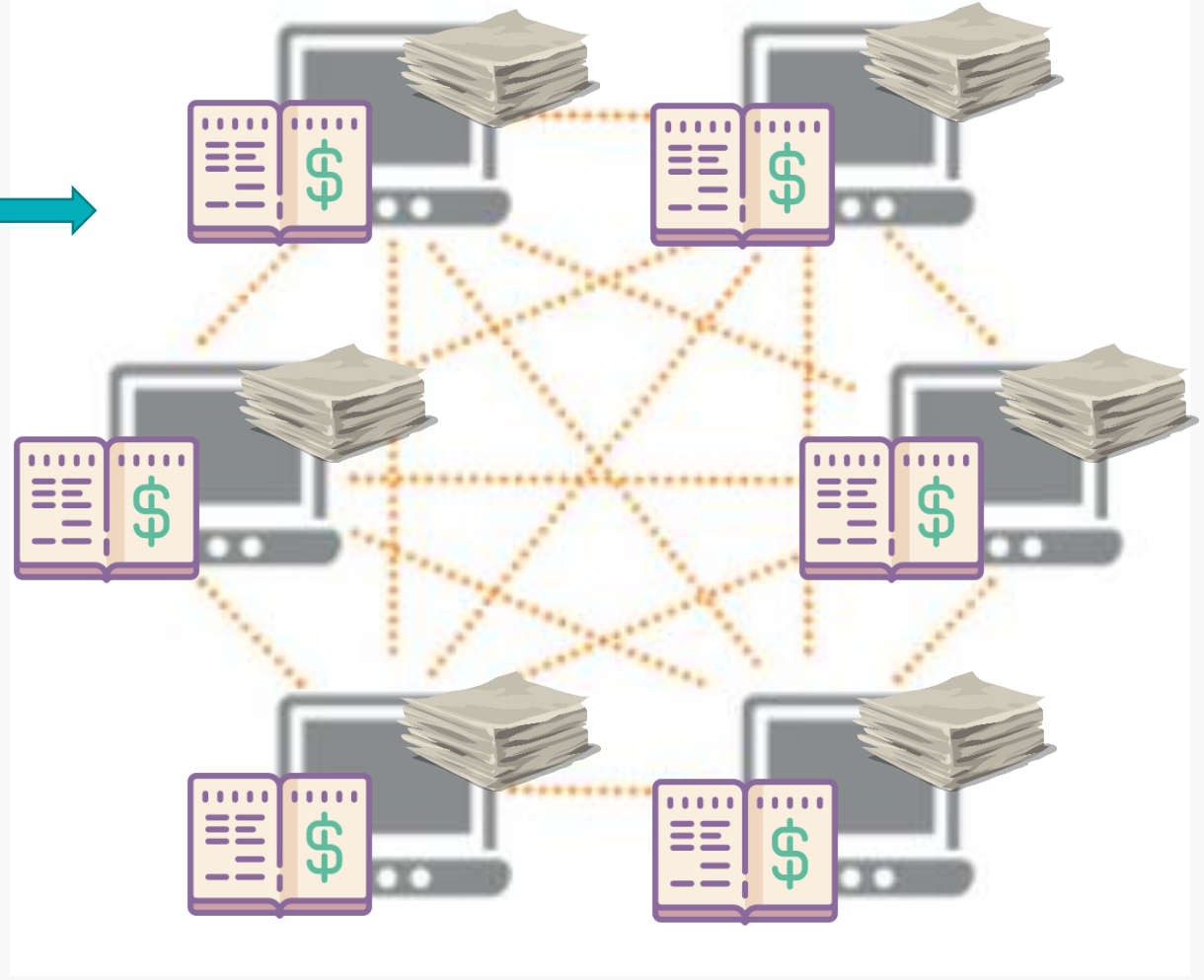
The Bitcoin network - ... using a mobile wallet



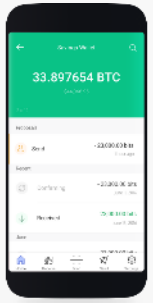


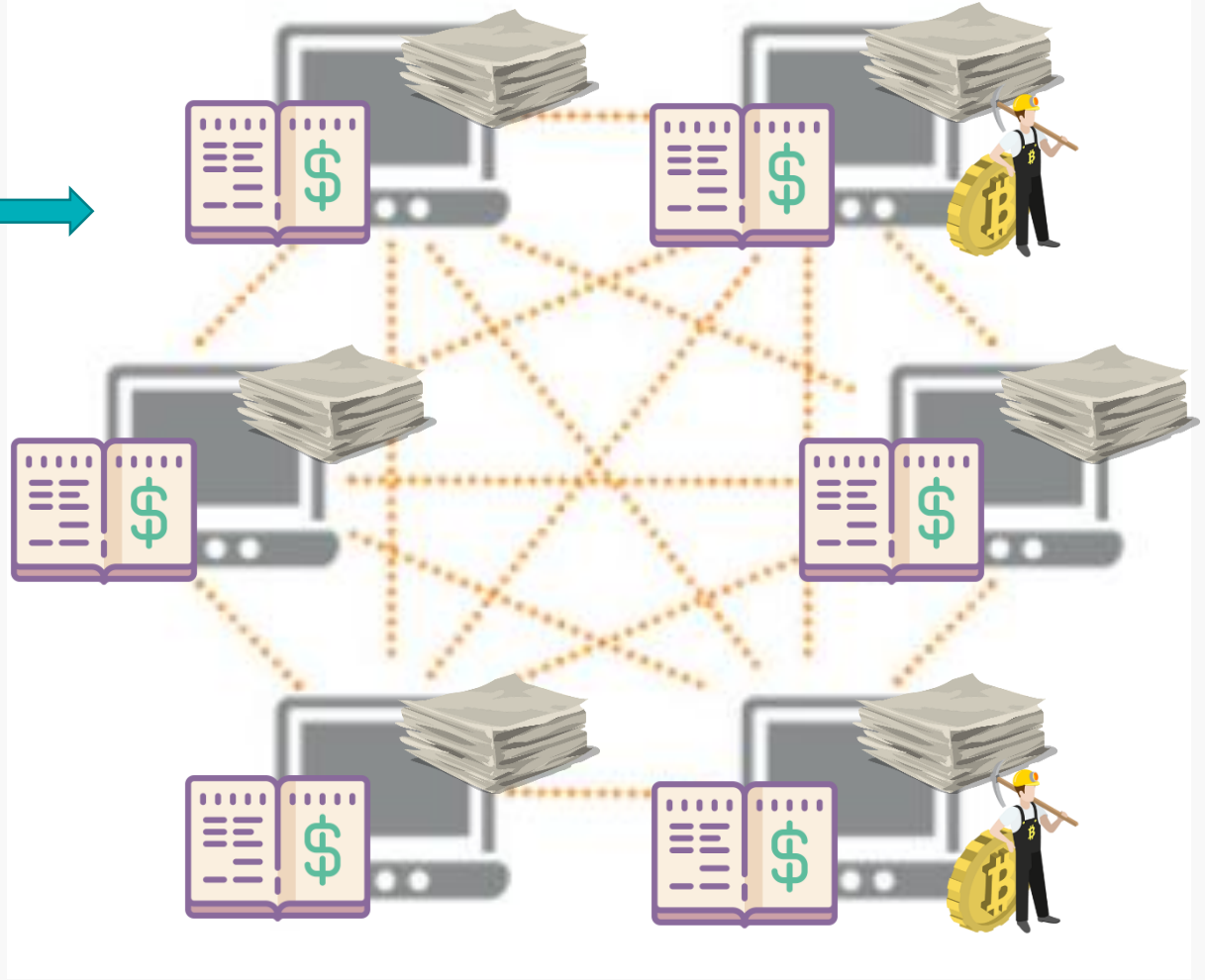
The Bitcoin network - ... with piles of pending transactions



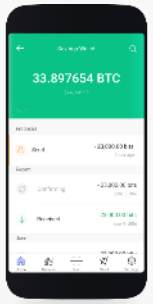


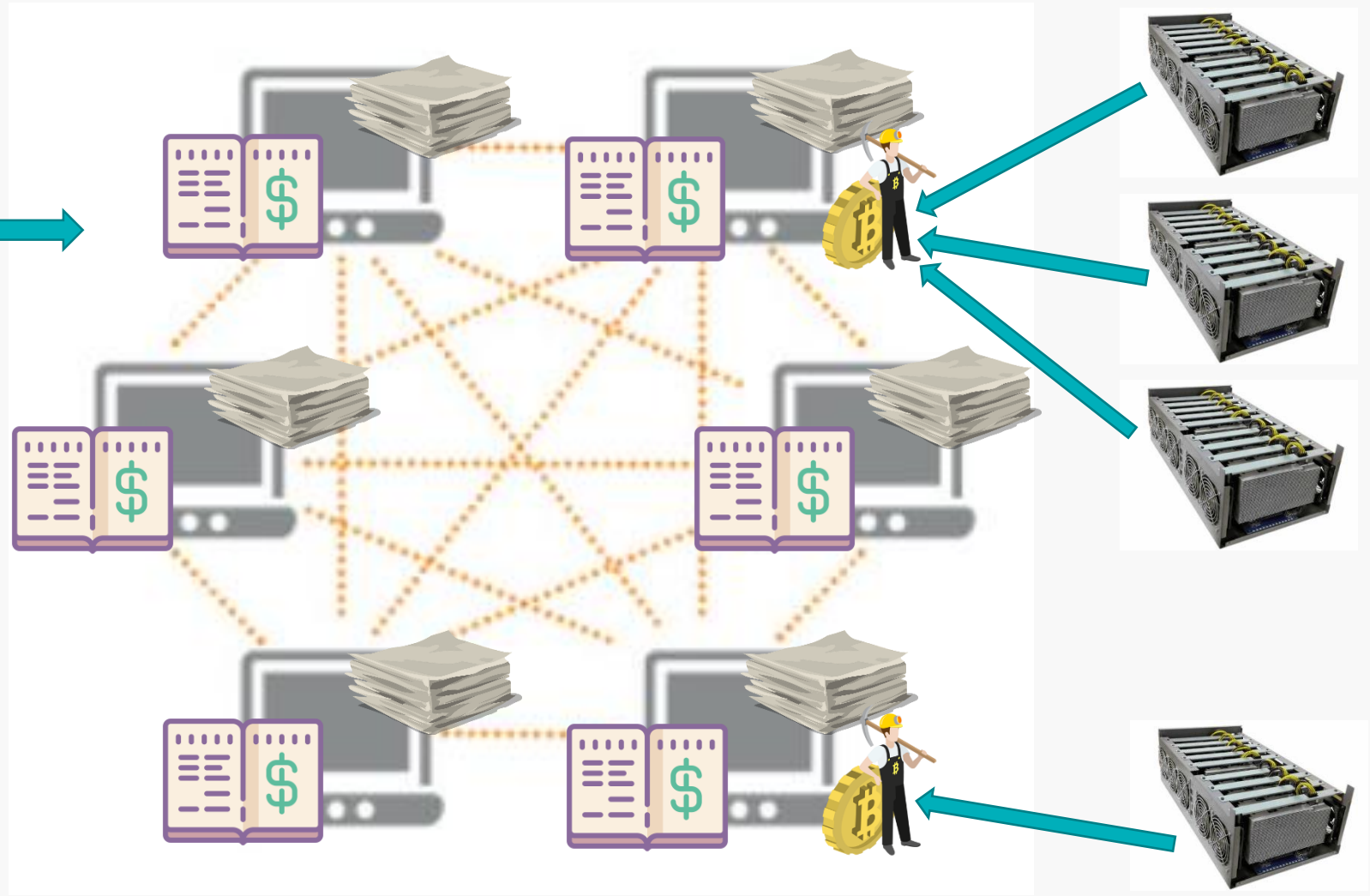
The Bitcoin network - ... with miner nodes





The Bitcoin network - ... some operate mining pools



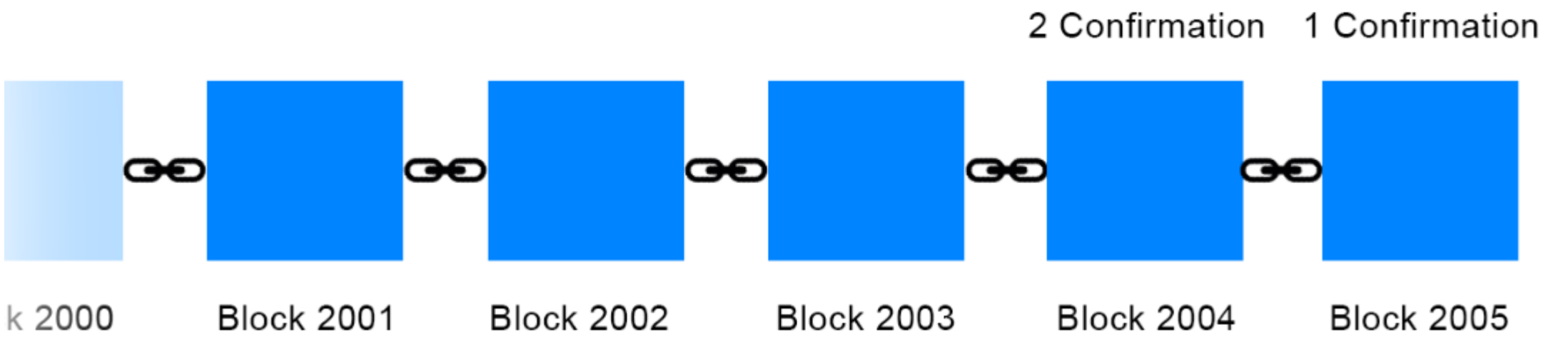


Mining

- The main purpose of mining is **not** to create new bitcoin
- The main purpose of mining **is to secure the blockchain** by creating a "signed" tamper-resistant block that can be appended to the blockchain. The new bitcoin that is created is a reward for the effort.
- A miner chooses a number of transactions, creates a candidate block, and tries to solve the "mining puzzle" to create a valid block.
- If/when the miner finds a solution, the new block is broadcasted to the rest of the network for validation.
- A new block is in this way appended to the blockchain in average every 10 minutes.

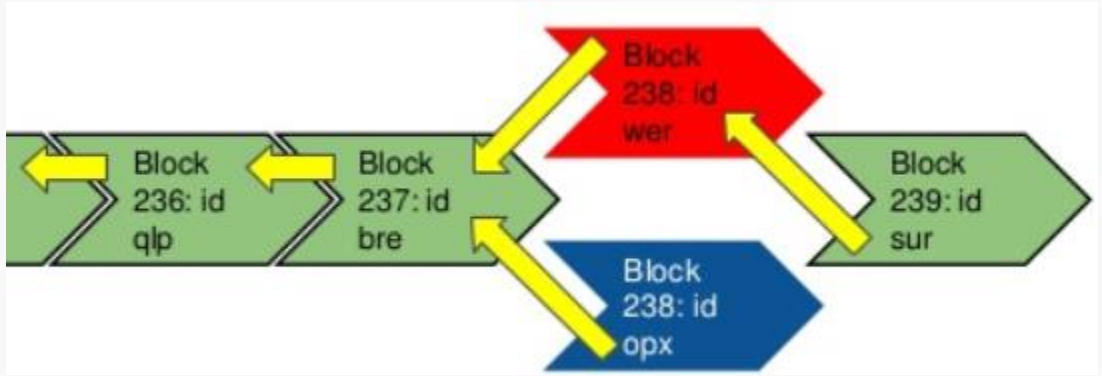
How is our transaction doing?

- When a block explorer shows 1 confirmation, that means that the transaction is contained in the last block appended to the blockchain.
- (In most cases,) this means that the transaction is confirmed.



Why did I say "(In most cases,) this means ..."

- Can the transaction be "unconfirmed" once it is confirmed?
- Remember that this is a distributed ledger. Different nodes can in a short period of time have different blocks at the end of the chain. Miners can possibly start to mine on a chain not containing your block.
- The rule is that the longest chain is the valid chain. Differences will soon settle, and one chain is the "winner".
- The more confirmations you have, the more "confirmed" your transaction is.
- It is very rare to be "unconfirmed" after 2 confirmations.

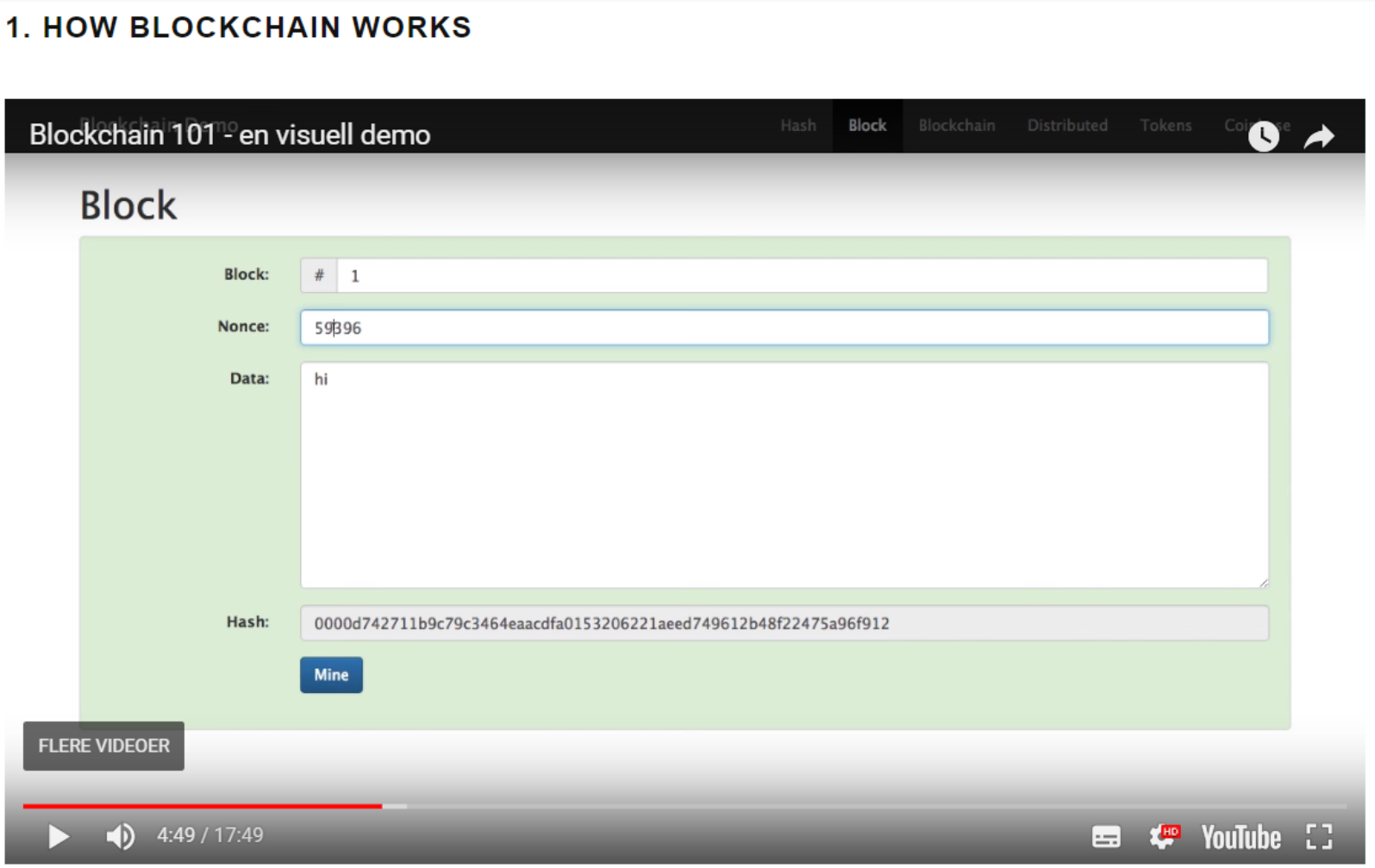



Pause

- Now: Blockchain

http://blockchain.mit.edu/how-blockchain-works

18 minutes

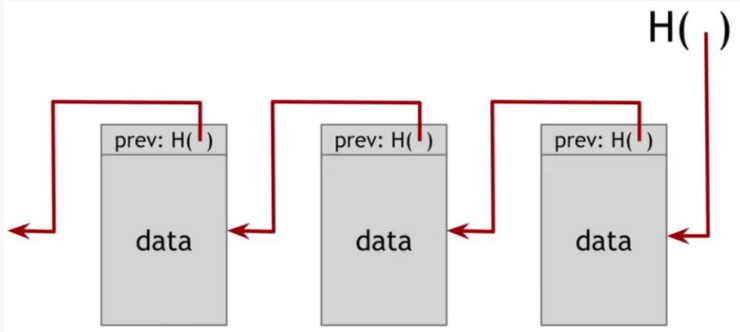


A few remarks to the video

- You may have recognized that **Prev** changed automatically in subsequent blocks when **Hash** changed in a block, which caused the subsequent blocks to be invalid. In practice, the blocks will be invalid because there is a mismatch between the **Hash** of a previous block and **Prev**.
- You may have recognized that he talked about democracy and voting between the nodes to settle what is the valid chain. In practice (in Bitcoin) there is no voting, but a rule that **the "longest" chain** is the valid chain.

Hash pointers

- In many presentations, a blockchain is depicted as a kind of linked list, with hash pointers pointing to previous blocks.
- In practice, a blockchain is stored in a database.
- Hash pointers can also be viewed as foreign keys.



- The point is that you can
  - Traverse the chain backwards
  - Verify that the chain is not broken by comparing the hash values

- Different implementations exist

Before we contiunue

The programming assignment for this week

- You are going to implement a simple blockchain similar to what you saw in the video.
- You will get a skeleton ...

[Look at it briefly]

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of

Bitcoin white paper - Abstract, I

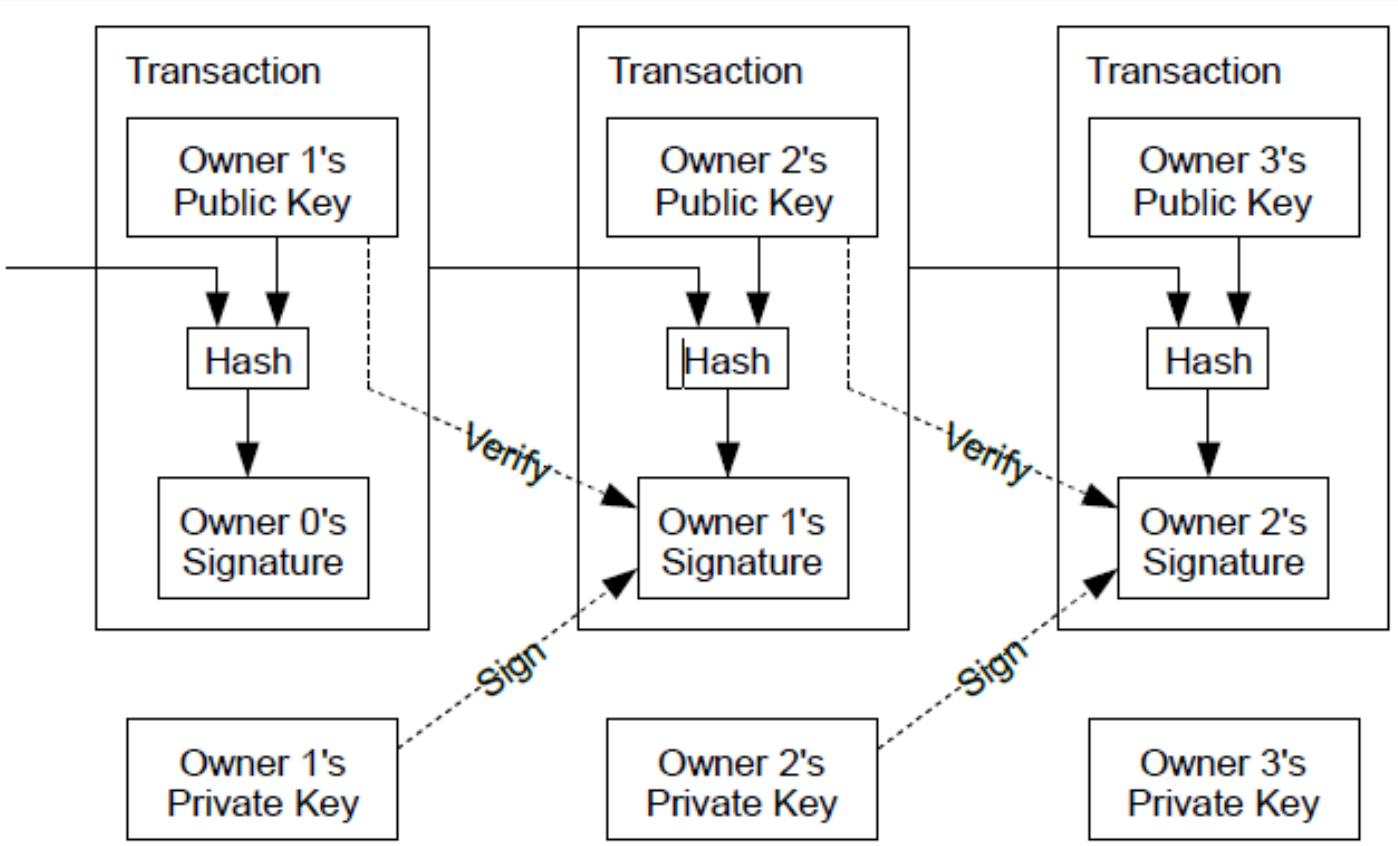
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work.

Bitcoin white paper - Abstract, II

Abstract. ... The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

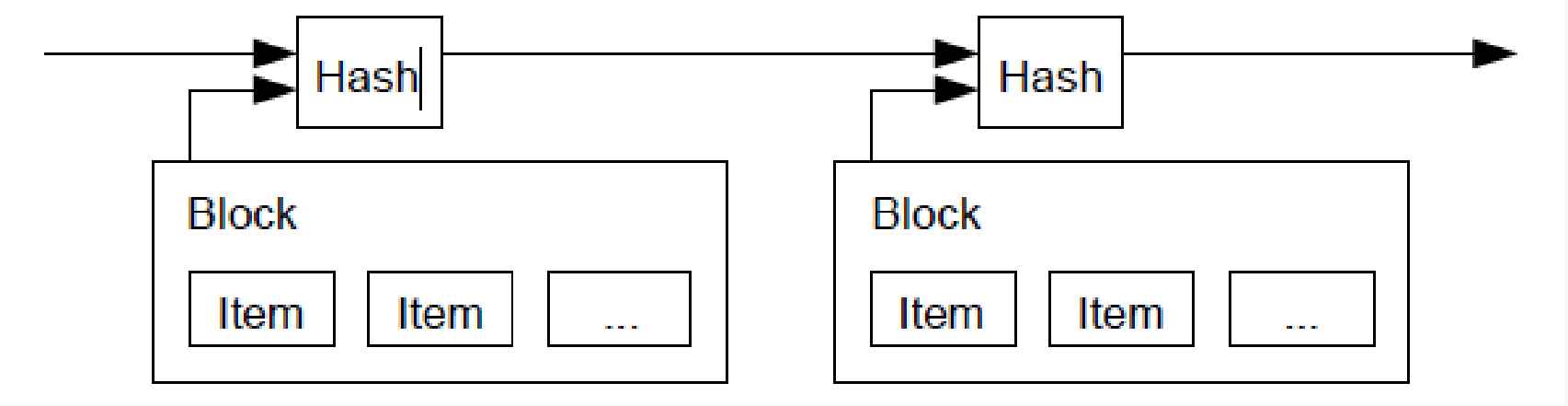
Bitcoin white paper - Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.



Bitcoin white paper - Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



Bitcoin white paper - Proof-of-Work

Tomorrow

Bitcoin white paper - Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it.

Bitcoin white paper - Incentive

Tomorrow

Bitcoin white paper - Reclaiming Disk Space

Next week

Bitcoin white paper - Simplified Payment Verification

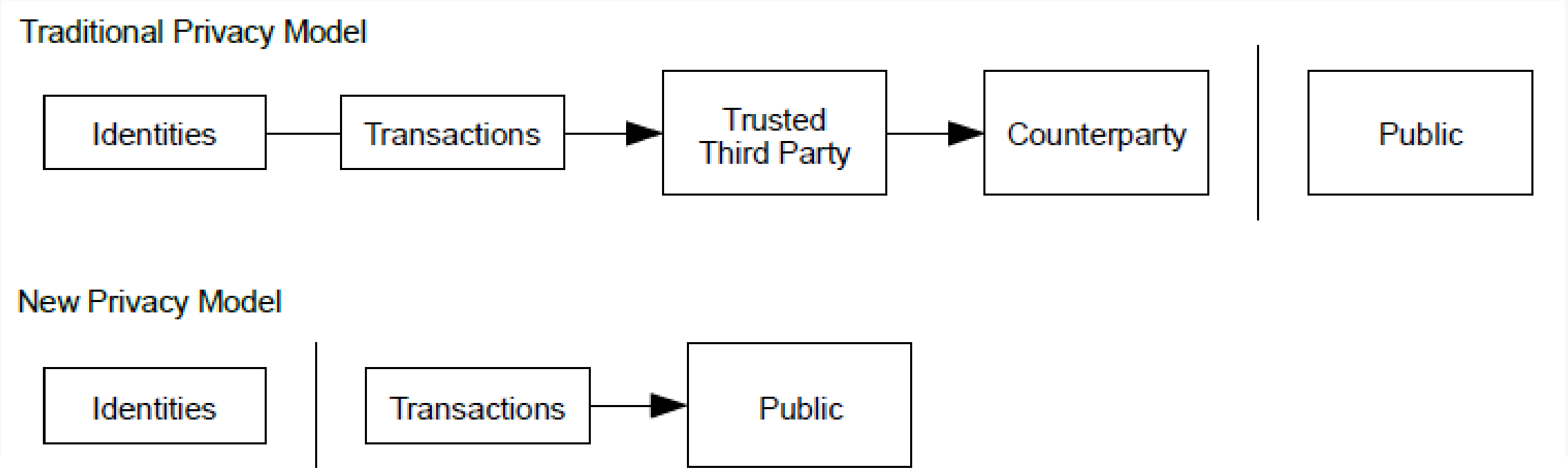
Next week

Bitcoin white paper - Combining and Splitting Value

Next week

Bitcoin white paper - Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous.

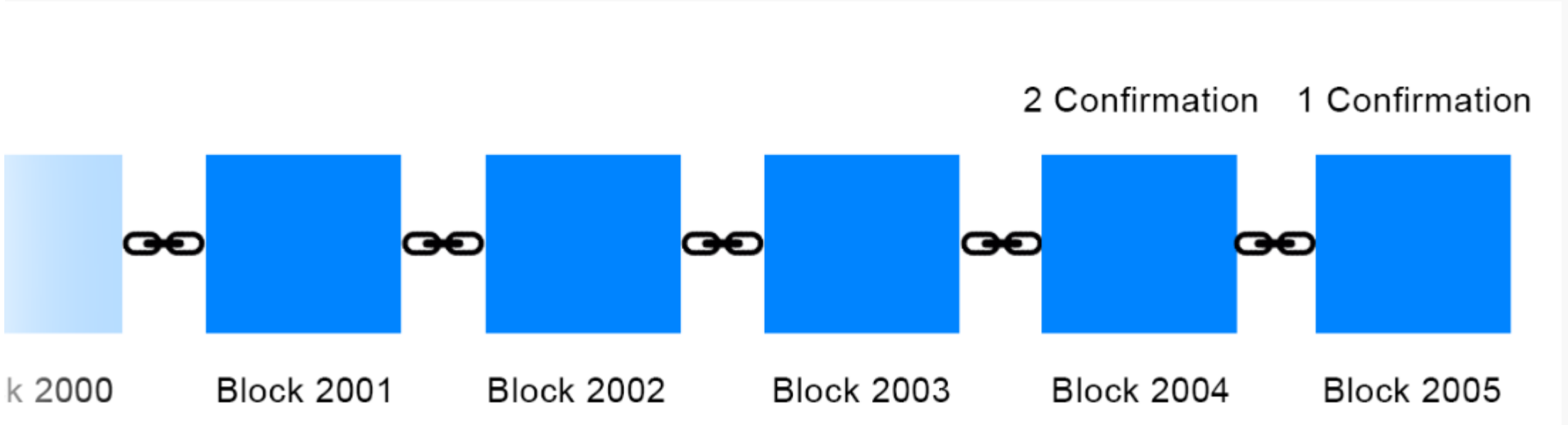


Bitcoin white paper - Calculations

Tomorrow

How is our transaction doing?

- Let us see how many confirmations we have now.s



Next

- Tomorrow: Distributed consensus
  - Reading material: [NA Ch2] + [SN]

- Lab this week: Implement a simple blockchain i Java
  - (start by downloading skeleton / spec. from Canvas)