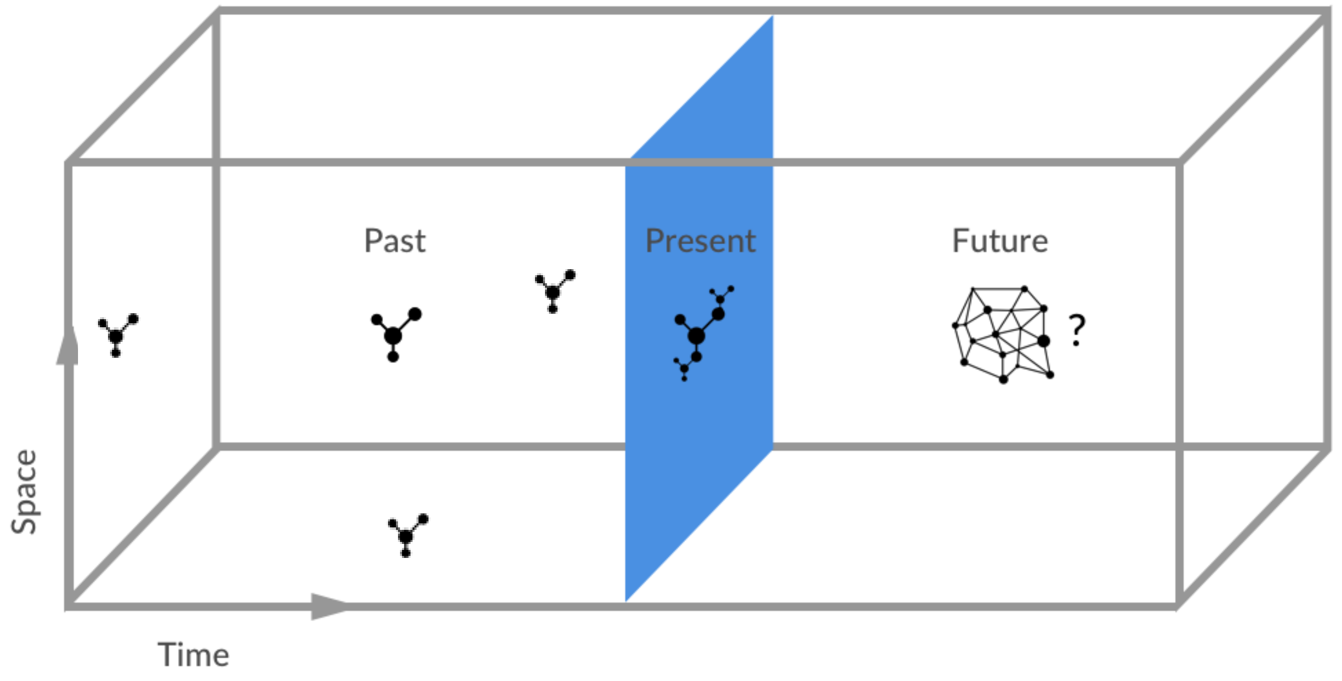
M183 Applikationssicherheit Implementieren
17

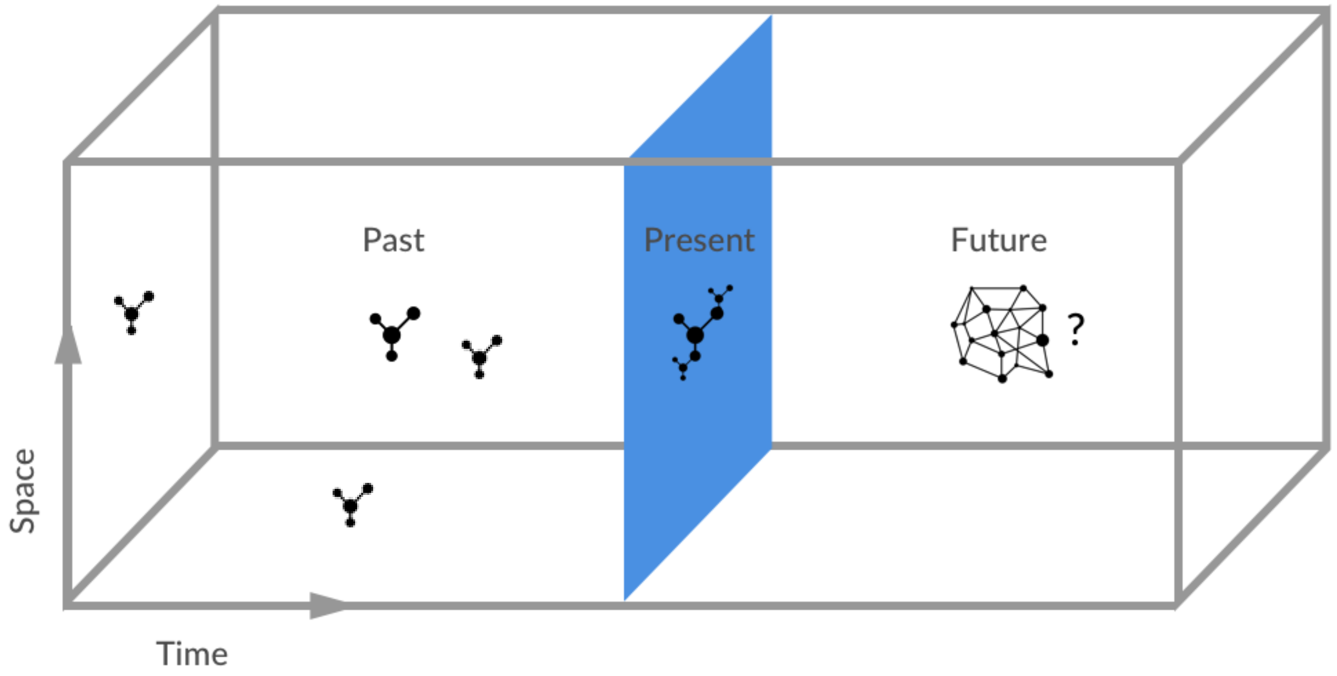
By Jürg Nietlispach

The Internet of the Past, Present and Future



What is happening?
What stands out?

The Internet of the Past, Present and Future



- **Isolated** Networks around organizations
  - CERN, etc
- **Centralized** (Client-Server)
  - Mandatory centralized Point (Server)
  - Centralized Databases
- **Distributed** / Decentralized
  - Peer-to-Peer

Isolated Networks

1970 - NPL Data Communications Network was a local area computer network operated by a team from the National Physical Laboratory in England that pioneered the concept of packet switching

1970 - Advanced Research Projects Agency Network (**ARPANET**) was an early packet switching network and the first network to implement the protocol suite TCP/IP. Both technologies became the technical foundation of the Internet.

Isolated Networks

Benefits

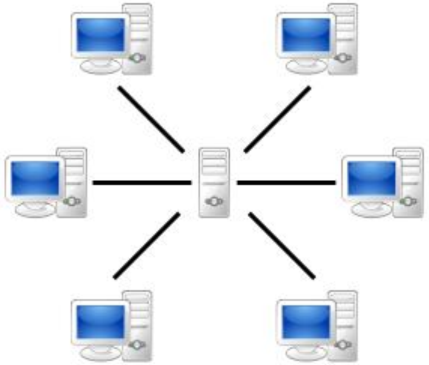
- **Security – isolated network traffic**
- **Access Control**
- **…**

Drawbacks

- **Isolation**
- **…**

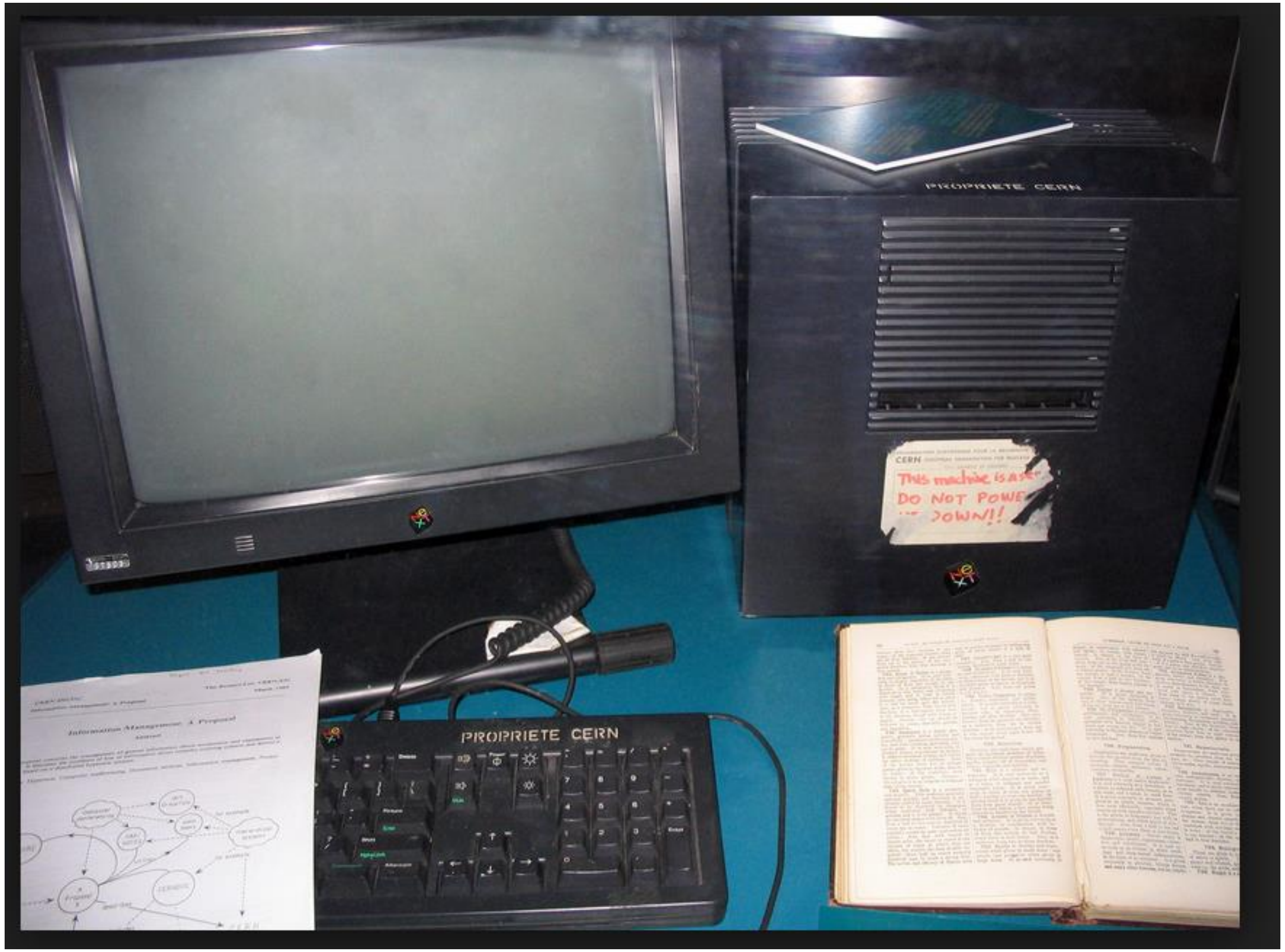
Centralized Networks

1990 – WWW, Client/Browser – Server Networks (Master/Slave) upon proposal of Tim Berners-Lee (https://www.w3.org/History/1989/proposal.html)



Info.cern.ch was the address of the world's first website and **web server**, running on a NeXT computer at CERN. The first web page address (for a **browser**) was http://info.cern.ch/hypertext/WWW/TheProject.html

First Web-Server

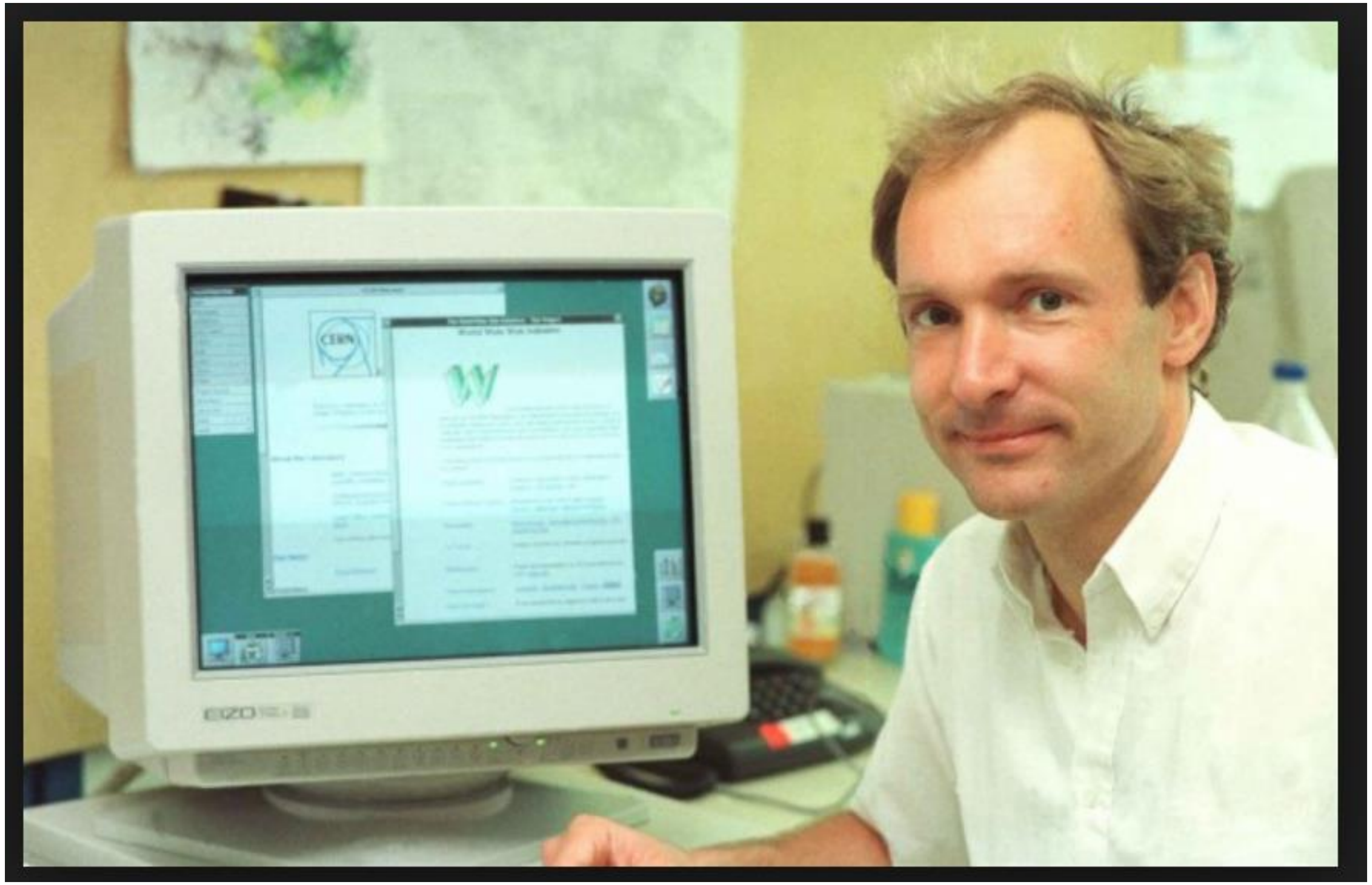


You can see the orginal NeXT computer still bearing the label, hand-written in red ink:

"This machine is a server. DO NOT POWER IT DOWN!!"

«First» Web-Browser

Browser & Tim Berners-Lee



Centralized Networks

Benefits

- spy (governments, big internet companies) on the common but mandatory points through which data has to pass before it goes to the recipients
- reducing data loss
- SaaS
- …

Drawbacks

- Spy (governments, big internet companies) on the common but mandatory points through which data has to pass before it goes to the recipients
- Only the Authorities/Owners define the Rules of the mandatory points (Servers)
- Single Point of Attack/Failure (Performance, Availability and Security)
- …

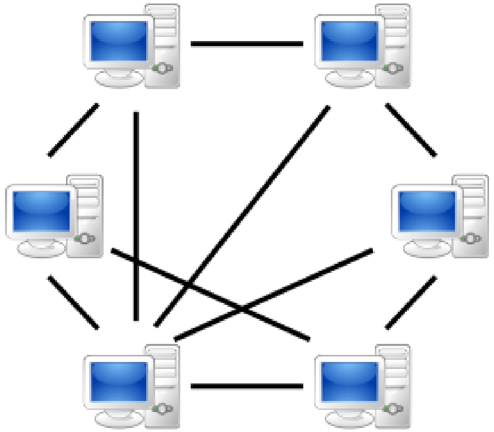
Centralized Networks

Most Webapplications that are in use today

- Sharepoint
- Google-Search
- Facebook
- Twitter
- Whattsapp
- …

Decentralized Networks

Peer-to-peer (**P2P**) computing or networking is a distributed application architecture that partitions tasks or workloads between peers.
Peers are equally privileged, equipotent participants in the application.
They are said to form a peer-to-peer network of nodes.



Decentralized Networks

Benefits

- Distributed resources, processing power, disk storage or network bandwidth
- No central coordination!
- Every Peer is Consumers and Producers at the same time.
- …

Drawbacks

- Can not be administered (i.e. illegal file-sharing?)
- Trust?
- Data recovery?
- …

Applications Decentralized Networks

- **Content delivery**

- File Sharing
  - Napster
  - Limewire

- Multimedia
  - BitTorrent

- Other
  - I2p
  - Blockchain
  - I2P
- …

Most of them have a bad flavour attached …

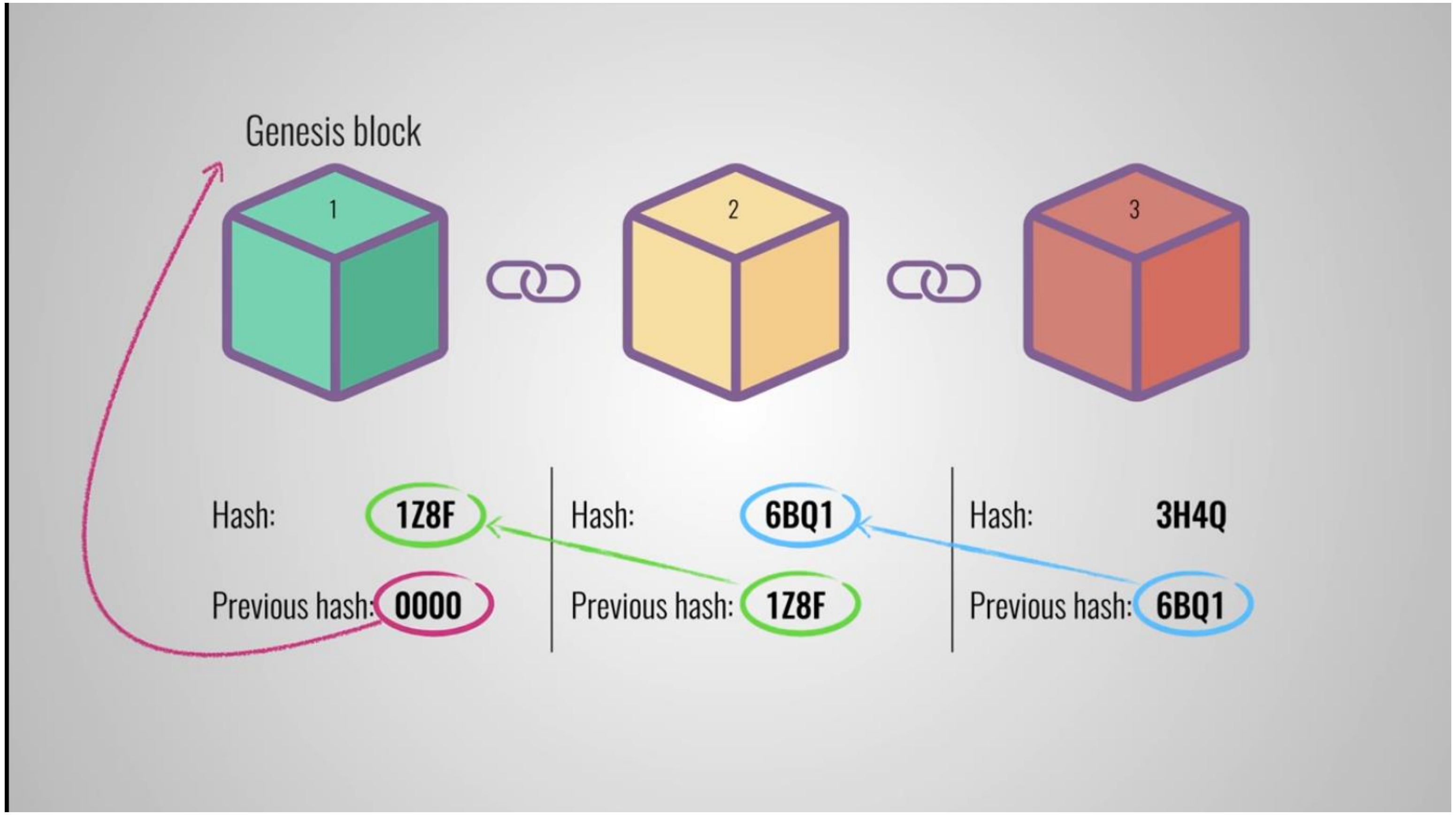
How to gain Trust (an other «good» things) in decentralized networks?

- **Policy-based trust (**focused on managing and exchanging credentials and enforcing access policies**)**

- **Reputation-based trust.** Using reputation to establish trust, where past interactions or performance for an entity are combined to assess its future behavior

- **Consensus-based trust (Blockchains)** is a trusted system of records (transactions, payments, data, …)

How Blockchain Works



https://www.youtube.com/watch?v=SSo_EIwHSd4

Private & Public Blockchains

The sole distinction between public and private blockchain is related to who is allowed to participate in the network, execute the *consensus* protocol and maintain the shared ledger (transaction-database)

Public Blockchains

A public blockchain network is completely open and anyone can join and participate in the network.
The network typically has an incentivizing mechanism to encourage more participants to join the network.

Examples (besides Bitcoin)

Ethereum, Provider of a decentralized platform and programming language that helps running smart contracts and allows developers to publish distributed applications.

Blockstream – Provider of blockchain technology, focused on extending capabilities of cryptography and distributed systems. Their vision is to form an ecosystem for solving problems in financial systems related to fraud, counterfeiting, accountability and transparency.

Factom – Have developed underlying blockchain data infrastructure for an open source platform called Factom technology.

Private Blockchains

A private blockchain network requires an invitation and must be validated by either the network starter or by a set of rules put in place by the network starter.
Businesses who set up a private blockchain, will generally set up a *permissioned* network

Eris Industries – Provider of multi-network blockchain client. It is a controllable, smart contract-enabled, proof-of-stake based blockchain design.

Blockstack – Developers can use APIs by blockstack.js to authenticate the user, fetching and storing application data.

MultiChain – Provides an open source distributed database for financial transactions.

Chain Inc. – Similar to Multichain, it's an enterprise grade blockchain infrastructure that enables organizations to build better financial services from the ground up.

Overall Benefits of Blockchains

1. Trustworthy system:
Data structure build using blockchain allows users to make and verify data-transactions without a third-party involvement.

2. Transparency:
Blockchain data is complete, accurate and consistent with all the members (distributed ledger-system)

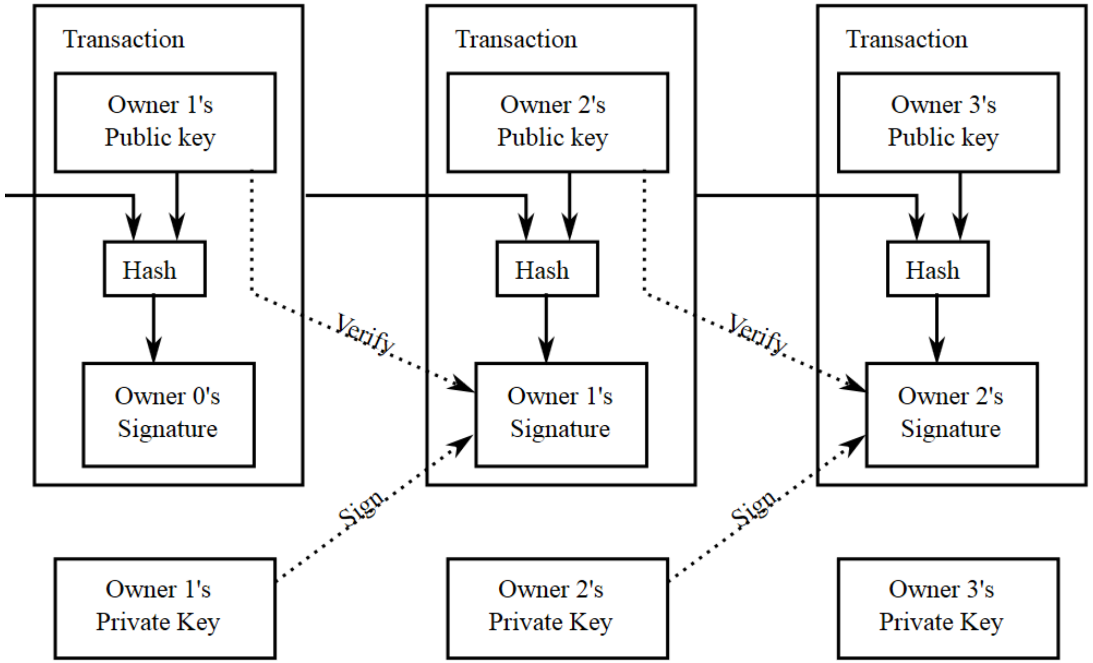
3. Faster transactions:
Physical parties even working with digital documentation takes longer time to execute transactions

4. Reduced transaction costs:
A transaction system build using blockchain eliminates third party intermediaries and overhead costs for exchanging assets.

Applications of Blockchains

Bitcoins, …

How Bitcoins work



Bitcoin-Network bases on a blockchain network - **but** with a special Proof-of-Work behaviour (called Mining)!

Mining / Proof of work

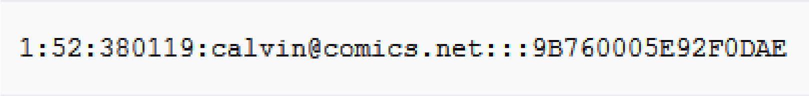
In order to validate a new transaction in the bitcoin network, the following proof-of-work (puzzle) has to be calculated:

Find a dedicated hash for a block requiring a certain number of leading zeros by incrementing a nonce value and recalculating sha256 again and again.

When a node finds a proof-of-work, it broadcasts the block t
o all nodes.

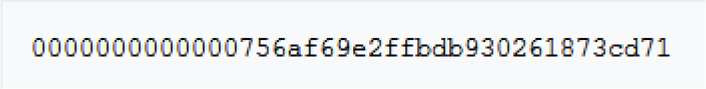
Mining Example

In order to verify the following e-mail transaction for calvin@comics.net on January 19, 2038,



```
1:52:380119:calvin@comics.net:::9B760005E92F0DAE
```

We have to verify first, that the Sha1 of the message meets our proof-of-work, requirement, i.e.



```
0000000000000756af69e2ffbdb930261873cd71
```

Which requires 2^{52} hash computations!

Proof of work Puzzles

- Integer square root modulo a large prime[1]
- Weaken Fiat–Shamir signatures[1]
- Ong–Schnorr–Shamir signature broken by Pollard[1]
- Partial hash inversion[11][12][2] This paper formalizes the idea of a proof of work (POW) and introduces "the dependent idea of a bread pudding protocol", a "re-usable proof of work" (RPOW) system.*[13] as Hashcash*
- Hash sequences[14]
- Puzzles[15]
- Diffie–Hellman-based puzzle[16]

Applications of Blockchains

Read the Paper von Satoshi Nakamoto https://bitcoin.org/bitcoin.pdf

And subscribe to https://www.udemy.com/the-bitcoin-course/