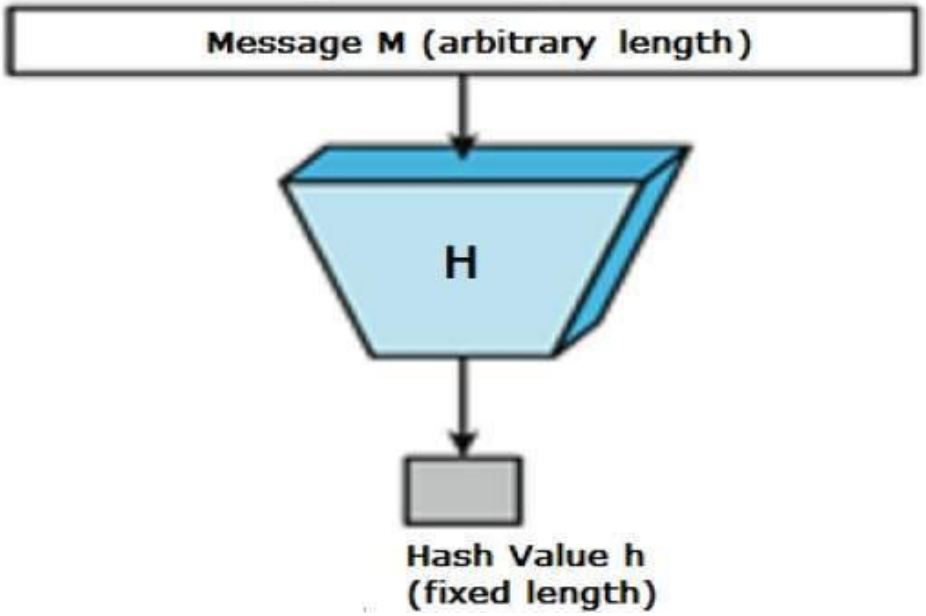
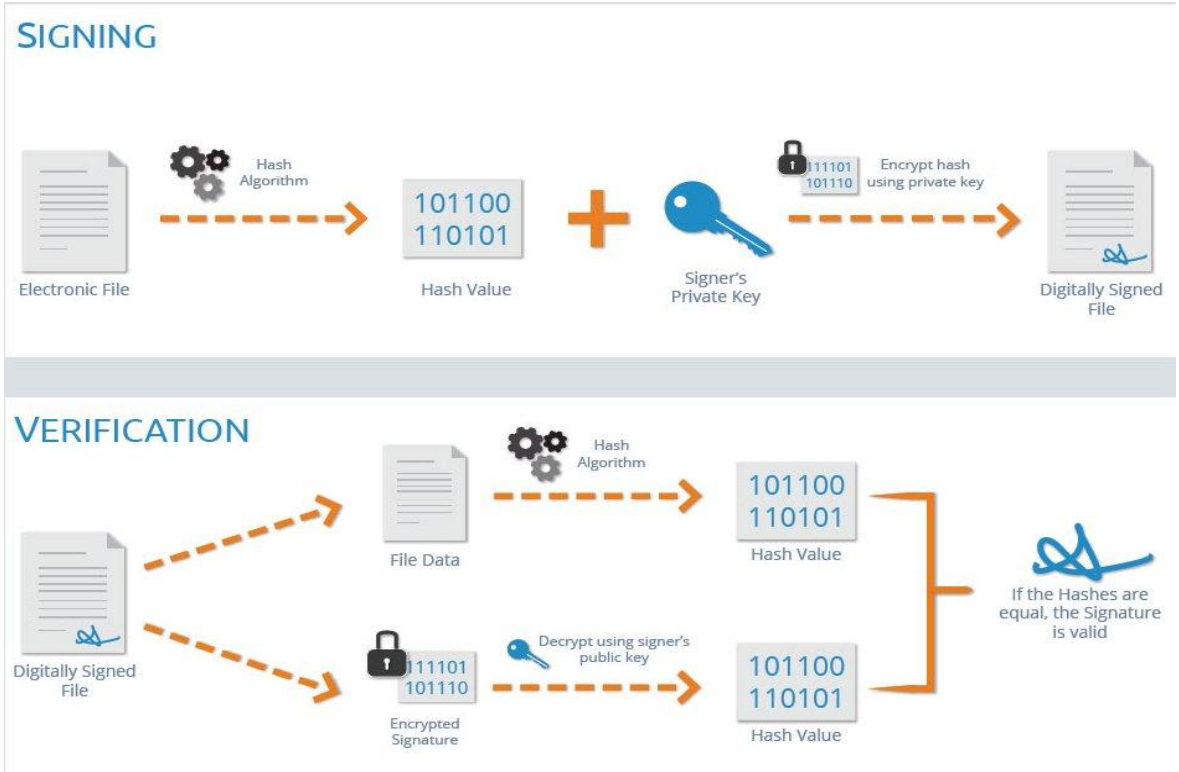
Blockchain Technology

Karampinakis Manolis
mkarabin@csd.uoc.gr

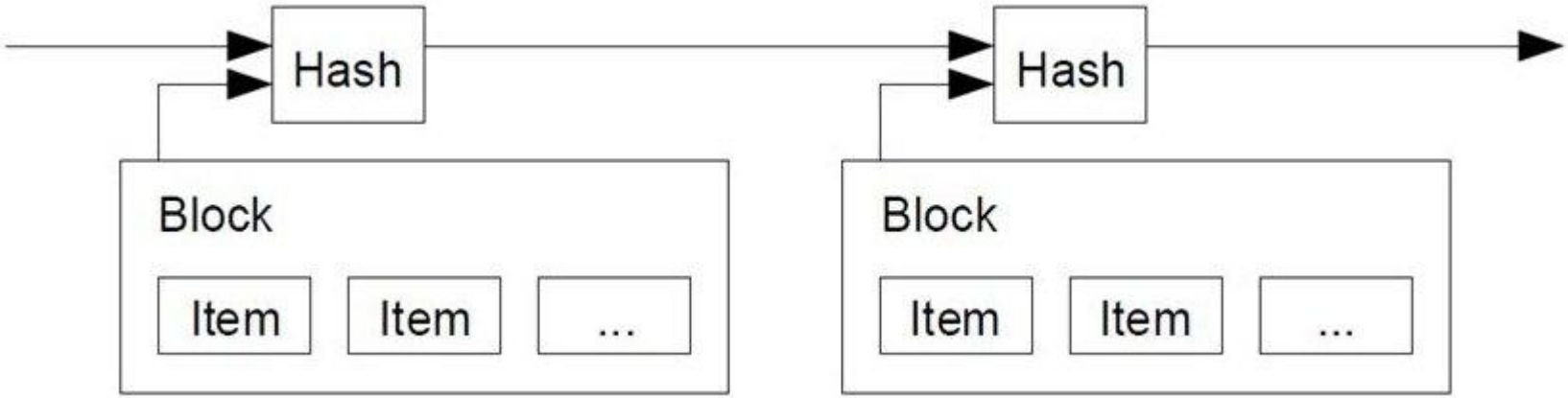
Hash functions (1975): one-way easy to compute but hard to invert



Digital signatures (1975): “equivalent” to manual signature

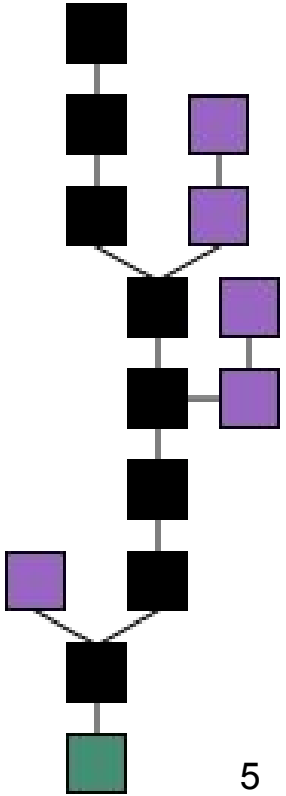


Timestamping: temporal order among sets of events

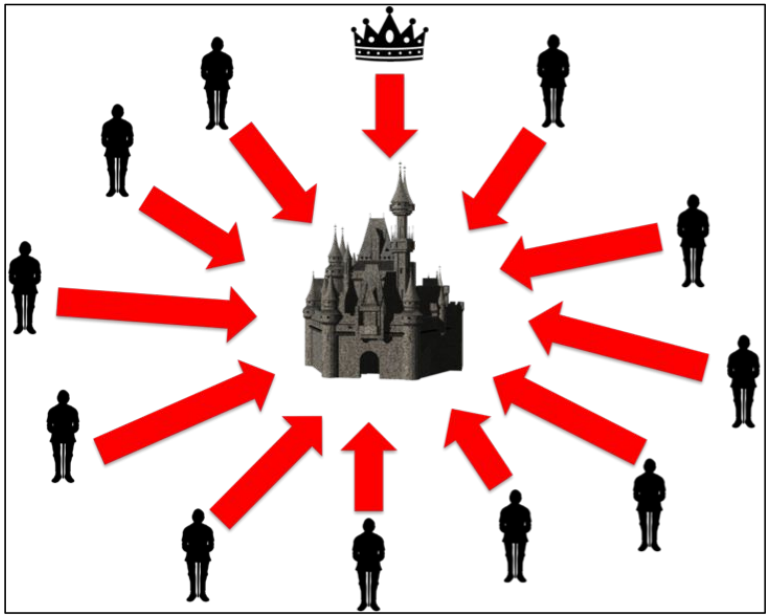


Blockchain

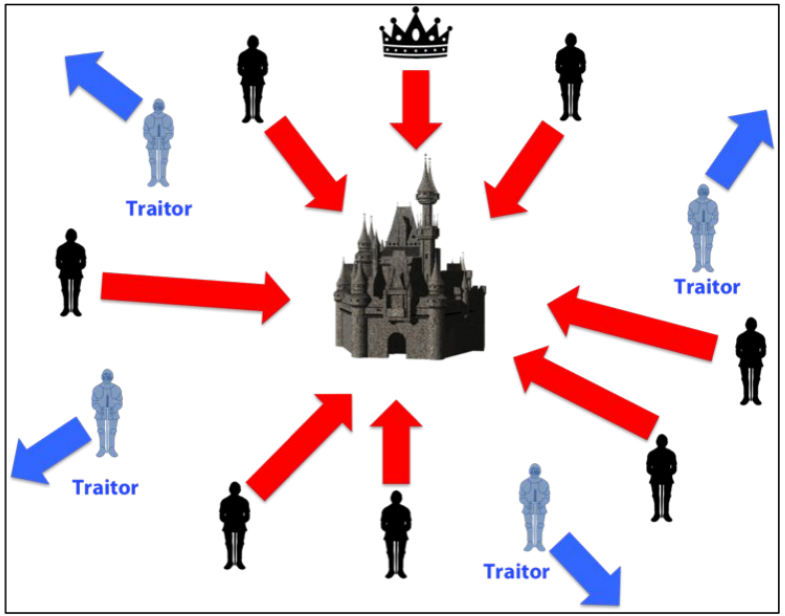
- A continuously grwing list of records (blocks), which are linked and secured using cryptography.
- By design, inherently resistant to modification of the data.
- Secure by design.
- Anonymity can be ensured, but is not a prominent design goal.
- Distributed computing system with high Byzantine fault tolerance



Byzantine generals problem



Coordinated Attack Leading to Victory



Uncoordinated Attack Leading to Defeat

Blockchain as a decentralized ledger

Introduced in 2008 by an anonymous person (or persons) under the pseudonym Shatoshi Nakamoto as the technology that implements bitcoin.

- Using a peer-to-peer network.
- Each peer has his own copy of the ledger.
- Peers follow a protocol to validate new blocks.
- When a block enters the chain it cannot be altered without the alteration of all subsequent blocks and the consensus of the majority of peers.

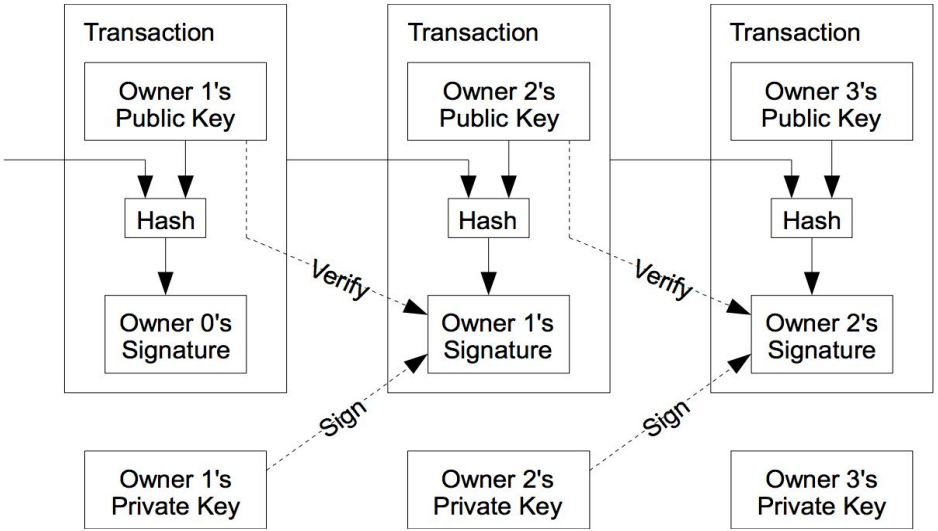
Blockchain as a decentralized ledger

Changed the rules in digital currency solving the **verification** and the **double spending** problems.

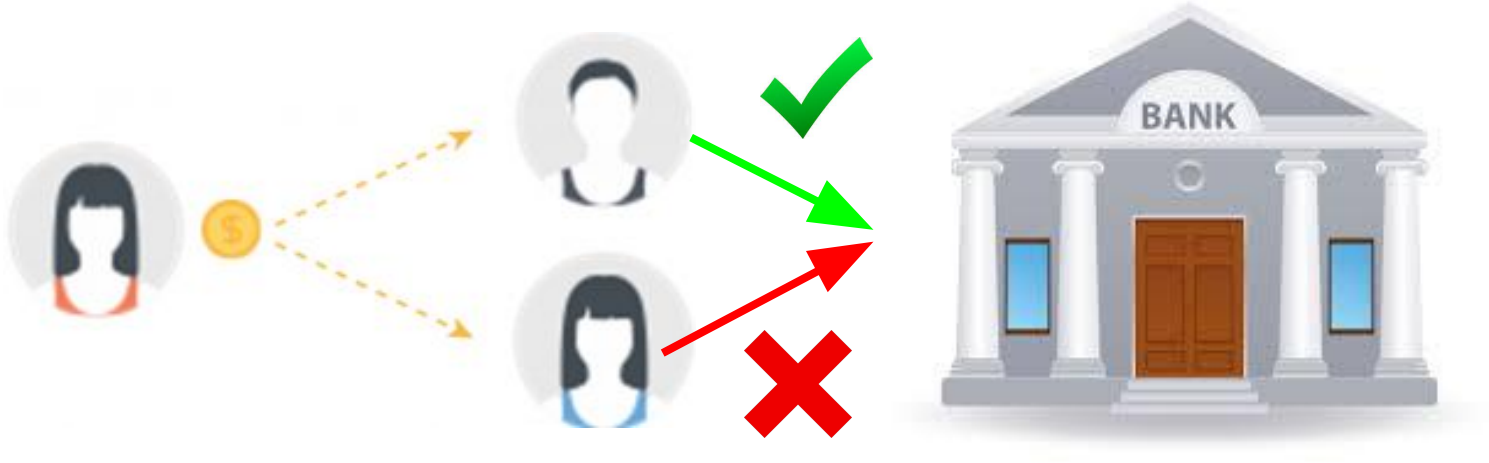
1. **Verification:** Digital signatures.
2. **Double spending:** timestamp server.

Verification

Electronic coin is a chain of digital signatures.Every bitcoin node digitally signs a hash of the previous transaction where this bitcoin was spend, along with the future owner's public key, and incorporates this signature in the transaction.



Double spending with a central authority



The bank will validate only the first transaction.

Double spending on a distributed system

- Solved with a **timestamp server**.
- Every transaction is public and users agree to a single history of transactions.
- The majority is described as the longest chain.
- Miners add new blocks in the blockchain by trying to find a proof-of-work, and receive some free coins if they succeed.
- To add a non-valid block, one must have 51% or more, of the computational power of all the miners.

Other uses of the blockchain

Decentralized consensus has been achieved with blockchain.

We have solved the problem of **TRUST** between parties without a central authority.

Other uses of the blockchain

Apart from financial services, the blockchain is potentially suitable for:

- Recording of events
- medical records
- identity management
- transaction processing
- food tracebility

Other uses of the blockchain - How?

Bitcoin: Turing incomplete scripting language for security and efficiency. It can only be used as a cryptocurrency.

Ethereum: A blockchain based platform with additional features and applications. It is Turing complete, meaning that you can write programs (contracts) that can solve any reasonable computational problem. It is thus able to implement ***smart contracts.***

Other uses of the blockchain - Examples

- **Registering land:** Sweden is putting its land registry system on a blockchain: stamp out fraud, real estate transactions visible.
- **Music Industry – copyrights:** *Imogen Heap* released her song *Tiny Human* using a blockchain platform: artists sell direct to their fans.
- **Digital Voting:** In 2014, Liberal Alliance, a political party in Denmark, became the first organization to use blockchain to vote.
- **Tracking blood diamonds:** *Everledger* is using blockchain to certify and track diamonds.

Summary

- Blockchain is a ***decentralized*** database.
- Blockchain is **public**, **secure** and resistant to modification of the data.
- Apart from cryptocurrencies, a blockchain platform can do a lot more.

Thanks!