Blockchain – the basics

Michael Claudius, Associate Professor, Roskilde

16.03.2020

What is blockchain?

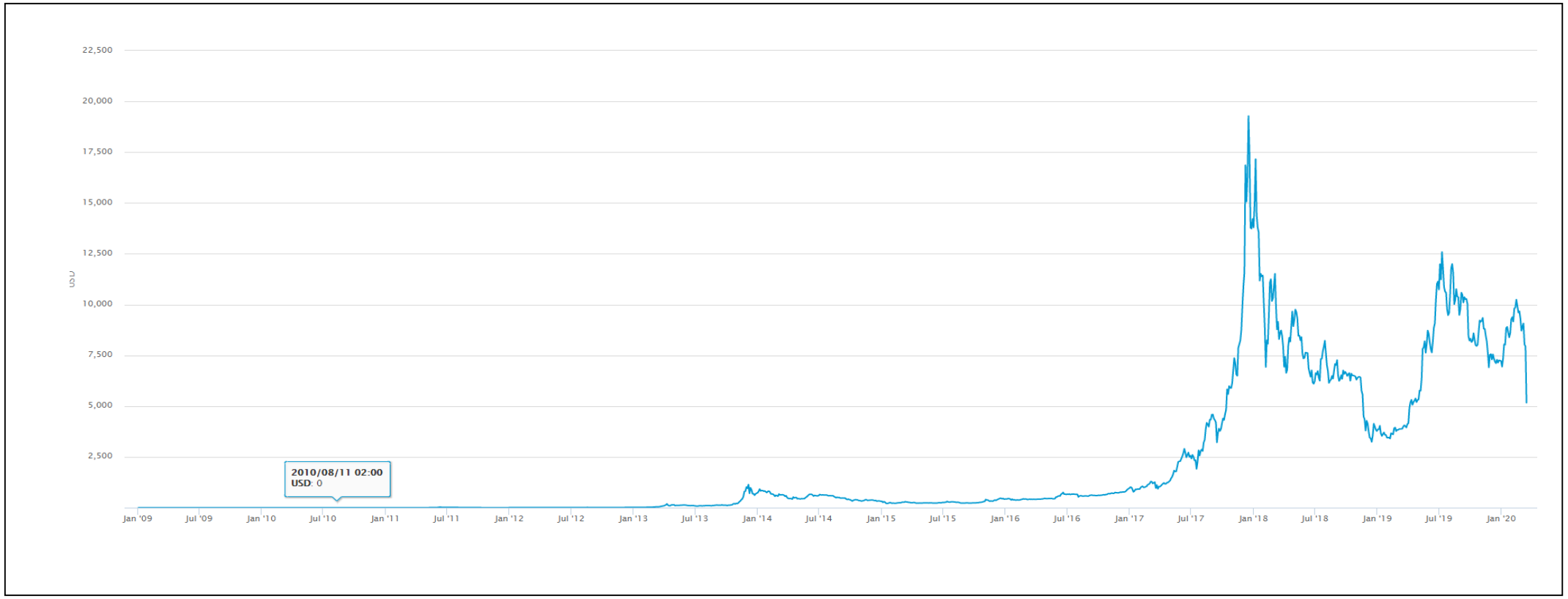
- **A distributed ledger.** Keeps tracks of all transactions from start up till now.
- **P2P network with nodes/peers (members).** We are all equal!
- **100% Decentralized.**
- **100% redundant information.** We all have the same bitcoin block!

- **A chain of blocks**
- **Each block has a reference to the previous block**

History the start 1991

- **Stuart Haber & W. Scott Stornetta 1991, one block one document**
- **Bayer, Haber and Stornetta 1992: Merkle trees: one block several documents (transactions)**
- **Satoshi Nakamoto 2008,**
- **Bitcoin article:** https://bitcoin.org/bitcoin.pdf

Bitcoin, Exchange rate



Bitcoin

- **Bitcoin,** https://www.bitcoin.com/

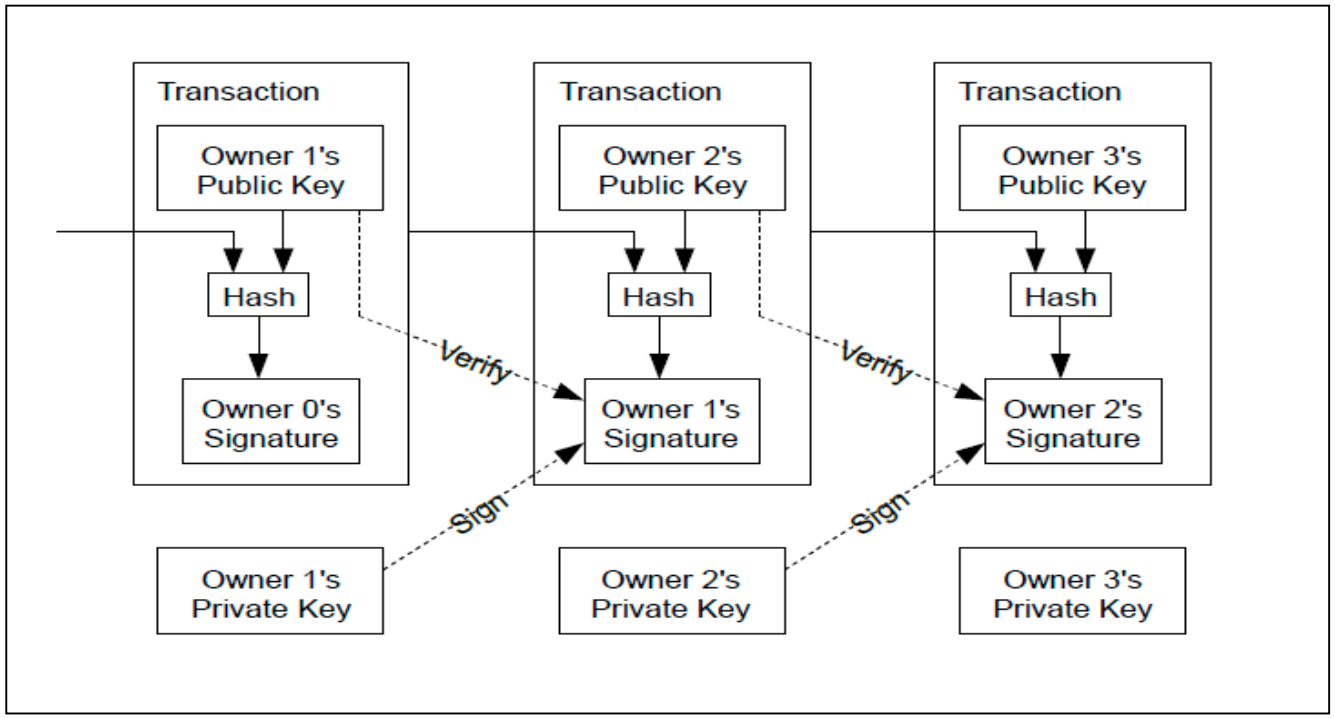
Well known examples

- **Bitcoin,** https://www.bitcoin.com/
- **Ethereum**
- **Shipping applied**
- **More examples, you will find them later !**

- Lets see blockchain in action: BlockChain Introduction (6 minutes)

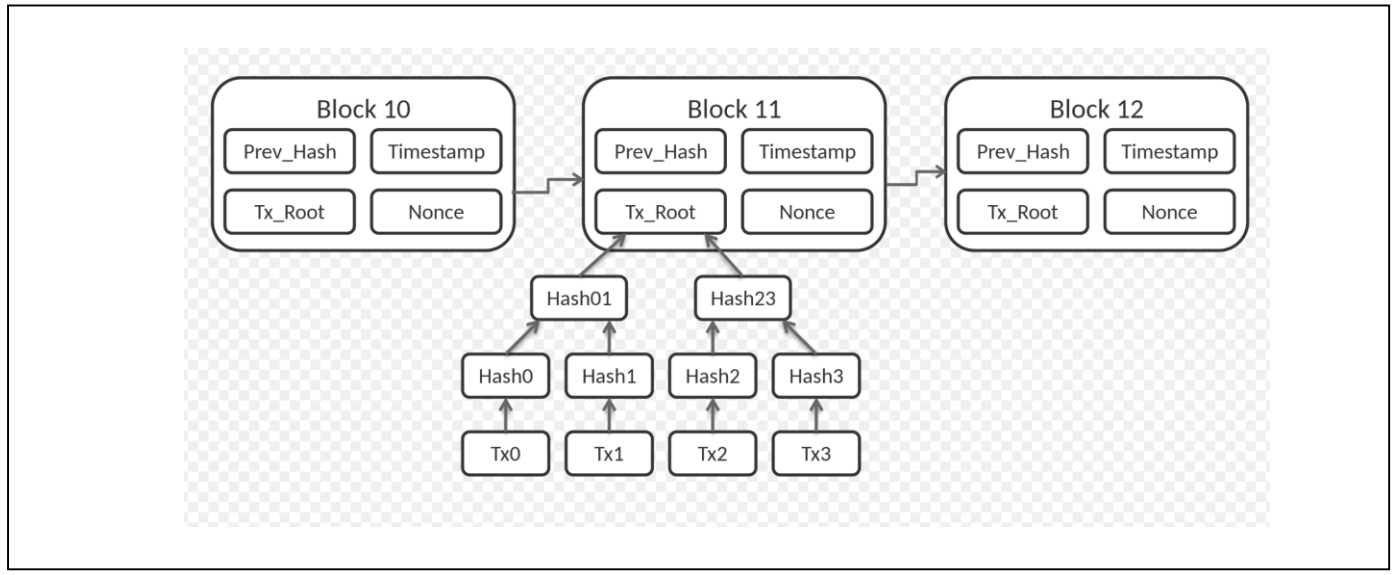
Transactions (T)

Problem: How to transfer an electronic coin from Owner no. 1 to Owner no. 2: O1 ->-----T_1----> O2
Solutions: Each owner signs a hash of previous transaction. $K_1^-(H(T_1,K_2^+))$



Security

Problem: How to avoid one sneaky node to spend the same the e-coin two times (double spending problem?
Solution: All nodes know all transactions and must agree on this
Ensure the order by a timestamp. Hash[Hash(previous block), timestamp, transaction data]



Security

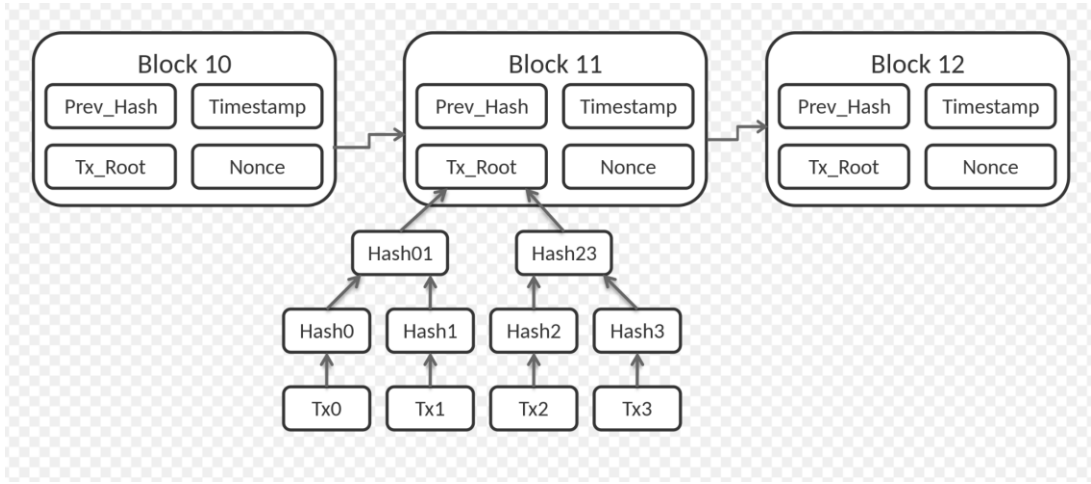
Problem: How to ensure nobody can tamper a hash value in block ?

Solution: Proof of work, add a nonce to the block.

The nonce is found by incrementing the value untill the block's hash begins with required number of zeros

The more zeroes, the more difficult, the longer time it will take to generate a block

Since the hash changed all later blocks declare the block for invalid



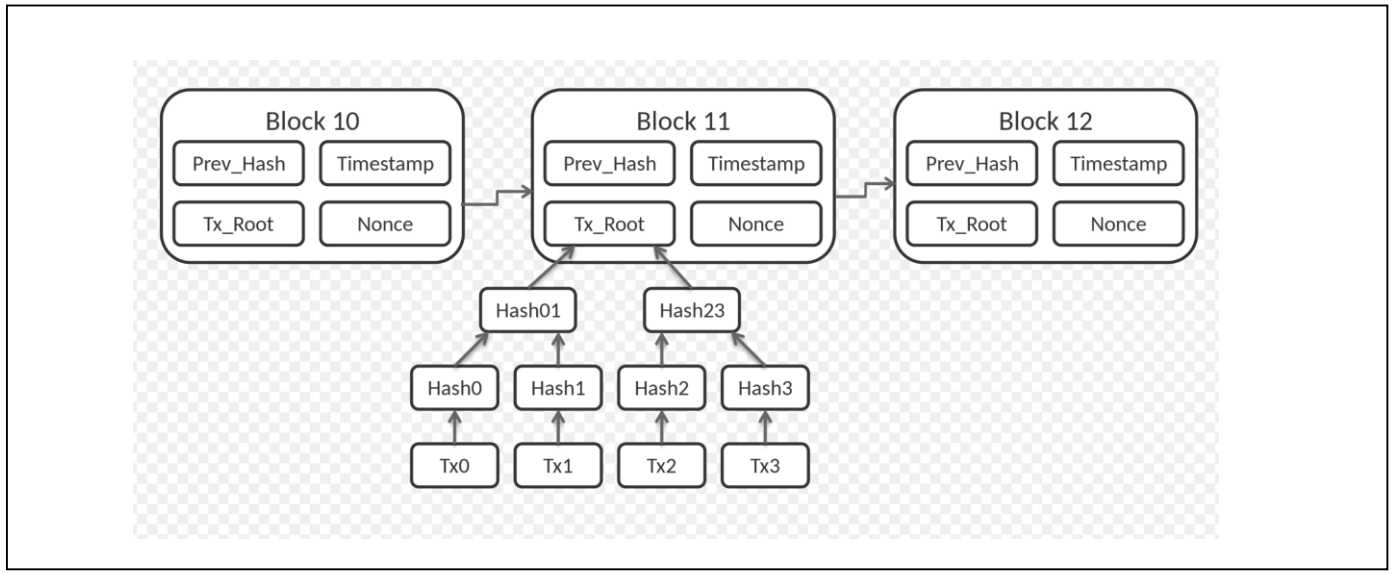
The network procedure

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.

- Lets see it in action: Secret Chinese Bitcoin Mine

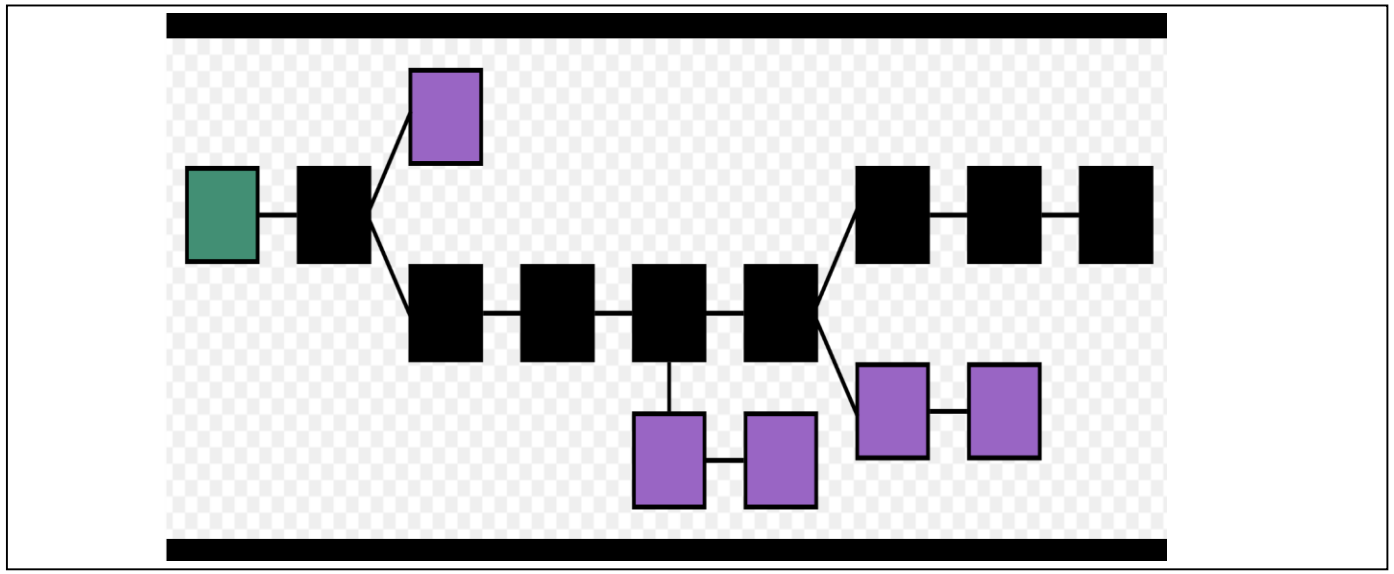
Security

Problem: How to avoid one miner getting the 51% power in bitcoin
Solution: Control the difficulty of *“Proof of work”*. Too fast increase difficulty, too slow decrease difficulty



Temporary fork

Problem: What if two miners at the same time solves the block and a node receives two blocks at the nearly same time?
Solution: Choose later the longest chain when transactions covered by many others, I.e. wait 6 blocks..



Hard fork

Problem: Attacked by hacker due to SW error.
Solution: Hard fork 51% agreement needed.
Success: All nodes change old SW to new SW. Succes for Ethereum split into new and clssiv
Failure: All nodes deny and old SW is not replaced new SW. Failure then what ?
Worst case: Pay ransom Nxt 50 million ?!

Can you Google other attacks ?

Assignments

Time for a little discussion and some work.

Blockchain questions

Mandatory Blockchain project