# H4 BitCoin intro

## Bitcoin: A peer-to-Peer Electronic Cash System (Nakamoto 2008)

* Peer-to-peer electronic cash system directly to one party to another without financial institution.
* Digital signatures without the double-spending are part of the solution.
* Trust based model is still weakness in online payment.
* Peer-to-peer distributed timestamp server to resolve the double-spending problem.
* Electronic coin is a chain of digital signatures. A coin is transferred to each owner using digital signing with hash and public key.
* Timestamp server takes a hash from block, sign it and publish.
* Timestamp server forms a process using signing and the hashes to be creating block chains.
* First transaction in a block that starts a new coin is a special transaction owned by the creator. this adds incentive for nodes to support the network and initially distribute coins into circulation.
* Block chain is possible break in with luck and fast computers. This behavior is controllable by honest nodes which are set to control CPU power.

## Bitcoin and Cryptocurrency Technologies (Felten 2015)

Learn about cryptographic building blocks: Crypto background, hash functions, digital signatures and applications.

* Cryptographic hash functions
  + Mathematical function which takes whatever string as an input. Collision free, meaning that no one can find values of x or y, hash values. Theoretically the collision is possible to open, but in practice it’s infinitesimally small. Bit coin uses SHA-256 hash function. In a nutshell, bitcoin uses the collision free hash functions to securely hide the functions it uses.
* Hash Pointer and Data Structures
  + Hash pointers are pointers which indicates places where information is stored. Hash pointer let possibility to ask information back also verifying that information has not changed. It is possible to build different kind of data structures using hash pointers and pointing to the structure using the pointers after.
* Digital Signatures
  + Basically, there two things what digital signatures need to do: Only you can assign the signature and anyone who sees it can verify that it’s valid. And the second one is that the signature is tied to particular document. Meaning, the signature can’t be used any other document. On top of the previous ones, one key element is that the signatures can’t forge by any adversaries. Bitcoin uses specific digital signature scheme called ECDSA which is also US government standard.
* Public keys as Identities
  + Using public keys with secret keys to assign digital signatures is fairly simple process to give someone to access write the document. Giving access to assign digital documents by generating the key pair and creating random identity with decentralized identity management. Bitcoin does identities this kind of way.
* A Simple Cryptocurrency
  + Hash functions and digital signatures related to cryptocurrency. GoofyCoin is the simplest cryptocurrency there is. Digital signature is generated to the coin, and it points out who’s ever the coin is. Passing the coin to someone else using hash pointer and public key. GoofyCoin is not secure as it makes double-spending possible. ScroogeCoin solves the double-spending problem by publishing its transaction history and that will be a block chain. ScroogeCoin is thing that it does in practice.

## a) Really black Friday

How much is one BitCoin’s (BTC) worth now? The value is:16 620.10$

How much money could I have won investing a BitCoin at the early phases: One BitCoin’s value was 0.0009$ when the first transaction has made in 2009 (Ashmore, Powell 2022). Compering one BitCoin’s value in October 2009 to current course and value, is the worth approximately: 18 466 593,11$. Using official calculator which starts counting the values from December 2015 to current. One bitcoin’s value is increased from that time 55.7 times (Influencemarketinghub). BitCoin’s value was 324.47$ in 2014 and compering that to current value 16620.10$ makes the difference approximately 51.2 times. So, compering the early stage when the investment was possible according to Coindesk.com’s page. The win buying one BitCoin in 2014 could have been 16295,63$ to current. Based on Coindesk.com’s page the highest value for the BitCoin was in 2021 increasing up to 67553.95$. Buying one bitcoin at that time could cause a buyer as much as 50933,85$ lost.

## b) What’s a block chain?

Block chain is data storage which uses SHA-256 algorithm to secure data inside of the storage. The storage itself contains transaction data which is secured by the encryption methods. As a new transaction occurs a new block is created, and the systems contains earlier transactions history. The Block chain is a way to manage BitCoin transactions.

## c) Not a BitCoin.

There are quite many other cryptocurrencies on the market now. Giving a couple of examples: LiteCoin, Ethereum, Dash, and PeerCoin. Most of the altcoins uses a similar BlockChain technology as BitCoin. PeerCoin offers improved the efficiency of mining and better currency security. Dash strives faster transactions and offers enhanced privacy protection. Ethereum and BitShares offer digital platform to make smart contracts. LiteCoin give a guarantee of improved computer power to mining (Ciaian, Rajcaniova & Kancs 2018).

## Sources:

Ashmore, D. Powell, F., 2022, Readable: <https://www.forbes.com/advisor/in/investing/cryptocurrency/bitcoin-price-history-chart/> Read: 20.11.2022

Ciaian, P., Rajcaniova, M., Kancs, d’A. 2018. Journal of International Financial Markets, Institutions and Money, Virtual relationships: Short- and long-run evidence from BitCoin and altcoin markets , Readable: [Virtual relationships: Short- and long-run evidence from BitCoin and altcoin markets - ScienceDirect](https://www.sciencedirect.com/science/article/pii/S1042443117302858) Read: 22.11.2022

Coindesk.com, Readable:<https://www.coindesk.com/price/bitcoin/> Read: 20.11.2022

Felten W. E, 2015, Coursera, Bitcoin: A Peer-to-Peer Electronic Cash System, Readable: [A Simple Cryptocurrency | Coursera](https://www.coursera.org/learn/cryptocurrency/lecture/rJ8KJ/a-simple-cryptocurrency) Read: 19.11.2022

Google finance, Kryptovaluutta, Readable: <https://www.google.com/finance/quote/BTC-EUR?sa=X&ved=2ahUKEwjW06rUwLz7AhVBpIsKHWuxDusQ-fUHegQIBhAe&window=MAX> Read: 20.11.2022

Influencemarketinghub.com, Crypto Profit Calculator, 2022, Readable: <https://influencermarketinghub.com/crypto-profit-calculator/> Read: 20.11.2022

Nakamoto, S. Bitcoin: A peer-to-Peer Electronic Cash System, Readable: [bitcoin.pdf](https://bitcoin.org/bitcoin.pdf), Read: 20.11.2022