FINTECH AFTER DARK

Short Introduction to Blockchain

Boosting your performance in the connected world.

Jouni Mykkänen
22.11.2017

Blockchain - contents

- Blockchain – what is it?
- Historical steps
- Idea
- Pros and cons
- Applications

Blockchain – what is it?

- A collection of cryptographic methods for distributed and persistence in a trustless environment.
- Blockchain is a list of transactions arranged in blocks which form a chain.
- Blockchain is replicated and transparent to all participants.
- Participants maintain the infrastructure and integrity of the blockchain without trusting each other.
  - Compare internet.

Blockchain – beginning

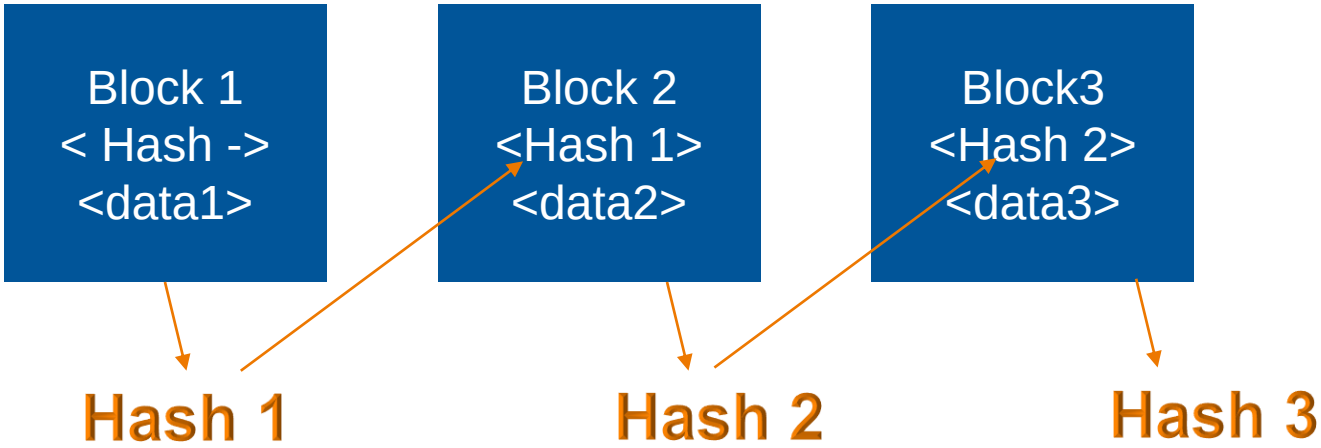
- 1991 Cryptographically secured chain of blocks (Stuart Haber and W. Scott Stornetta).
- 1992: Merkle trees to store several documents efficiently in a block (Bayer, Haber, Stornetta).
- 2008 digital currency: **Bitcoin** (Satoshi Nakamoto)
  - Solved double spending problem without requiring a trusted administrator.
  - Term “block chain”

Blockchain – recent steps

- 2014
  - “Blockchain 2.0” new applications of the distributed blockchain database.
  - 2nd generation programmable blockchains for smart contracts
- 2016
  - IBM blockchain innovation research centre, Singapore

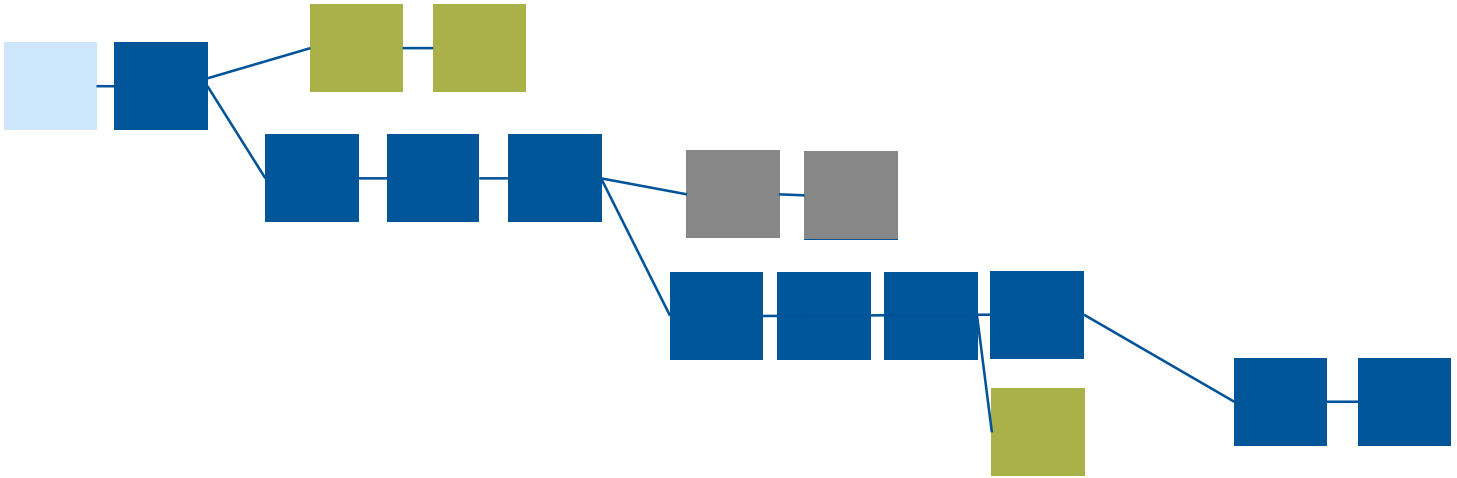
Blockchain – key idea

- Each block contains a hash digest of the previous block.



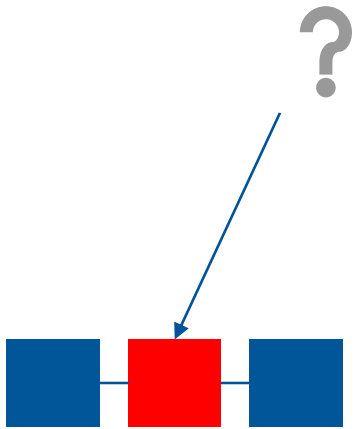
Blockchain – longest valid blockchain

- Branches occur in blockchain due to nature of distributed processing.
- Consensus rules are used to decide which blockchain is the most authoritative, in practice the longest valid one.



Blockchain – transaction updates?

- Changing a transaction in a historical block requires building a new valid longest blockchain on top of the newly changed block.
- In real world applications, this is not feasible.
  - blocks can only be created in a constant rate
  - the longest blockchain has a head start.



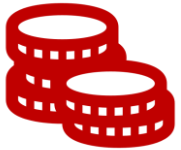
Blockchain – pros and cons

CYBERCOM GROUP

Pros	Cons
Distributed	Design flaws, how to handle
No single authority	Currently limited transaction rate (e.g. stock markets)
Transaction fees compared to traditional techniques	Transaction fees (with some implementations)
Trust between unknown parties	Are involved parties really independent?
Publish immutable information	Information clean-up (right to be forgotten, illegal content)
Transparent to all participants	Key management challenges

Blockchain - applications

- Money transactions: tight competition on going
  - Bitcoin, Ethereum, Dash, …etc.
- Agreements (land owning, etc.)
- Royalty collection for music industry.
- Data integrity
  - Healthcare records
    - On going work with health record integrity verification.
  - Log data integrity



Blockchain – future applications

- Smart contracts
  - mortgage, marriage, …etc.
- Clearing and settlement
  - Stock transactions
- Payments
  - Peer to peer
- Smart assets
  - Shipping goods
- Digital identity
  - Own identity + added objects
- Voting
  - Secure, reliable, … etc.
- Healthcare
  - Data collaboration, secure share, …
- Insurance
  - Avoid identical claims, …

Blockchain – points to start

CYBERCOM GROUP

- https://en.wikipedia.org/wiki/Blockchain
- http://www.ledger.org
  - Hyperledger Fabric: a framework
- https://en.wikipedia.org/wiki/Ripple_(payment_protocol)

- https://www.ethereum.org
- https://www.blockchain.com
- https://ripple.com
- https://www.dash.org

Blockchain – case fintech

- Blockchain era has begun.
- It is time to explore new potential applications.
- For bank and related business blockchain ecosystem open very interesting opportunities.

- Next, Tero introduces the case in fintech: Chain identity management.
- Workshop: Let's Code Ethereum!

CYBERCOM GROUP

cybercom.com