Blockchain matters

Why does blockchain matter?

Balázs Héder, Ph.D.

December 2021

PART 3

Have you ever heard these phrases?

Blockchain matters

Blockchain is going to change the World!

Bitcoin bubble has been popped!

Bitcoin is a bubble!

Bitcoin is the money of criminals!

Bitcoin bubble is going to be popped!

Bitcoin is dead! Bitcoin Obituaries, url

Blockchain is immutable!

Bitcoin is the blockchain!

Blockchain is not Bitcoin!

Blockchain contains the truth!

Smart contracts are running on the blockchain.

Cryptocurrencies are useless, but blockchain is good!

Blockchain is secure!

Have you ever heard these phrases?

Blockchain matters

Blockchain is going to change the World!

Bitcoin bubble has been popped!

Bitcoin is a bubble!

Bitcoin is the money of criminals!

Bitcoin bubble is going to be popped!

Bitcoin is the blockchain!

Blockchain is immutable!

Blockchain contains the truth!

Smart contracts are running on the blockchain.

Cryptocurrencies are useless, but blockchain is good!

Blockchain is secure!

Confusing, isn't it? To get better understanding and to be able to decide which statement is true, follow this presentation series!

Outline of the whole series

Blockchain matters

- Little steps to the beginning
- The born of the technology
- Bitcoin, why is it so important?
- OK, so what is blockchain? And what is DLT?
- Consensus mechanisms
- Oracles
- Ethereum, the world computer
- Smart contracts
- Tokens and the digitization of physical objects, NFTs, SFTs
- The tsunami of cryptocurrencies
- ICO, IEO, STO, CeFi/DeFi, DID and other buzzwords
- The enterprise answer: consortium/private blockchain solutions
- When can/should I use blockchain? - The blockchain solution feasibility chart
- Possible use cases

Notation of references

Blockchain matters

References related to a slide are listed at the bottom of the slide, or right next to the text.

Visual Capitalist, G. Bhutada, “Purchasing Power of the U.S. Dollar Over Time”, 2021, url.

EOS, url

Solana, url

CertiK, “The Blockchain Trilemma: Decentralized, Scalable, and Secure?”, 2019, url

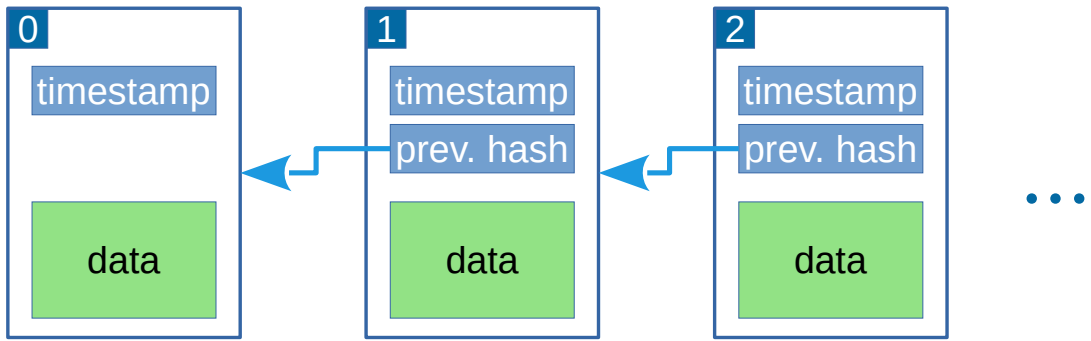
Blockchain matters

Part 3 – Blockchain

The technical definition

Blockchain matters

- A kind of distributed ledger
- Data is arranged into blocks
- Blocks are linked using cryptographic hash functions
- The software maintaining the blockchain run by nodes
- Nodes form a P2P network
- Nodes must agree on the data to be written in the next block



The pillars of blockchain

Blockchain matters

- The blockchain not only means the form of storing the data
- These components altogether form the blockchain
  - Decentralized (P2P) network
  - Cryptography
    - Signatures (authentication, credibility, integrity, nonrepudiation)
    - Hashing (signatures, block generation, addresses)
  - Shared ledger (distributed ledger, blockchain)
  - Consensus

The consensus

Blockchain matters

- Consensus among the nodes regarding the network state (blockchain state)
- Finally the same version of the blockchain must be stored on each node (no forks)
- Consensus mechanism is the protocol followed by the nodes in order to reach consensus regarding the network state.
  - Which nodes are permitted to add blocks to the blockchain?
  - Which node will add the next block to blockchain?
  - What to do with the forks? How to decide which version of the blockchain is valid?
- Consensus characteristics
  - Crash fault tolerance (CFT)
  - Byzantine fault tolerance (BFT)
- Consensus performance
  - Transaction processing time
  - Number of transactions per second
- Consensus style
  - Quorum: choosing a set of nodes and the chosen nodes vote / create for the next block (RAFT, PoA, PBFT)
  - Nakamoto Consensus: choosing a leader in each round and the leader creates the next block (PoW, PoS)
  - Mixed consensus

The Secret Lives of Data, RAFT, url

D. Szegő, Nordic Blockchain Association, Solidity Services, “Consortium Blockchains á la Hyperledger”

Consensus algorithms

Blockchain matters

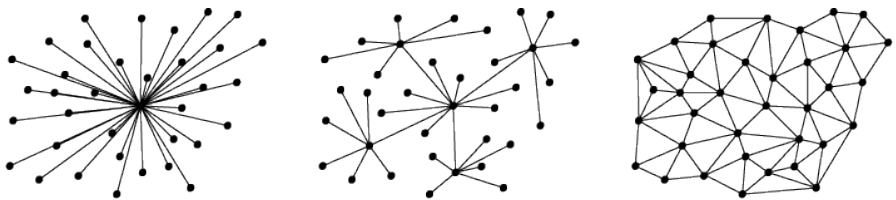
- Proof of Work (PoW) — BTC, ETH, Zcash, Monero, Dogecoin
  - The work done guarantees the security.
  - The more hash power the miner has the more mining power it has.
  - Cost: electricity
  - Only secure if there are a lot of miners, the total hash power is high, no entity owns more than 50% of the total hash power and if anybody can become a miner.
- Proof of Stake (PoS) — QTUM, ETH2, ADA, BITG
  - First mentioned in a forum in 2011.
  - The miners' own cryptocurrency holding (stake) guarantees the security.
  - The more coins the miner has the more mining power it has.
  - Cost: the cost of buying the coins
  - Only secure, if there a lot of miners, the total stake is large and no entity owns more than 50% of the total stake and if anybody can become a miner.
- Delegated Proof of Stake (dPoS) — ONT, Tezos
  - Offline staking
- Proof of History (PoH) — Solana
  - Validity check: preceding or succeeding transactions, i.e. prove that the tx occurred before and after an event
  - If it is easy to be a validator, it can be secure. If it is difficult, then it is rather a centralized solution
- Proof of Authority (PoA) — NEO, BSC, VeChain
  - Typically private networks or public networks with centralized validation (NEO)
  - Very fast

Types of blockchain

Blockchain matters

- Based on (de)centralization
  - Centralized (the ledger exists only at one node, or only one node can add new block; it doesn't make sense, a relational database would be a cheaper solution)
  - Decentralized (a copy of the ledger exists at each node)
  - Distributed (no distinguished node, each node is equal)
- Based on publicity
  - Public
  - Enterprise
    - Consortium (more distinguished participants, several consortium members)
    - Private (only one distinguished participants, or all nodes at the same company – not always make sense)
- Participation in consensus
  - Permissionless (every node can add new block)
  - Permissioned (only distinguished nodes can add new block)
- Transaction privacy
  - Public transactions
  - Private transactions (Privacy Coins – Zcash, Monero)

Wikimedia Commons, url



Bitcoin
- distributed
- public
- permissionless
- public transactions

Types of blockchain

Blockchain matters

Usual combinations

Centralization	Publicity	Participation in consensus	Transaction privacy	Example
Distributed	Public	Permissionless	Public	Bitcoin, Ethereum
Distributed	Public	Permissionless	Private	Monero, Zcash
Distributed	Public	Permissioned	Public	Ontology, Stellar
Decentralized	Consortium	Permissioned	Public	Hyperledger Fabric
Decentralized	Consortium	Permissioned	Private	Hyperledger Fabric

OK, so what is blockchain?

Blockchain matters

- **Technically**: Nothing more than a sophisticated data structure for permanent and immutable storage; data is arranged in cryptographically linked blocks.
- **Practically**: A new thinking in trustless environment with many actors, what is able to prevent fraud without any intermediaries. A software platform on the Internet with automatic contracts. However, blockchain without tokens or cryptocurrencies is only a dumb database. Blockchain is an abstraction providing mathematical solution for dealing with a lack of trust.
- **Legally**: A distributed ledger which is public in general and credibly proves the transactions (contract fulfillment, asset movement) without intermediaries thanks to the cryptographic procedures.

Why it is hard to find the place of blockchain?

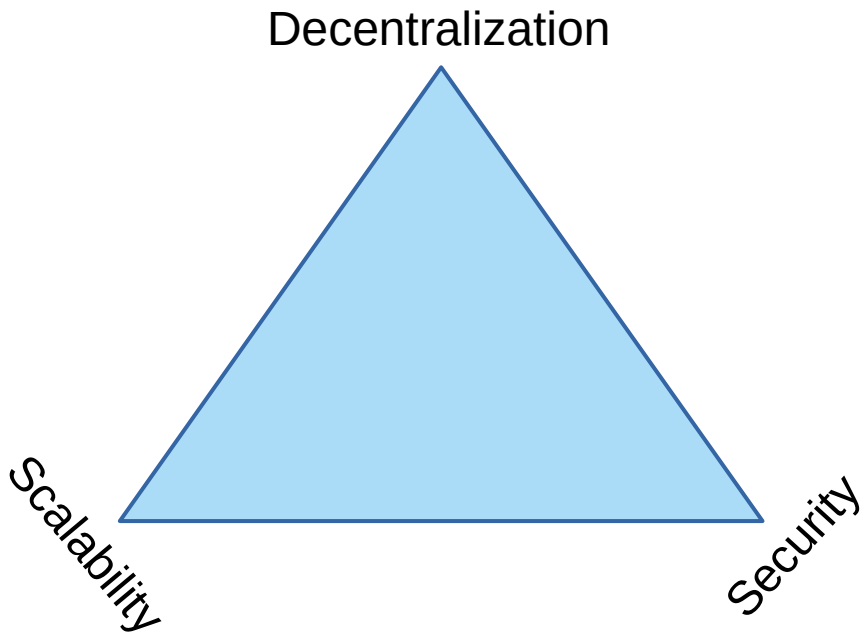
Blockchain matters

- Hard to understand what blockchain is good for
- Blockchain is multidisciplinary
  - Information theory (P2P, fault tolerance,...)
  - Mathematics (cryptography, game theory)
  - Finance
  - Economics
  - Law
- Fast evolving technology
- Few developers, few specialists
- Thousands of projects
- Several blockchain types
- Blockchain is not good for everything!
  - The wrong thinking: I have a product, how can I blockchainize it? (Find a problem for the technology/solution)
  - The good thinking: I have a problem with my product. Can blockchain help me? (Find the technology/solution for the problem)

The blockchain trilemma

Blockchain matters

- Term by Vitalik Buterin
- The trilemma: a blockchain can have two of the following three attributes: decentralization, scalability (speed) and security.
- Examples
  - Bitcoin is secure and decentralized but not scalable
  - EOS is secure and scalable but too centralized
- But there is no law stating that the three aspects cannot be achieved (e.g. Solana tries to achieve them)



EOS, url

Solana, url

CertiK, “The Blockchain Trilemma: Decentralized, Scalable, and Secure?”, 2019, url

The promise of blockchain is not true by default

Blockchain matters

- Trustless (eliminating trusted third parties and intermediaries via decentralization)
  - But not every blockchain is decentralized!
  - A certain degree of trust is required in private / consortium blockchains.
- Transparency
  - But not every blockchain is transparent!
- Non-repudiation
  - Only when blockchain platform is immutable.
- Immutability, tamper-proof
  - The blockchain is not immutable by default. Some conditions must met.
- Elimination of single point of failure
  - Only when the blockchain platform is decentralized enough.

The immutability and security of blockchain

Blockchain matters

- What do security and immutability mean?
  - 51% attack, double spending is economically inefficient.
  - Transaction history is immutable.
- Every blockchain is secure and immutable? - No.
- Immutability and security are only guaranteed when the block generation right is not in the hand of one participant or a narrow group of participants.
- To be immutable and secure
  - The 51% attack must be very expensive i.e. practically impossible.
  - Theoretically the blockchain must be **decentralized** with a **huge number of participants** (miners, validators) and with an **appropriate consensus** mechanism. (e.g. PoW – total hash rate must be high enough, PoS - total stake must be high enough)
    - Public and permissionless properties can facilitate the high number of participants.
    - Private / consortium and permissioned blockchains usually have only a few participants, however, if they use appropriate consensus mechanism they can be secure and immutable enough.
- Centralized blockchains or are neither secure nor immutable

The truth and the blockchain

Blockchain matters

- Does every blockchain contain the truth? - No
- If blockchain is immutable and secure then there is a chance to contain the truth. But it depends on the type of the data the blocks contain.
- What data is contained by the blocks?
  - If data is cryprocurrency transactions than validator nodes are able to check the correctness of the data.
  - In case of other type of data, e.g. measurement data, who will decide whether it is correct, or not?
  - Oracles may help, but validators must trust the Oracles…
- The truth can be only guaranteed if validators are able to check the truth.

Oracles

Blockchain matters

- Oracles are applications that provide data from real world to blockchain applications.
- Oracles therefore connects real world and blockchain.
- Oracles can provide real time data:
  - aviation data
  - meteorological data
  - cryptocurrency exchange rates
  - etc.

V. Mou, “Blockchain Oracles Explained”, 2020, url

The distributed ledger technology

Blockchain matters

- Blockchain is only one type of DLT (Distributed Ledger Technology)
- Blockchain
  - Bitcoin (~7 tx/s)
  - Ethereum (~30 tx/s)
  - Ontology (~4000 tx/s)
  - Solana (~50000 tx/s)
  - etc.
- Tangle
  - Iota (500-800 tx/s)
- Hashgraph
  - Hedera Hashgraph (>250000 tx/s)

Ontology, url | Solana, url | Iota, url | Hedera, url

Blockchain

matters

Coming up next: Ethereum

Blockchain matters

Thank you!

If you liked this material you can tip me

Blockchain matters

- Bitcoin: *3FvgmYScorEje3WTrdDn5synEU6j917SZz*
- Litecoin: *ltc1qs457h3899qj4yry8k6u5xva79wa8f6xspant4e*
- Ethereum: *0xdF7eAab54BC9070a140D0251247406cEe40029B7*
- QTUM: *MGo31aQ74yHJ9Lan4tgYeFy5XhtHZuoimQ*
- Tezos: *tz1VpDWz45fvqv69Laa6YVa3h6MtkCoq1BDc*

Blockchain

matters

Thank you again!