

Blockchains

Cryptocurrencies and Consortium Blockchains

Tero Keski-Valkama



2017-02-05

- Blockchain is a collection of cryptotechnologies to achieve a distributed consensus about immutable, additive data in an untrusted environment.
 - ① Blockchain is a sequence of records, or blocks, so that each block contains a hash digest of the previous block (which recursively contains the hash digest of the previous block and so on).
 - ② A consensus mechanism with rules to determine which blocks are accepted to be the next block in the blockchain. Many solutions such as proof-of-work, proof-of-stake, proof-of-burn, Practical Byzantine Fault Tolerance, and hybrids.
 - ③ A discovery and broadcast infrastructure to relay transactions and blocks to peers and miners.
 - ④ Application-specific public key or other cryptography to prove identities of parties in transactions, wallets and so on.
 - ⑤ Microcode used to define the transaction semantics or smart contracts, such as Bitcoin Script, Solidity or Chaincode.
- In blockchain, a single valid block can be used to validate the whole chain of blocks to deep history so that anyone can make sure that nothing has been altered in the stored data, by checking that the hashes of the previous block always matches the content of the previous block.
- The consensus mechanism offers guarantees that all parties have a converging view in the blockchain regarding what is valid and what is not. It prevents changing the history and that the whole blockchain integrity is guaranteed.

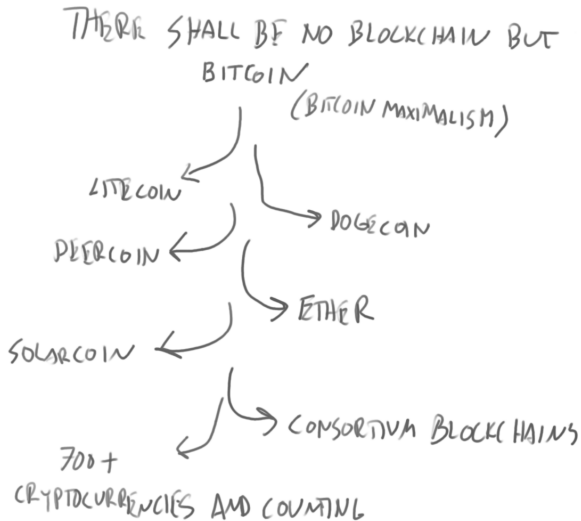


Figure: Bitcoin Maximalism vs. The Reality

Example of a Consortium Blockchain: Hyperledger Architecture



Figure: Hyperledger Architecture

| | Distributed Database | Consortium Blockchain | Cryptocurrency Blockchain |
|-------------------------------------|-----------------------------|---------------------------|--|
| Consensus mechanism | Simple parallel consistency | Byzantine Fault Tolerance | Proof-of-Work, Proof-of-Stake, Proof-of-Burn or a hybrid |
| Requires a cryptocurrency | | | X |
| Open ecosystem of untrusted peers | | | X |
| Peers validate each other's actions | | X | X |
| Access centrally managed | X | X | |

Comparison of Consensus Methods

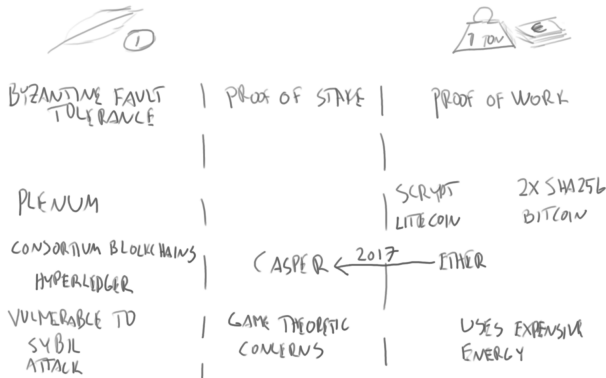


Figure: Consensus Methods

- Consensus is inherently a game theoretic concept in Byzantine systems, because the peers can try to cheat.
- In open ecosystems it must be made economically infeasible to break the rules or the goals of the system. This leads to the requirement of having a cryptocurrency built into the system. In practice, a validating peer gains cryptocurrency for processing transactions, and this cryptocurrency only has value if the whole system works.
- The Bitcoin network can process the maximum of 7 transactions per second with the current block size limit of 1 MB.
- Calculating Bitcoin mining hashes requires about 1 W of power for 1 GH/s of computation for the most energy efficient ASIC implementations.
- The current hashrate of the Bitcoin network of 3,051,683,778 GH/s translates to a power of about 3 GW.
- In standard reindeers of 200 kg, this amounts to burning 2.5 reindeers of equivalent coal every second.
- In closed consortiums, it is feasible to get rid of peers behaving incorrectly, so expensive proof-operations can be avoided.

click

- ◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡

This Much Coal Bitcoin Network Burns in 1 Hour

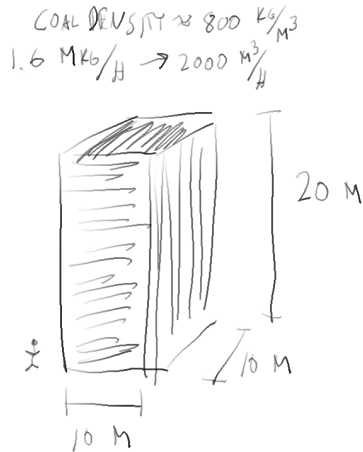


Figure: This Much Coal Bitcoin Network Burns in 1 Hour

- Proof-of-Stake is a proposed alternative to energy wasting Proof-of-Work.
Instead of proving you have done work, you prove you own a number of coins.
- Generally, for each block each coin gets a random chance of determining the next block.
- Game theoretic worries: If the miners have no stake, why would they play fair?

- Byzantine Fault Tolerance refers to a general game theoretic mathematical problem where distributed parties try to achieve consensus in spite of unreliable messaging and hostile actors.
- There are several algorithms and implementations with different characteristics.
- Practical Byzantine Fault Tolerance algorithm useful for consortium blockchains, but cannot be used for open blockchains.
- Byzantine Fault Tolerance algorithms do not generally consider an open system where new actors can join at will, and therefore they implicitly assume a kind of a Proof-of-Stake through association to the group.
- These algorithms generally need a centralized identity management to prevent a Sybil attack. Although it could be said that the centralized identity manager could freely perform a Sybil attack in these systems.

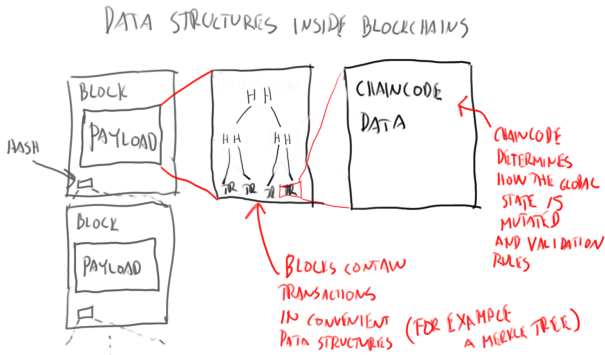


Figure: Inside Blockchain

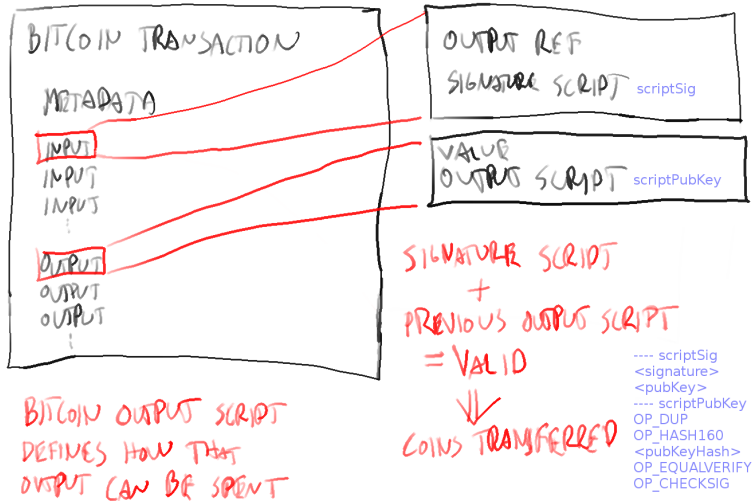


Figure: Inside Bitcoin Transactions

CONSTRAINED

BITCOIN SCRIPT

COMPLEX TRANSACTIONS

LIMITED EXECUTION TIME

TURING COMPLETE

HYPERLEDGER
CHAINCODE

ETHEREUM
SMART CONTRACTS

SOLIDITY

TRANSACTION GAS
OR

TRUST OF PARTICIPANTS
OR

WHITELISTING OF
VALID CODE PATTERNS

Figure: Chaincode Languages

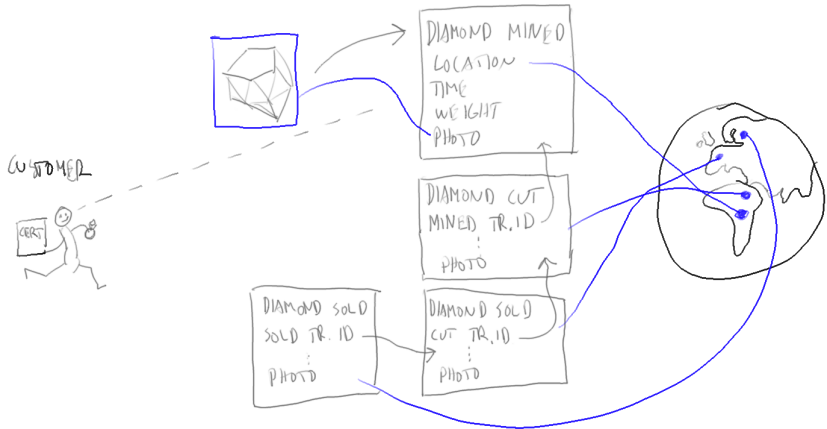


Figure: Diamond Supply Chain

- 

guardtime
a division of

UK Group 0800 30 00 00

AMSTERDAM - 020 631 00 00
 BIRMINGHAM - 0121 631 00 00
 BRISTOL - 01454 30 00 00
 CARDIFF - 01493 30 00 00
 DUBLIN - 01 454 30 00 00
 EDINBURGH - 0131 631 00 00

MARK

Friday July 17 2003

S&P 500 index



UK equities that invest abroad for exposure to the UK market about the previous column.

UK equities that invest abroad for exposure to the UK market about the previous column.

FTSE 100 index



UK equities that invest abroad for exposure to the UK market about the previous column.

UK equities that invest abroad for exposure to the UK market about the previous column.

- Princeton course book: Bitcoin and Cryptocurrency Technologies
- Guardtime KSI