INDUSTRY
CONNECT
Connect to your Future

Chapter 3 - Miner & Consensus

Learn Blockchain Technologies

Blockchain Mining

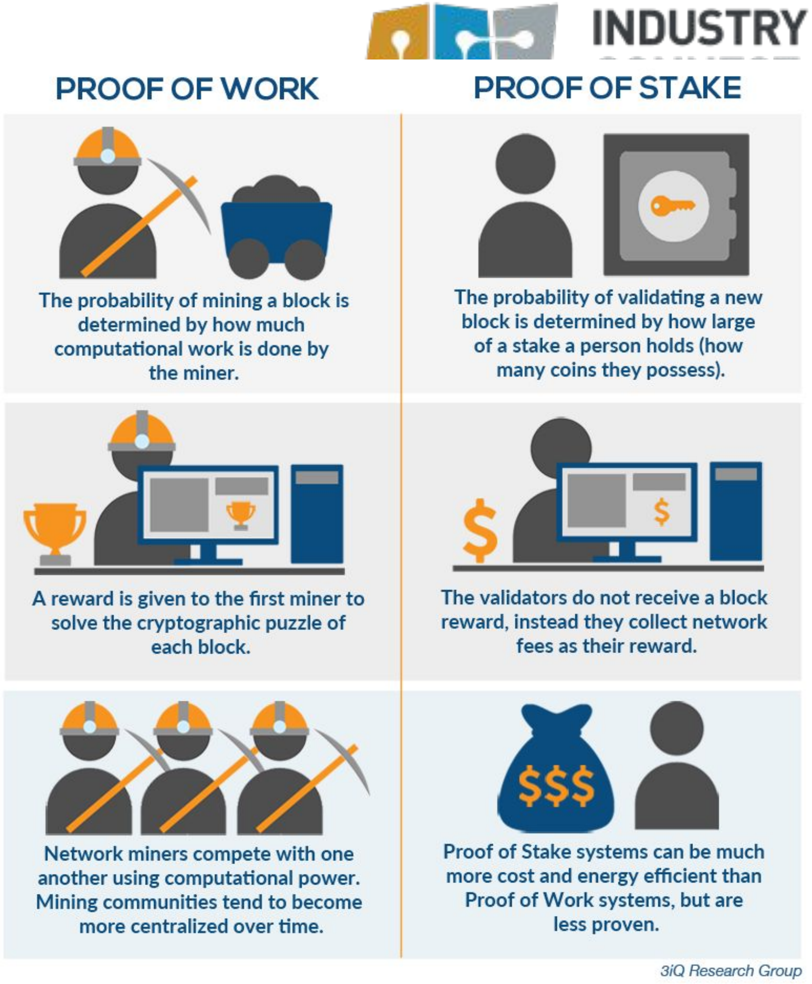
- The blockchain network requires nodes (computers) to maintain the entire decentralized system.
- The node is the miner as it makes money by doing certain work.
  - E.g. Bitcoin node software running in the computer is to add blocks to the chain by doing certain tasks.
  - The task is to find the nonce (string) of producing the expected hash value of the transactions.
  - The task is also called the process to form a consensus
- The more people run the nodes, the more decentralized the blockchain is.
  - E.g. you burn 1000 nodes, there are still 99999999 nodes out there holding the identical information.
- Now there is node running in the space!
  - That means even when earth had catastrophic event, it is a good chance your money is still there. https://medium.com/orbs-network/qtum-and-spacechains-satellites-os-bring-nodes-to-space-and-decentralization-to-nanosats-7a751d2b25d

Popular Consensus Algorithms

- Proof-of-Work aka PoW used by Bitcoin, Ethereum
  - Miner verifies the transactions and place them into a block.
  - Miner finds the right nonce(string) to produce the hash of the block with expected pattern.
  - Miners who find the nonce will be rewarded with the coins just mined.
- Proof-of-Stake aka PoS used by DASH, NEO
  - The more cryptos the node stakes, the more power it has for proving the transactions
  - The node who holds more token would never want to hack the system. So Truth is incentivized.
- Delegated Proof-of-Stake aka DPoS used by EOS, BitShares
  - In DPoS the community selects a number of **witnesses** or **block producers** to secure the cryptocurrency network. Witnesses sign each block in the blockchain, however, the users of the network must first approve the witnesses via a voting system.

Proof of Work vs Proof of Stake

- **PoW relies on computation power**
  - Consume lots of electricity
  - More proven to work well
  - Getting more centralized
  - Miner gets the coin reward
  - Hackers needs to own 51% of computation Power to hack the system.
- **PoS relies on staking a lot of coins (money)**
  - Energy efficient
  - Environment friendly
  - Less proven
  - Miner gets the reward from transaction fees.
  - Hackers need to own 51% of platform coins to Hack the system.
    (If you own 51% if the tokens, why you want to Screw up your own money!)



PROOF OF WORK

PROOF OF STAKE

The probability of mining a block is determined by how much computational work is done by the miner.

The probability of validating a new block is determined by how large of a stake a person holds (how many coins they possess).

A reward is given to the first miner to solve the cryptographic puzzle of each block.

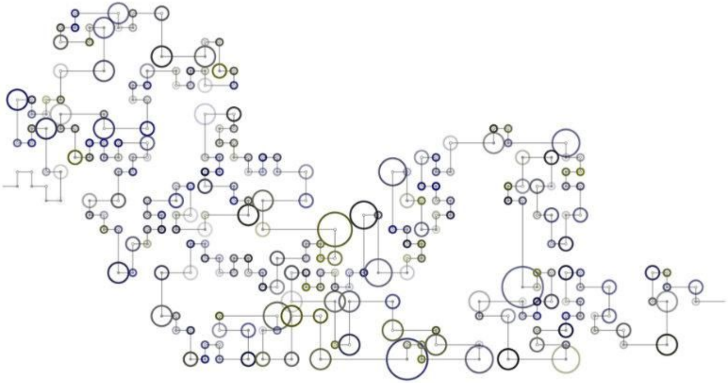
The validators do not receive a block reward, instead they collect network fees as their reward.

Network miners compete with one another using computational power. Mining communities tend to become more centralized over time.

Proof of Stake systems can be much more cost and energy efficient than Proof of Work systems, but are less proven.

3iQ Research Group

Other Consensus Algorithms



- Proof of Authority - PoA
  - Miners’s identities are verified as authority.
- Proof of Weight - PoWeight
  - Like PoS, it uses other weighted value such as Proof of Reputation.

Research on the others like

- Byzantine Fault Tolerance - BFT
- Directed Acyclic Graphs - DAGs
- Proof of Elapsed Time - PoET

Research

Find out how Bitcoin blockchain mining work.

https://bitcoin.org/en/ bitcoin