FACULTY OF AUTOMATIC CONTROL AND COMPUTERS

POLITEHNICA BUCUREȘTI 1818

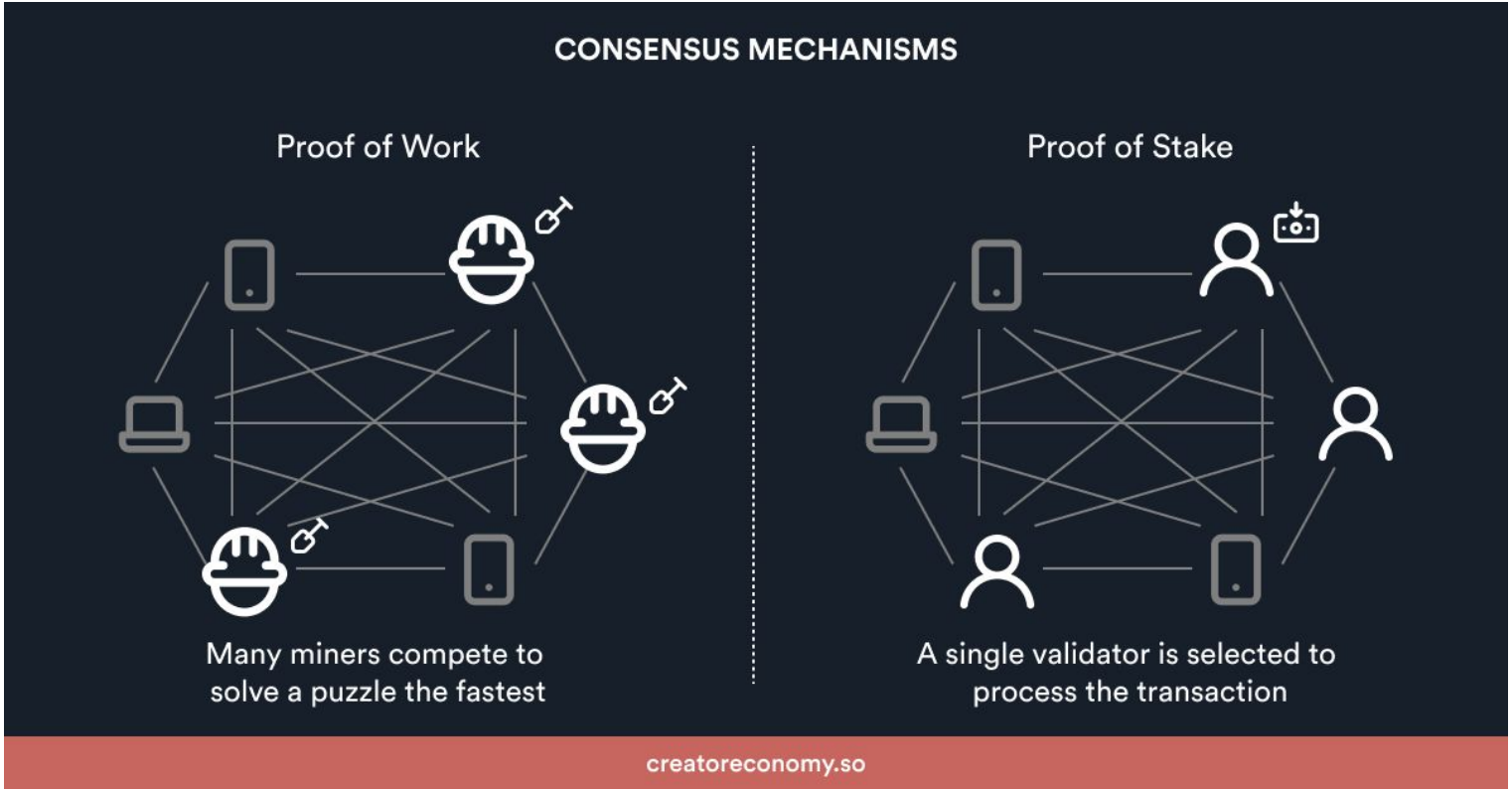
Sessions 04
Proof of Stake

Blockchain Protocols and Decentralized Applications

Proof of Work

- Nodes called miners compete to solve a math problem using brute force
- The first miner that solves the problem gets to create a block
- Other nodes check if the block is valid
  - If yes, the miner is rewarded cryptocurrency
  - If no, the miner wasted their time and energy
- All nodes add the new block to their copy of the blockchain
- Issues?

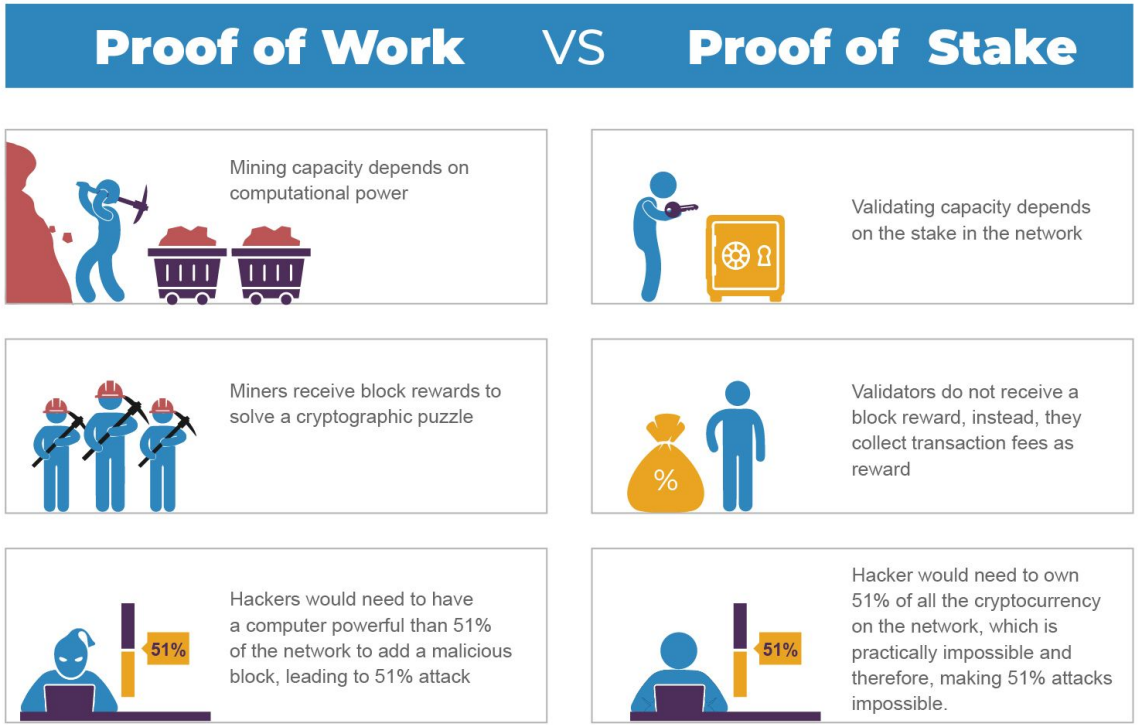
Proof of Work vs Proof of Stake



Proof of Stake

- Nodes called validators stake some cryptocurrency
  - A stake is like saying: “I’ll commit this amount of cryptocurrency to win the right to do this transaction.”
- Validators with more stake are more likely (but not guaranteed) to be selected to process the transaction and create a block
- Other validators check if the block is valid. If it is, all participating validators earn a transaction fee. If it’s not, the validator that created the block might lose its stake
- All nodes add the new block to their copy of the blockchain

Proof of Work vs Proof of Stake



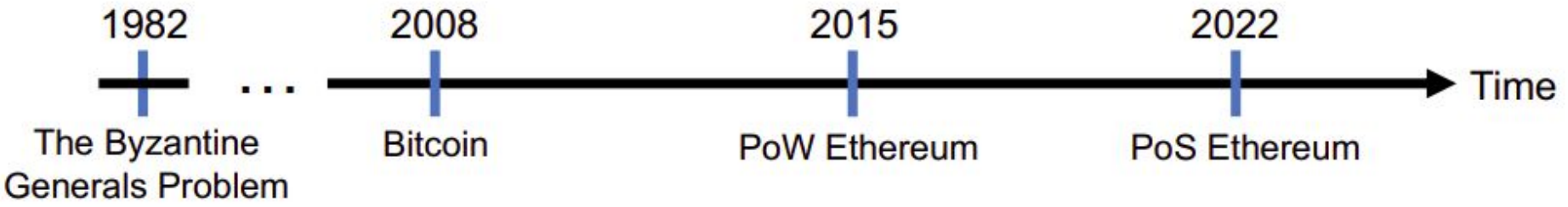
Source: https://www.leewayhertz.com/proof-of-work-vs-proof-of-stake/

Proof of Work vs Proof of Stake

Participating nodes are called miners	Participating nodes are called validators
Mining capacity depends on computational power	Validating capacity depends on the stake in the network
Mining produces new coins	No new coins are formed
Miners receive block rewards	Validators receive transaction fees
Massive energy consumption	Low energy consumption
Significantly prone to 51% attacks	51% attacks are virtually impossible

Proof of Stake

- Demo - Explorer
  - https://explorer.multiversx.com/
  - https://etherscan.io/
- Timeline



Transactions

- PoW, PoS gives us ..?
  - Agreement
- Bitcoin
  - Miners come to agreement to move tokens from one user to another
- Ethereum
  - Validators comes to agreement to execute a piece of code

Smart contracts

- Two types of accounts
  - Users
  - Externally Owned Accounts (Smart Contracts)
- EoA contain code
- Demo