PoW vs PoS

High-level Comparison

Kostas Karasavvas

@kkarasavvas

Agenda

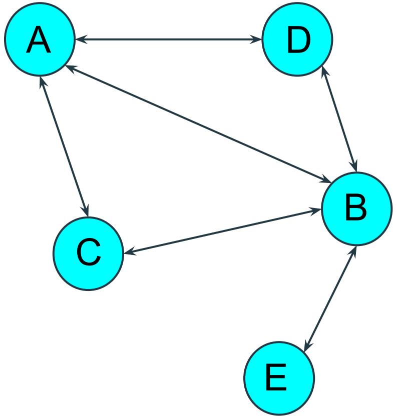
- Basic concepts
- Barriers to Entry
- Network Security
- Network Decentralization
- Resistance to Attacks
- Environment
- Summary

Agenda

- Basic concepts
- Barriers to Entry
- Network Security
- Network Decentralization
- Resistance to Attacks
- Environment
- Summary

Not Bitcoin vs Ethereum

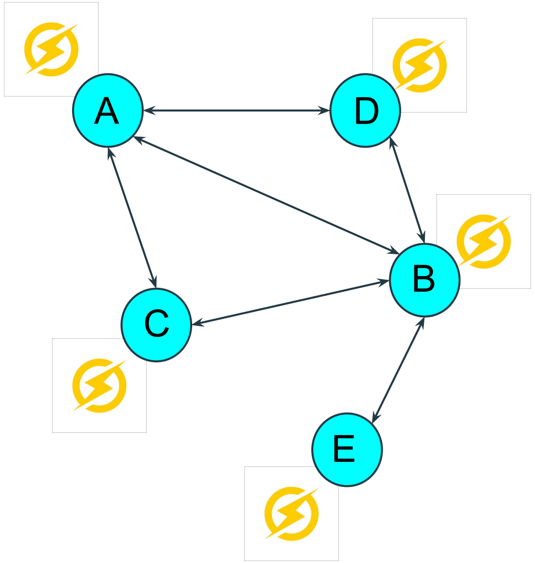
Introduction



- Consensus
  - the mechanism that nodes use to determine the *true* state
  - examples: Nakamoto Consensus (Chain-based), PBFT
- Sybil resistance
  - the mechanism that associates some cost to producing blocks
  - examples: PoW, PoS
- Block producer selection
  - the mechanism that determines who the next block producer is
  - examples: PoW, PoS

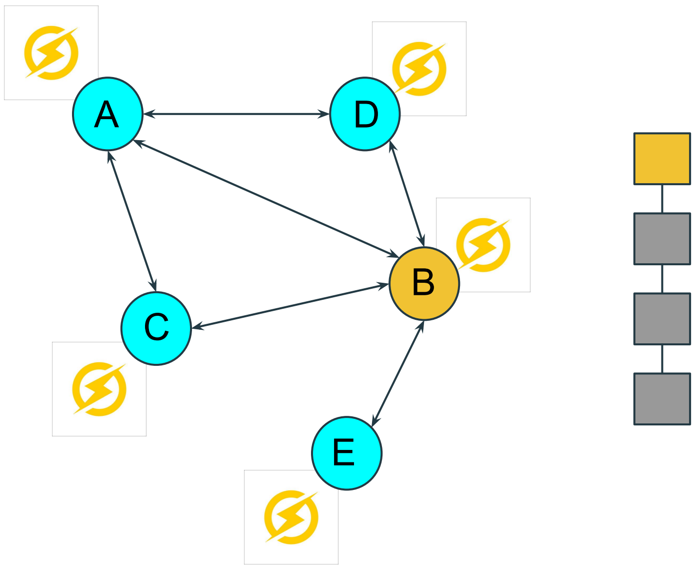
PoW

PoS

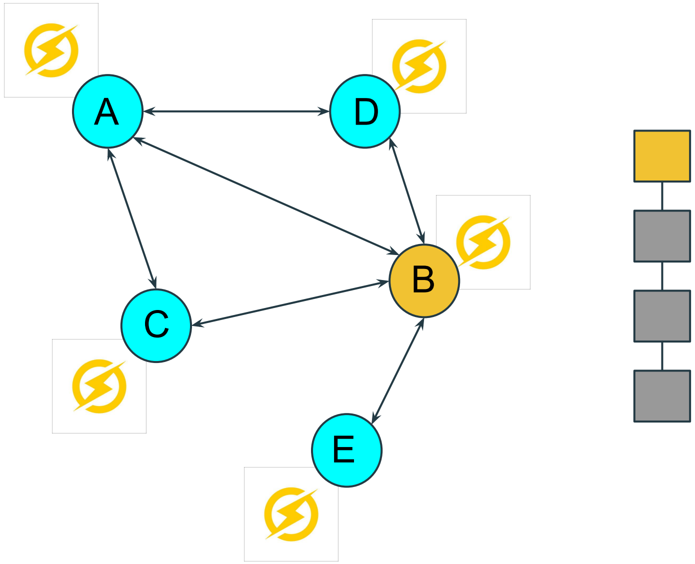


PoW

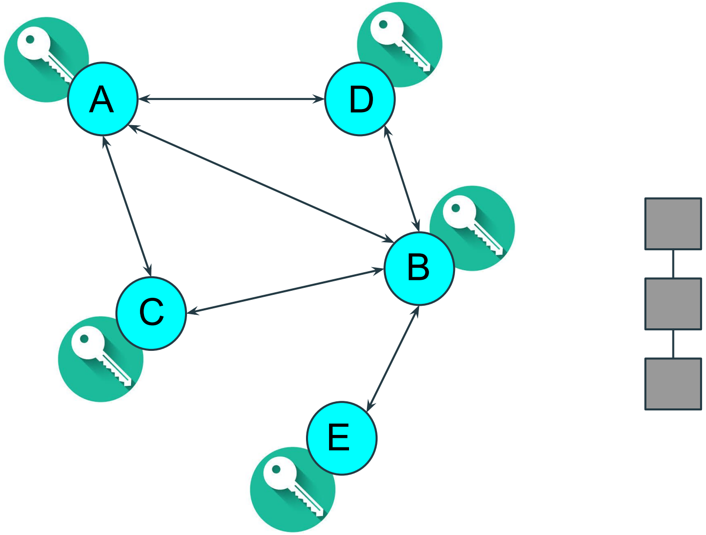
PoS



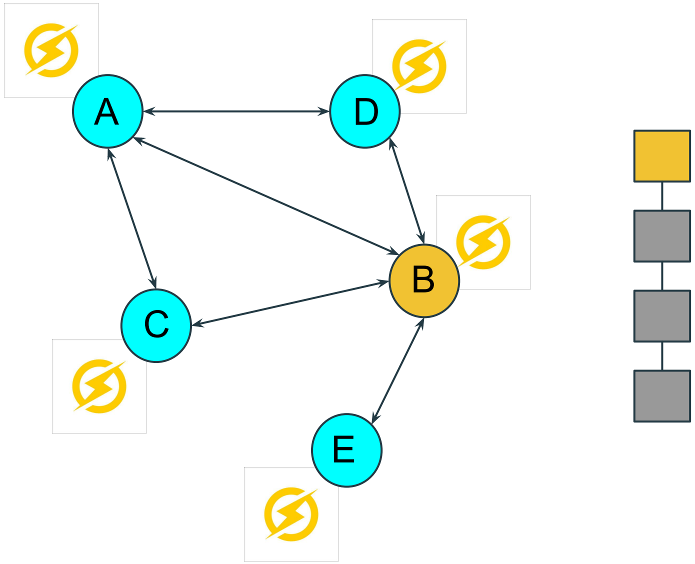
PoW



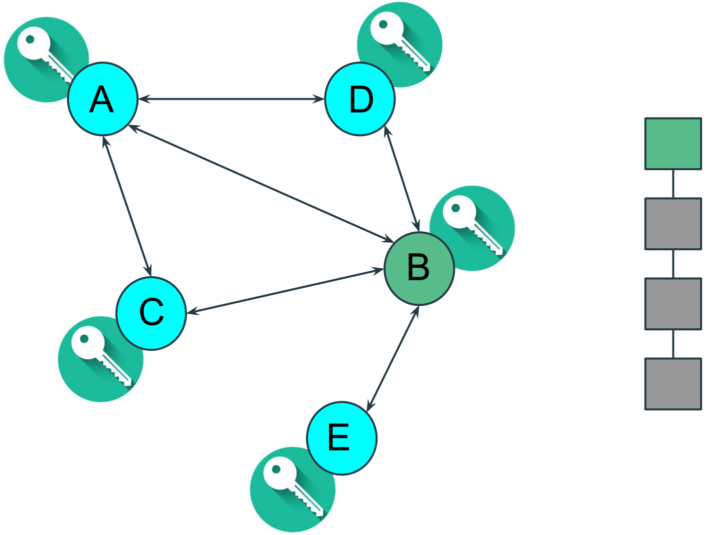
PoS



PoW



PoS



Barriers to Entry (1/2)

- Mining hardware
  - exogenous
  - energy (unforgeable)

- Buying mining rigs (GPUs/ASICs)
  - no permission is required
  - partial censorship possible

- Mining rig decay
  - profits constantly decrease
  - need to sell coins to cover costs and update their hardware
  - coin distribution is increased
  - newcomers buy new/better rigs

Barriers to Entry (1/2)

- Mining hardware
  - exogenous
  - energy (unforgeable)
- Buying mining rigs (GPUs/ASICs)
  - no permission is required
  - partial censorship possible
- Mining rig decay
  - profits constantly decrease
  - need to sell coins to cover costs and update their hardware
  - coin distribution is increased
  - newcomers buy new/better rigs

- Coins
  - endogenous
  - capital (software)
- Buying coins
  - indirect permission is required
  - full censorship possible
- Stake/Coins never decay
  - perfect ASICs
  - stakers can maintain advantage forever
- Is there a way for majority stakers to lose control of their stake?

Barriers to Entry (2/2)

- Can a user really mine?
  - very competitive
  - requires initial hardware investment

- Miners
  - companies will invest
  - only a handful of users will mine

- Easier for professionals with large farms
  - 3 top mining pools have 50%+ hashrate
  - misconception: mining pools control the hashrate

Barriers to Entry (2/2)

- Can a user really mine?
  - very competitive
  - requires initial hardware investment

- Miners
  - companies will invest
  - only a handful of users will mine

- Easier for professionals with large farms
  - 3 top mining pools have 50%+ hashrate
  - misconception: mining pools control the hashrate

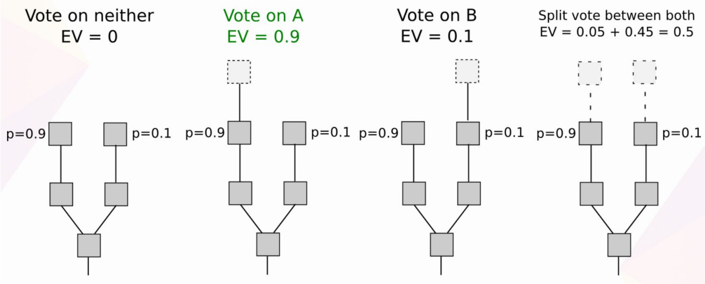
- Can a user really stake?
  - yes, easy and profitable
  - initial investment are the actual coins

- Stakers
  - both companies and users will stake
  - fair distribution %-wise

- Any user can stake even small amounts
  - it is easy because stake is delegated
  - delegation centralizes considerably
  - user can redelegate elsewhere
    - not always possible!

Network Security

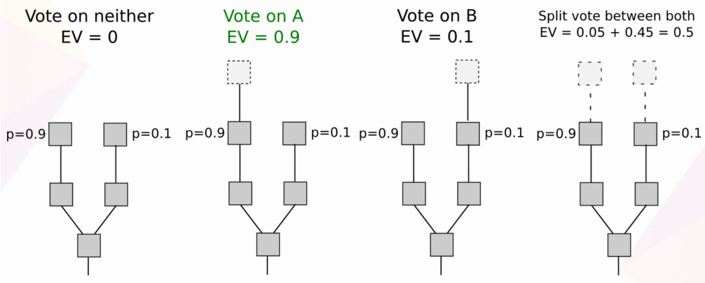
- Objective History
    - given multiple chains the *true* chain (history) can be determined objectively
    - most accumulated PoW chain; PoW requires computation and is thus thermodynamic
    - incentive to choose a chain



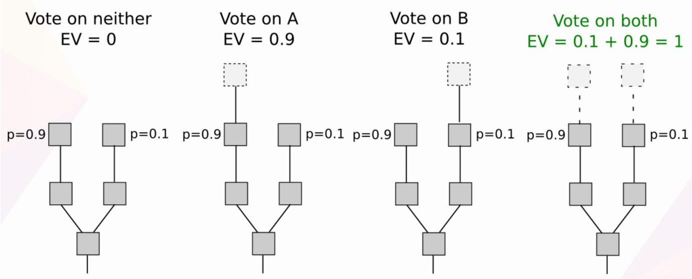
Diagrams from Vitalik's Weak Subjectivity blog post

Network Security

- Objective History
  - given multiple chains the *true* chain (history) can be determined objectively
  - most accumulated PoW chain; PoW requires computation and is thus thermodynamic
  - incentive to choose a chain



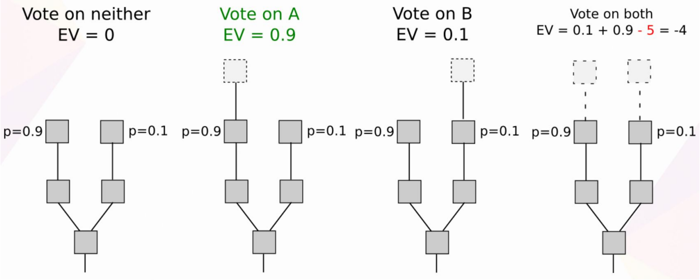
- Subjective History
  - given multiple chains the *true* chain (history) is subjective
  - trivial to sign a block so anyone can present multiple chains trivially
  - there is an incentive to sign in more than one chains; nothing-at-stake / costless simulation



Diagrams from Vitalik's Weak Subjectivity blog post

Network Security (Solving Subjectivity)

- Short-range attacks
  - can be avoided by locking the deposit staked for a certain amount of blocks *N*
  - if signatures are detected for multiple chains then part of the deposit is slashed
  - validators are incentivised to be honest



Diagrams from Vitalik's Weak Subjectivity blog post

Network Security (Solving Subjectivity)

- Long-range attacks
  - how long can *N* (for locking) be?
  - what if we introduce checkpoints?
  - a state *M* blocks ago is considered final
  - as long as *N* >= *M* we are safe
  - but how do new nodes (or nodes offline for more than *M* blocks) know of the checkpoints?
    - ask a trusted entity

Network Security (summing up)

- Objective History
  - given multiple chains the *true* chain (history) can be determined objectively
  - most accumulated PoW chain
  - PoW requires computation and is thus thermodynamic
- Complexity?

- Weakly Subjective History
- Short-range attacks
  - deposit+slashing
  - protected for *N* blocks
- Long-range attacks
  - checkpointing
  - online nodes are secured as above
  - new nodes or offline nodes (>*N* blocks)
    - ask a trusted entity for the last checkpoint
- Complexity?

Network Decentralization

- Incentivizes geographical distribution of mining power
  - cheap remote electricity
  - wasted electricity

- Coins are more distributed
  - miners have to sell to stay competitive

- What if governments
  - seize a lot of rigs?
  - buy a lot of rigs?
  - covertly use rigs of manufacturers?

Network Decentralization

- Incentivizes geographical distribution of mining power
  - cheap remote electricity
  - wasted electricity
- Coins are more distributed
  - miners have to sell to stay competitive
- What if governments
  - seize a lot of rigs?
  - buy a lot of rigs?
  - covertly use rigs of manufacturers?

- Coins are easier to centralize
- The majority of coins are created on network launch
  - concentration of wealth
- What if governments
  - seize a lot of coins?
  - buy a lot of coins?
  - covertly use coins of exchanges?

Resistance to Attacks

- fault-tolerance
  - 50%
  - neutral/arbitrary block producer selection
- 51% attacks
  - hard to accumulate mining rigs in secret
  - time will render rigs useless
- bribery attacks
  - difficult / resources are wasted

- fault-tolerance
  - 50% with chain-based consensus
  - 33% with BFT-like consensus
  - a-priori knowledge of block producer node
- 51% attacks (and 34%)
  - easy to accumulate coins in secret
  - time is irrelevant
  - stake to retain advantage
- bribery attacks
  - nothing-at-stake, using old keys
  - slashing is a solution to this
  - N/A to BFT-like consensus

Resistance to Attacks

- Sybil attacks
  - requires computation / energy / capital
- other attacks
  - selfish mining, censorship, eclipse attacks
- Application incentive attacks
  - N/A

- Sybil attacks
  - requires coins / capital
- other attacks
  - liveness denial, censorship, eclipse attacks, grinding attack
- Application incentive attacks
  - DeFi introduces a lot of incentives
    - what if lending % is higher than staking?
    - risk of reduced security?
  - Liquid staking to the rescue
  - what about the security implications of an 'intermediate' ?

Environment

- Requires significant energy
  - the more energy the more security

- But… but…
  - uses energy that would be wasted
  - uses cheap energy around the world
  - gold uses much more energy
  - banking sector uses even more energy
  - …

Environment

- Requires significant energy
    - the more energy the more security
- But… but…
    - uses energy that would be wasted
    - uses cheap energy around the world
    - gold uses much more energy
    - banking sector uses even more energy
    - …

- Requires minimal energy
    - energy is irrelevant to security

Summary

- more secure
  - objectivity / less susceptible to some attacks
  - requires both capital and labor to attack

- more decentralized
  - miners are geographically distributed
  - less susceptible to covert control

- more profitable
  - anyone can stake profitably

- more scalable
  - PBFT-like PoS

- more environmentally friendly

Thank You

@kkarasavvas

Thessaloniki's Bitcoin and Blockchain Tech Meetup

https://www.meetup.com/BlockchainGreece-1/
@Thess_Bitcoin

Python Bitcoin Library (FOSS)

https://github.com/karask/python-bitcoin-utils

Bitcoin Programming Book (CC)

https://github.com/karask/bitcoin-textbook