Comparison of PoW- and PoS-driven blockchains

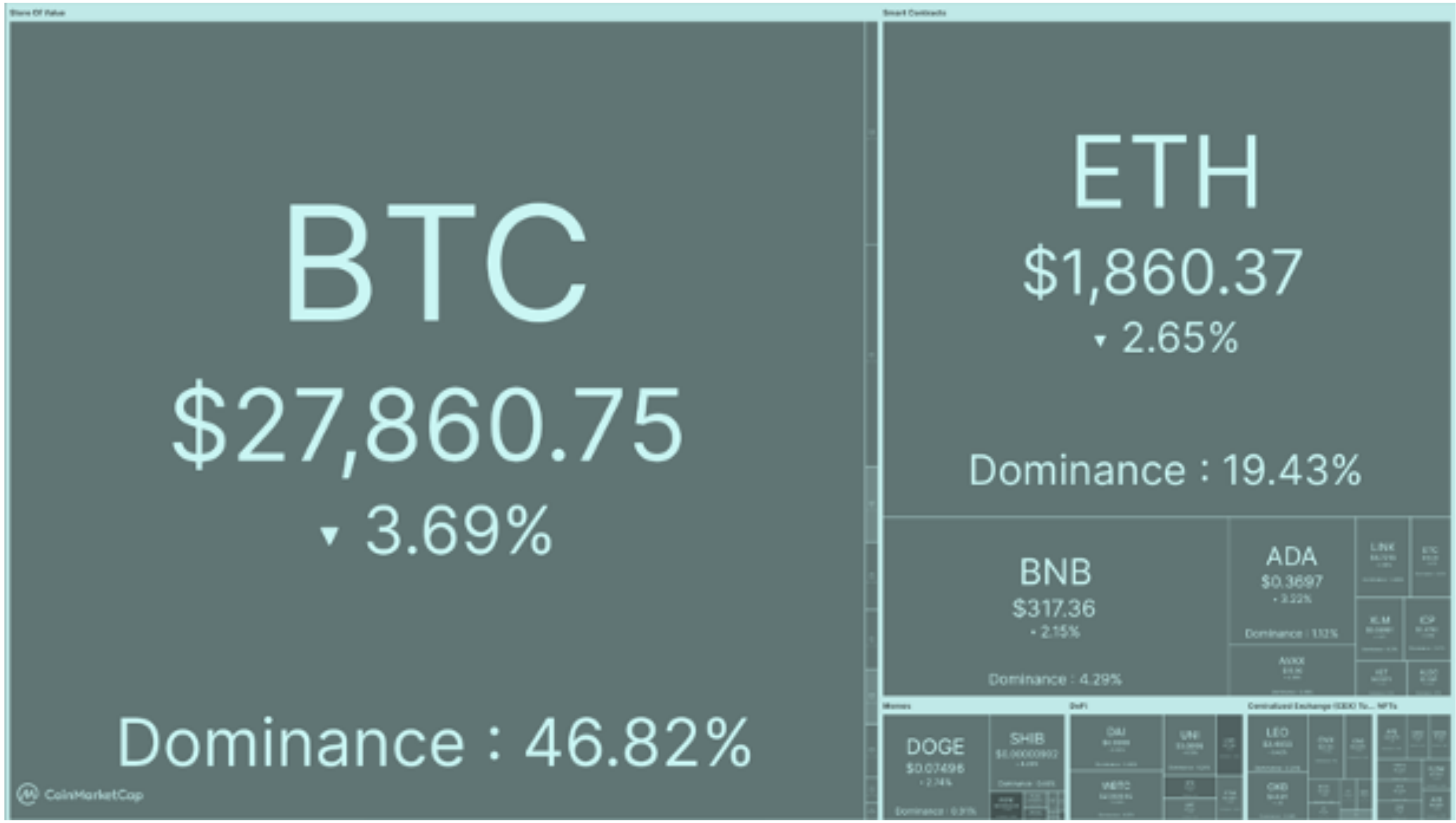
Ivan Malakhov

Background

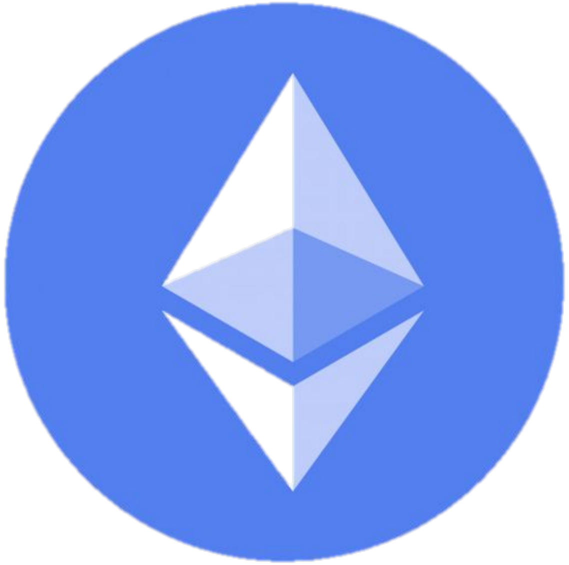
First implementations:

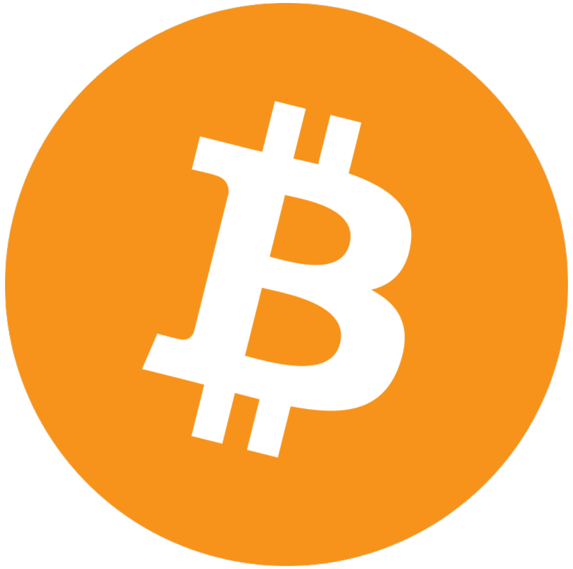
- PoS
  - Peercoin (2012)
- PoW
  - Bitcoin (2008)

Market Caps of blockchains



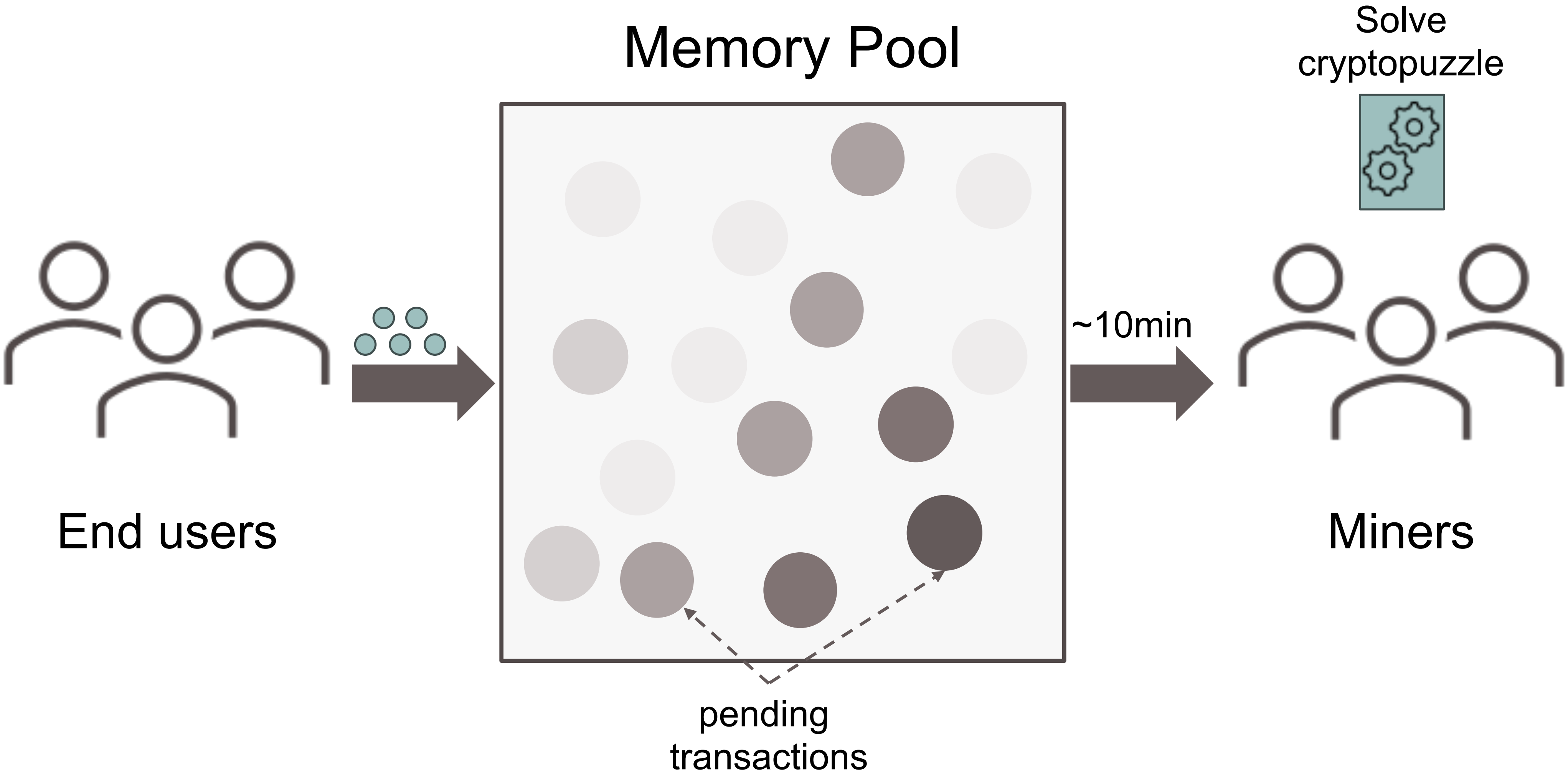
Chosen blockchains





In September, 2022 Ethereum moved from Proof-of-Work to Proof-of-Stake consensus mechanism (Paris upgrade)

PoW blockchain


Memory Pool

Solve cryptopuzzle

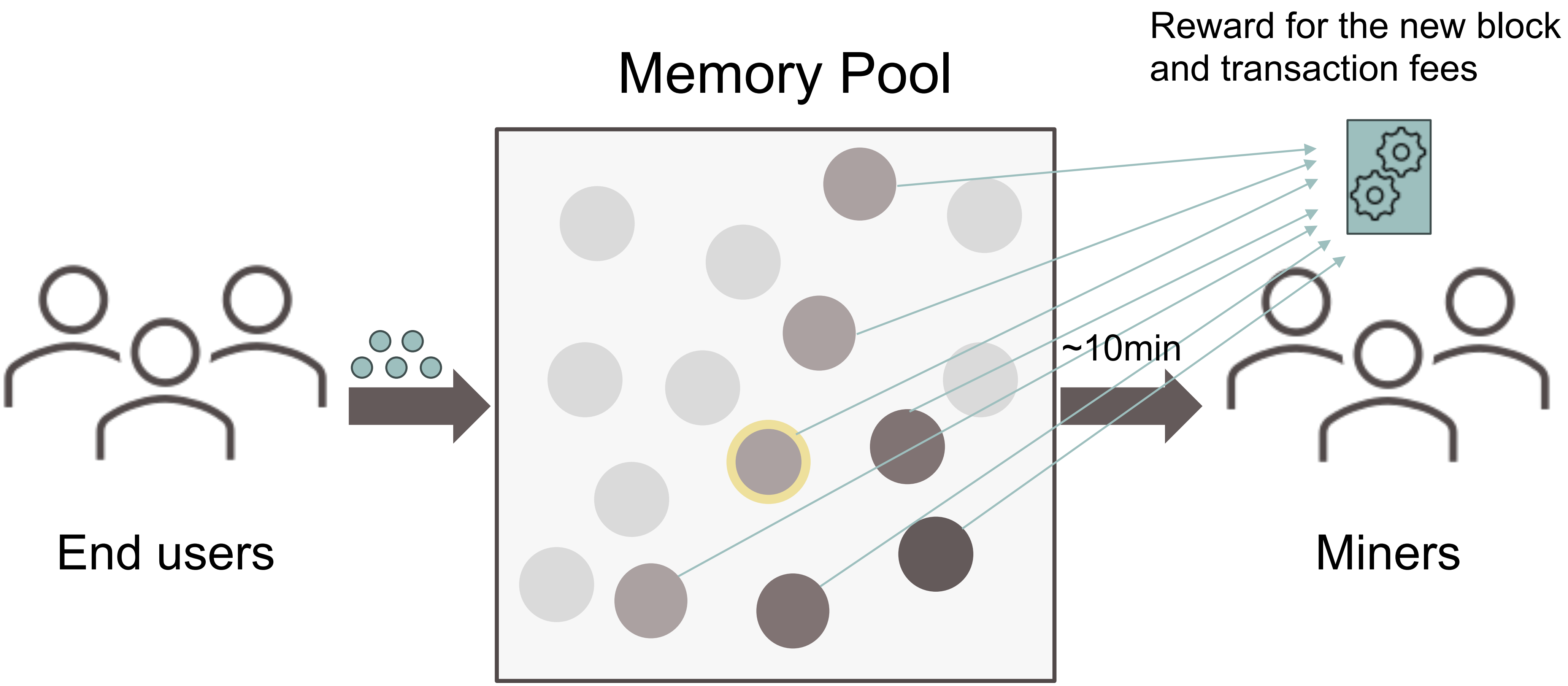
~10min

End users

Miners

pending transactions

PoW blockchain



Memory Pool

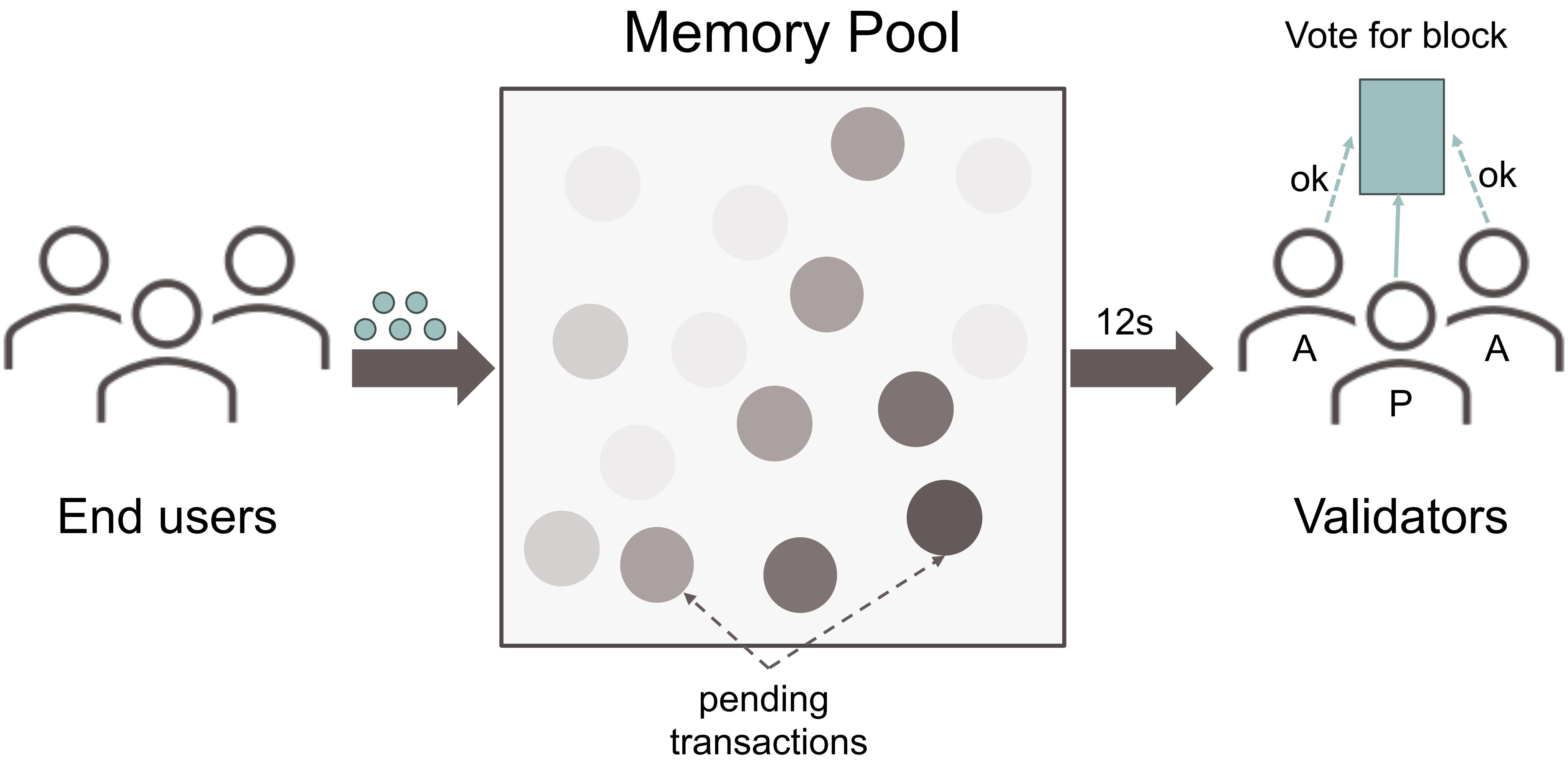
Reward for the new block
and transaction fees

~10min

End users

Miners

PoS blockchain



Comparison

PoW (Bitcoin)	PoS (Ethereum)
• Miners	• Validators
• Auction-based service	• Random committees
• Solving crypto puzzle	• Voting (*attestation*)
• Computationally heavy	• Not at all
• No miner entrance fee	• Deposit as a *stake* for validator
• Financial transactions only*	• Financial and SC transactions
• No penalty	• Complex reward/penalty system
• Longest chain fork choice rule	• GHOST fork choice rule
• Block mean time 10min	• Block time 12s
• 2 epoch finality	• Probabilistic finality after 6 blocks

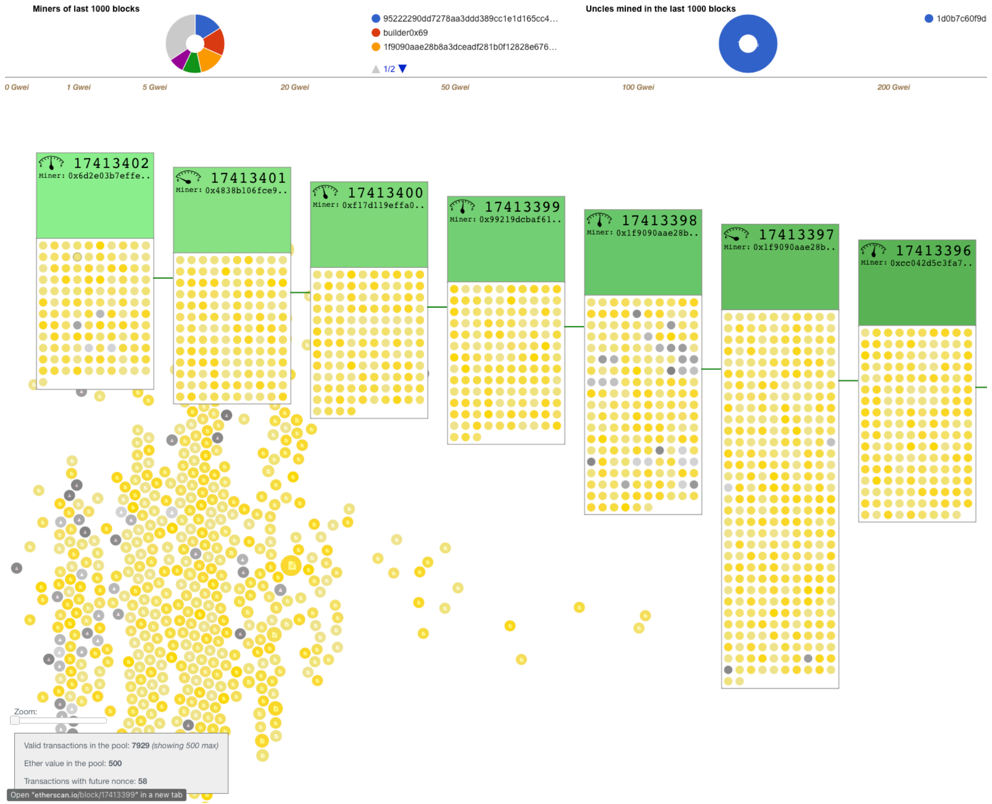
Blockchain market

- PoS (Ethereum)
  - Flexible block size
  - Flexible ETH supply
- PoW (Bitcoin)
  - Fixed block size
  - Maximum market capitalization

Ethereum’s PoS

- Based on Gasper protocol that is
  - Casper FFG

    +
  - GHOST



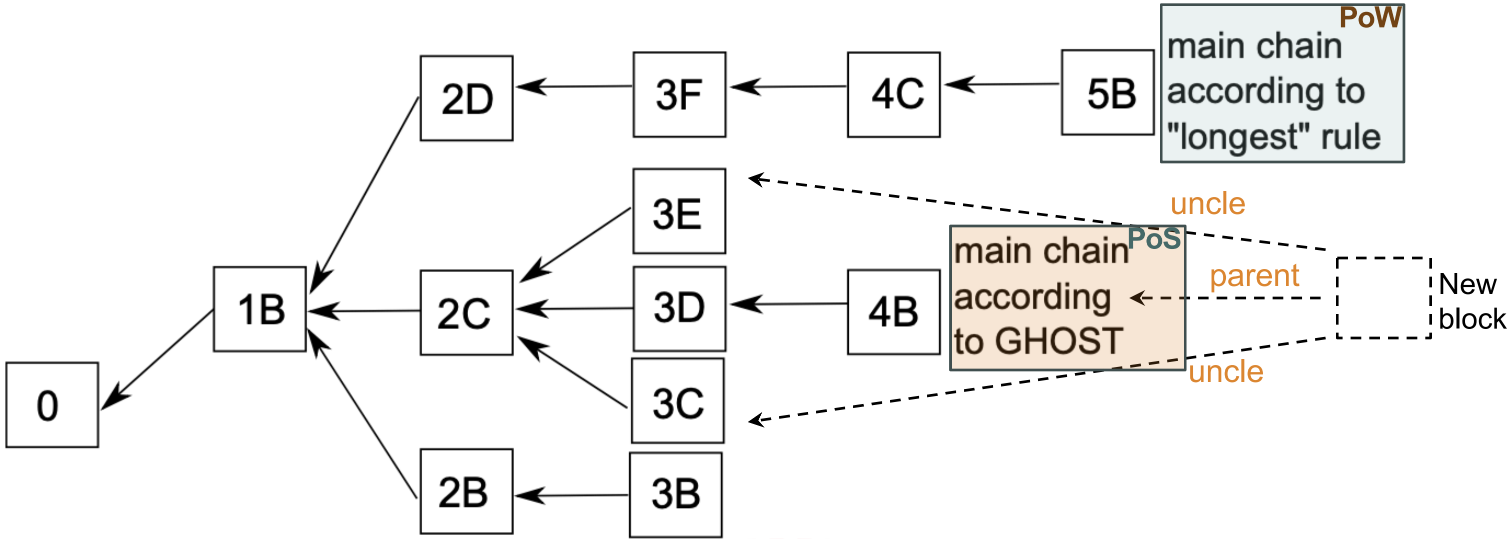
Valid transactions in the pool: **7929** *(showing 500 max)*

Ether value in the pool: **500**

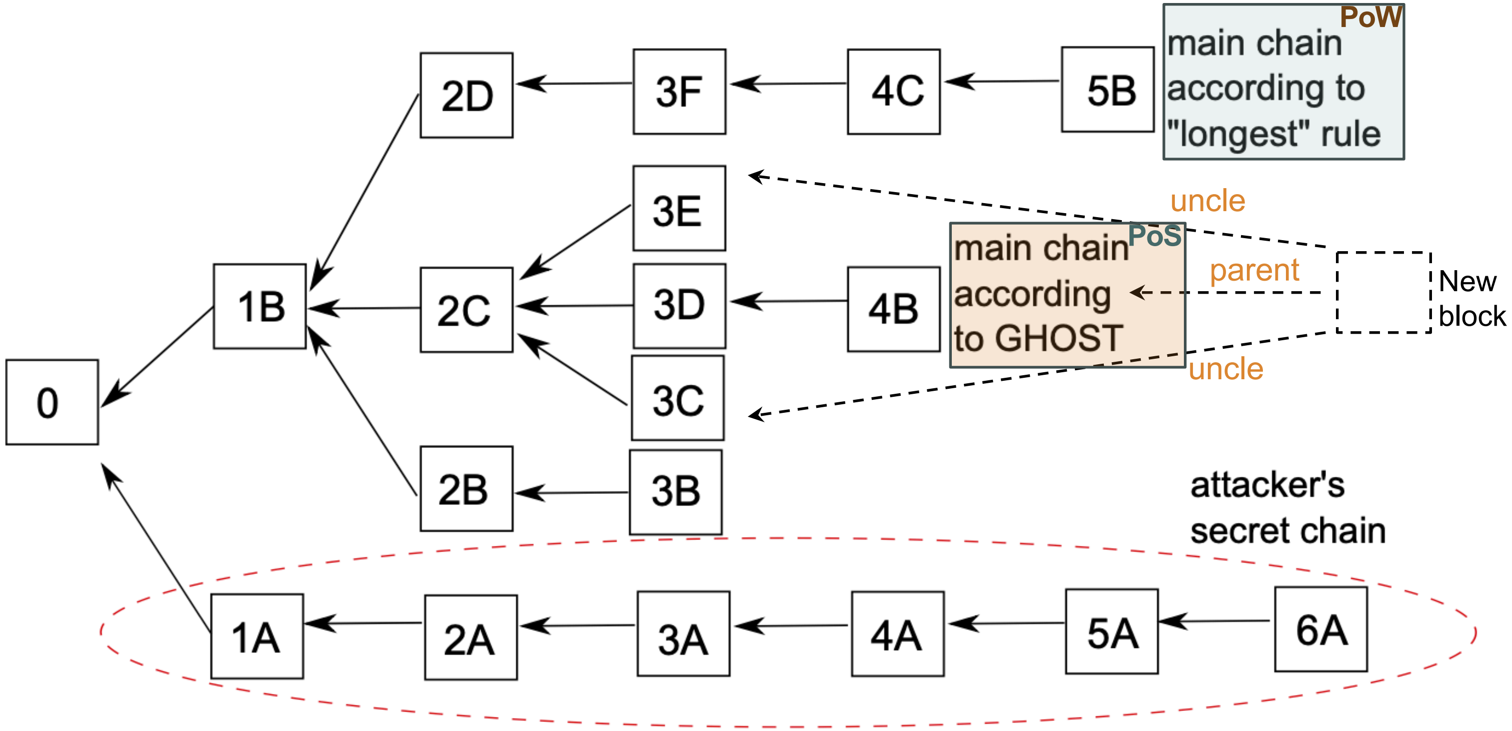
Transactions with future nonce: **58**

Open "etherscan.io/block/17413399" in a new tab

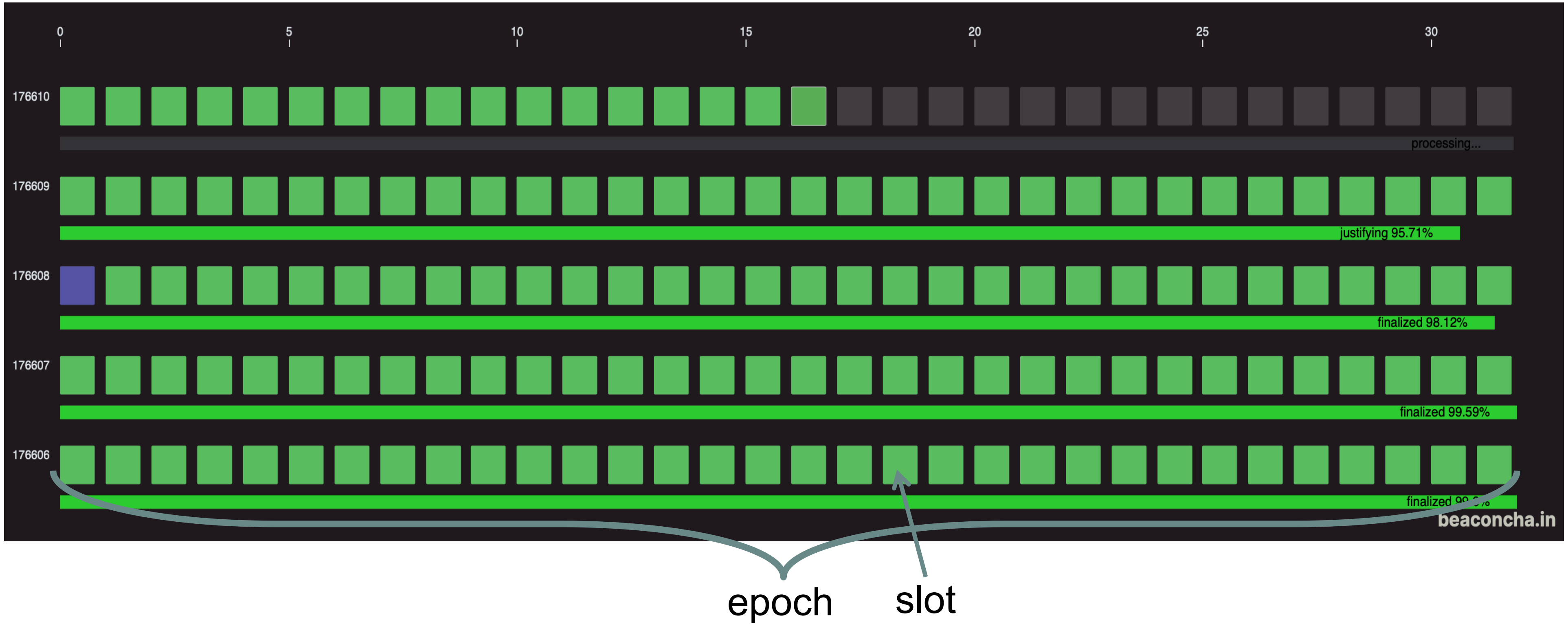
Fork choice mechanisms


PoW
main chain according to "longest" rule
2D
3F
4C
5B
3E
uncle
PoS
main chain according to GHOST
parent
New block
1B
2C
3D
4B
0
3C
uncle
2B
3B

Fork choice mechanisms



Finalization



176610 processing...

176609 justifying 95.71%

176608 finalized 98.12%

176607 finalized 99.59%

176606 finalized 99.[illegible]%

1 epoch = 32 slots ≈ 6.4 min
1 slot = 12 sec

Bitcoin PoW: 6 blocks
“finalization”

Blockchain extension

PoS

Validator:

- Deposit 32 ETH using a special smart contract
- Be constantly involved in blockchain extension process
- Be rewarded for following the protocol
- Be punished, otherwise

PoW

Miner:

- Have no entrance condition
- Can stop unconditionally
- Be rewarded for new mint blocks
- No punishment system

Validation process

- For each slot in an epoch the committee is pseudo randomly* formed
- Committee size should be at least 128 members
- Committee member can be only in *one* committee
- All committees are disjoint

* BLS signature is used with public key of current block proposer

Reward system

PoS (Ethereum)

- Distinguish 3 types:
  - For voting
  - For block proposal (+tx fee)
  - For signing off on block in the sync committee*

n ETH stake implies *nb* expected reward per epoch, where *b* – base reward per increment

84.4% of all rewards are from attestation

PoW (Bitcoin)

- Distinguish:
  - For block proposal[1] (+tx fee)

[1] – Stanard block reward is deminished gradually until Bitcoin reaches 21M BTC

Reward distribution in Ethereum

Reward type	Percentage
Timely head	21.9%
Timely source	21.9%
Timely target	40.6%
Sync reward	3.1%
Block proposal	12.5%

Attestation reward

Validators' penalty (Ethereum)

Validator penalized:

- By missing attestation
- Being late
- Incorrect
- Others*

Validator slashed:

- By multiple attestations
- By multiple blocks

Break-even uptime is 42.5%

* e.g. *Inactivity leak, slashing (for misbehaviour)*

Known attacks

PoS

- Reorg attack
- Bouncing attack
- Avalanche attack

PoW

- 50% attack
- Selfish miner attack

Conclusion

- Compare PoW- and PoS-driven blockchains on example of Bitcoin and Ethereum networks