DYOR when FOMO or FUD*

Bulat Nasrulin
b.nasrulin@tudelft.nl
Delft University of Technology

*Do your own research when fear of missing out or fear, uncertainty and doubt

Wonderful World of Web3

- Information overload
- Information asymmetry
- Highly dynamic
- Innovation (good and bad) done by amateurs

Challenge: Analyze and Navigate in Blockchain Technology

Blockchain as a Socio–Technical System

Social System:

- Developers
- Clients
- Validators
- Token holders

Technical system (Distributed system):

- Database
- P2P Network
- Consensus
- Security

Blockchain as a Socio–Technical System

Social System:

- Developers
- Clients
- Validators
- Token holders

Technical system (Distributed system):

- Database
- P2P Network
- Consensus
- Security

Useful Metrics and Properties

Incentive alignment

Game theoretical equilibrium

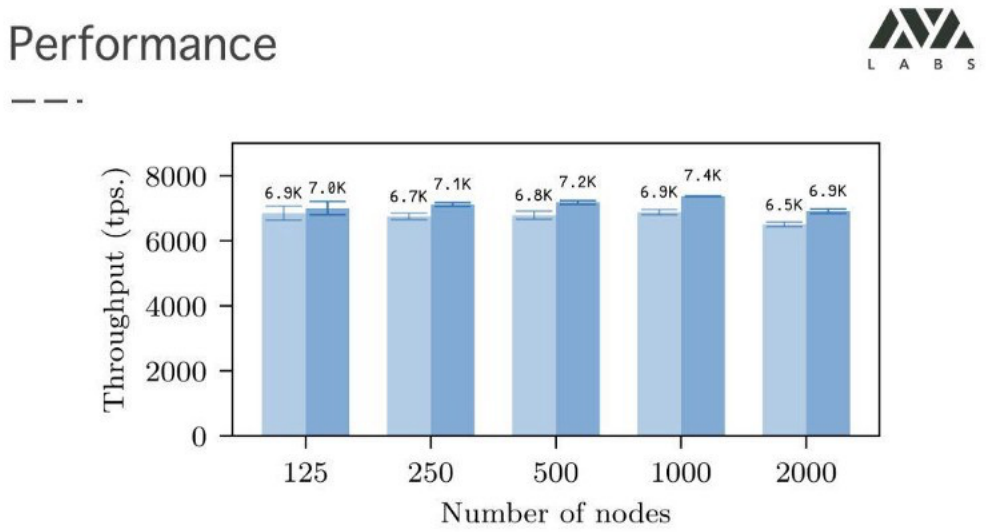
Throughput, Latency

Finality, Consistency

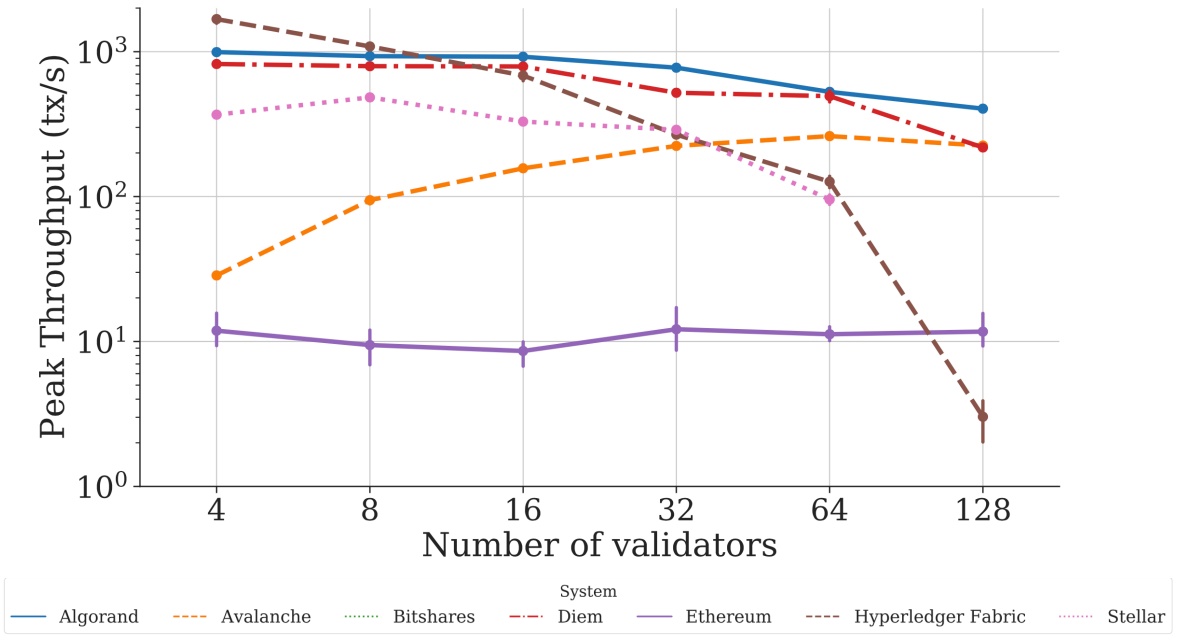
Resistance to Attacks

Benchmarking

Ad hoc benchmarks are often unreliable



Declared



Reproduced

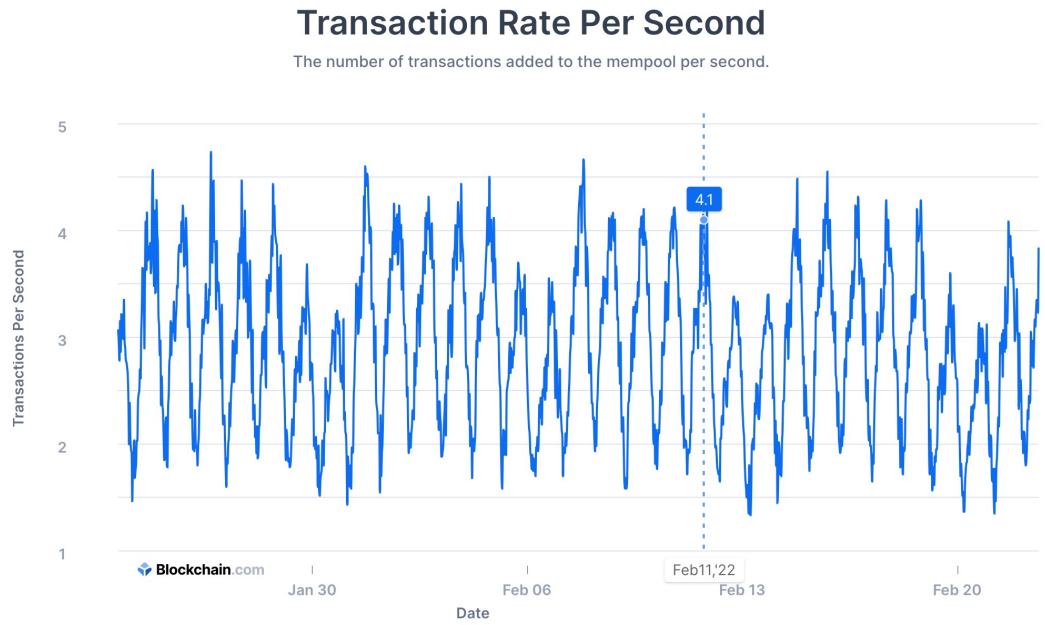
Benchmarking

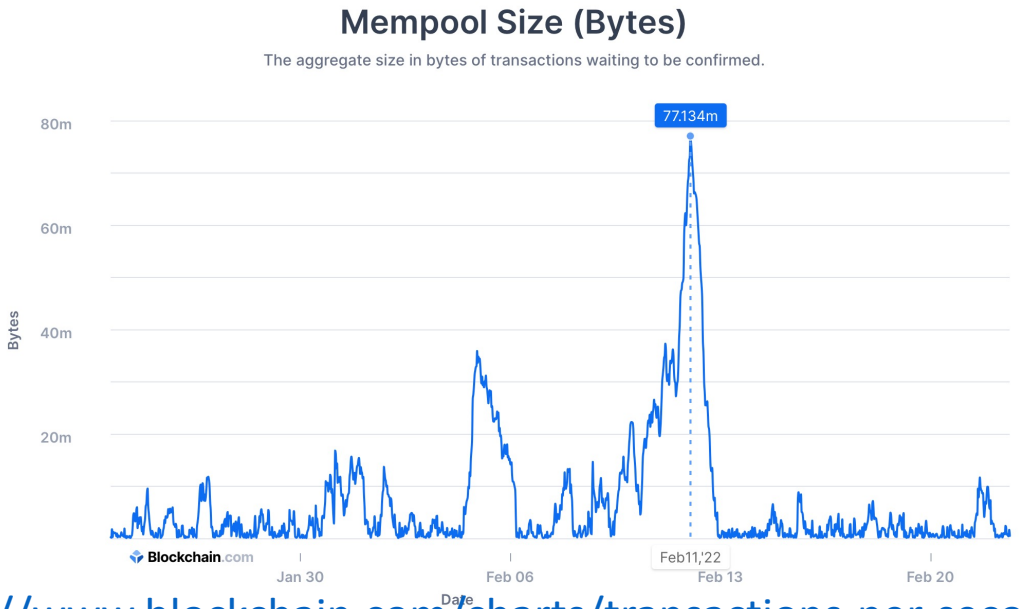
Ad hoc benchmarks are often unreliable. Why?

- Have limited usability:
  - Like maximum possible throughput by consensus
  - Test only ‘sunny-day’ scenarios
  - Cloud settings have predictable latency
  - Make small cheats here and there – like blockchain with simulated signatures
- Extreme conditions more usable:
  - Congestion – everyone send transactions, long wait times

More reliable numbers?

1. Test yourself. Make sure you test system under pressure
2. Explorers are more interesting + Mempool Size

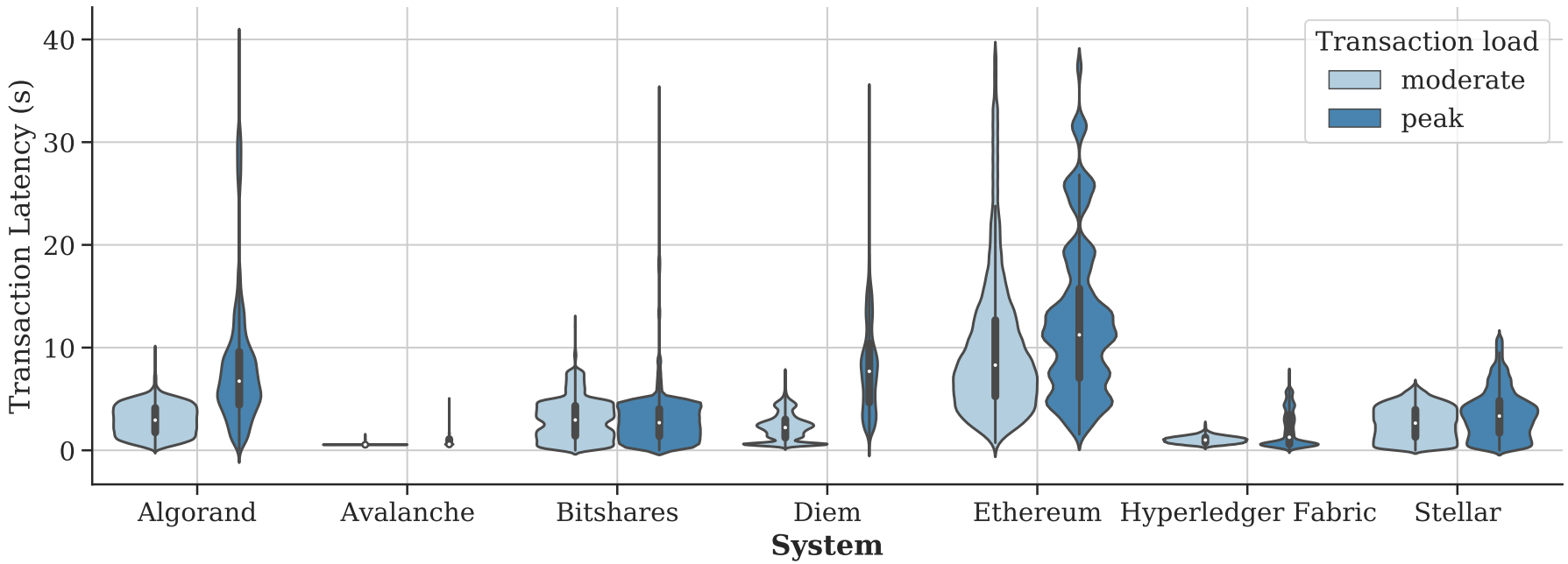




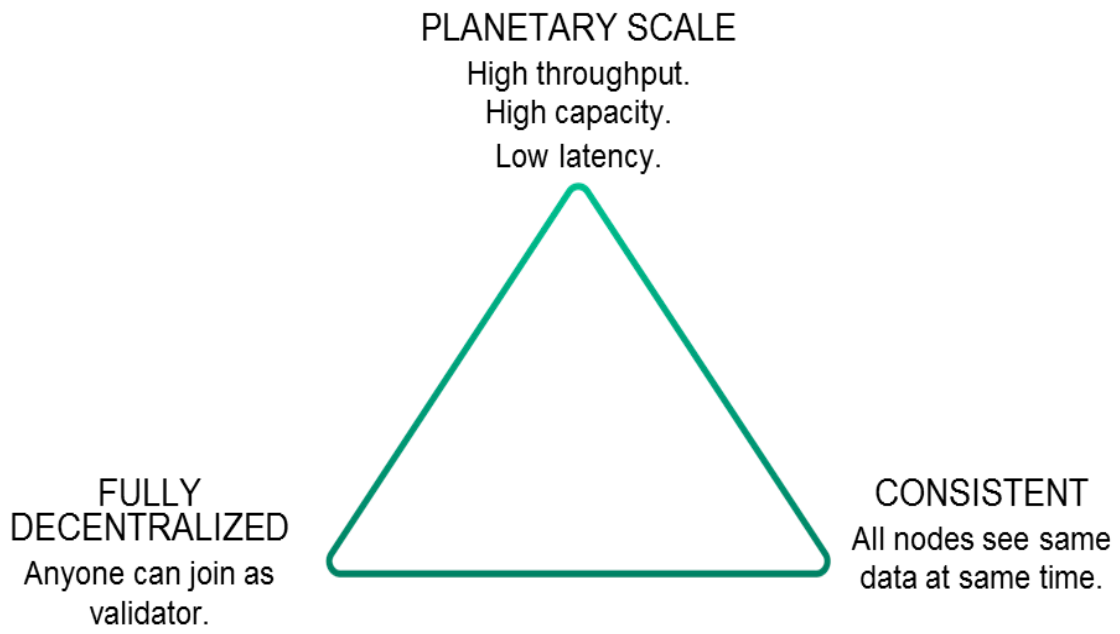
https://www.blockchain.com/charts/transactions-per-second

TPS vs Latency

Overloaded network either loses in throughput or in latency

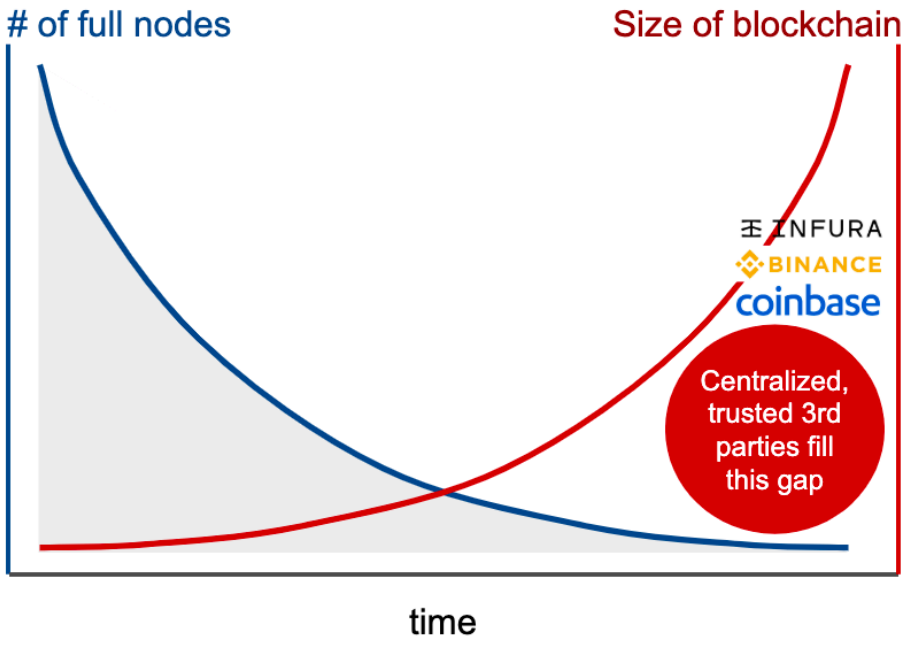


No Free Lunch



- Scalable and Decentralized Blokchcain is imposible
- Future:
  - Many blokchcains, bridges and layer 2
  - Beyond Consensus - based on different principles

No Free Lunch

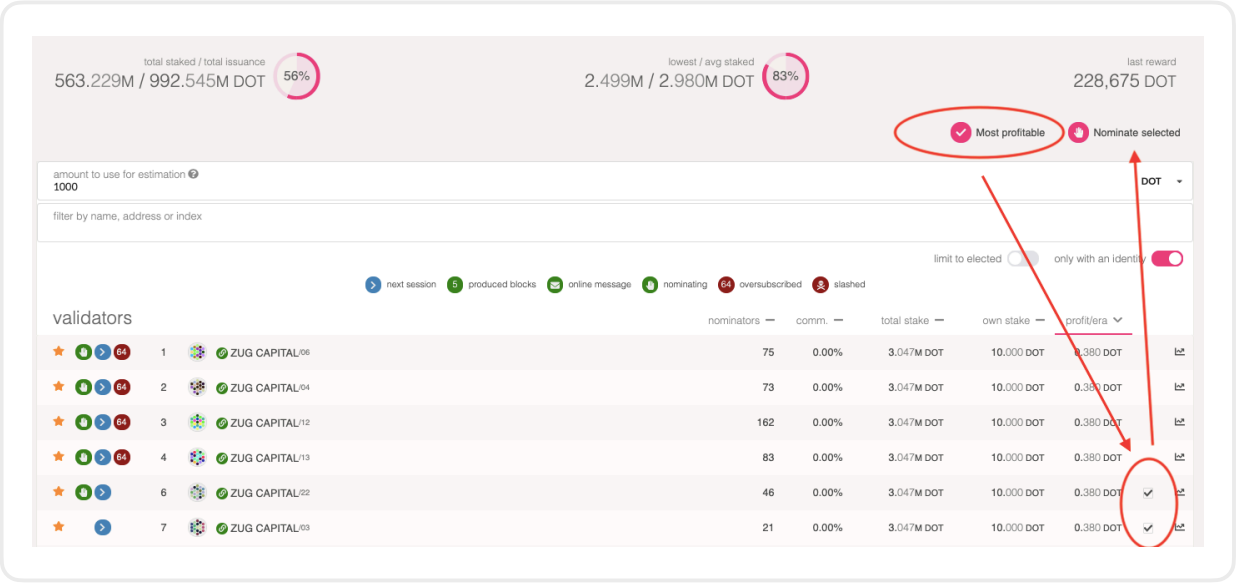


Not all peers are equal

Subsystem	Measure	Bitcoin (Gini)	Ethereum (Gini)	Bitcoin (Data Source)	Ethereum (Data Source)
Mining	Block reward	0.4	0.82	blockchain.info/pools	etherscan.io/stat/miner?range=1&blocktype=blocks
Client	Unique codebases	0.915	0.92	bitnodes.21.co/api/#list-nodes	ethernodes.org/network/1/nodes
Developer	Commits to main client	0.79	0.91	github.com/bitcoin/bitcoin	github.com/ethereum/go-ethereum
Exchange	24 hour volume	0.83	0.85	coinmarketcap.com/currencies/bitcoin/#markets	coinmarketcap.com/currencies/ethereum/#markets
Node	Distribution across countries	0.84	0.85	bitnodes.21.co/api/#list-nodes	ethernodes.org/network/1/nodes
Owner	Distribution across addresses with >$500k [Jul 2017]	0.65	0.76	bitinfocharts.com/top-100-richest-bitcoin-addresses-0.html	etherscan.io/accounts
Maximum Gini		**0.915**	**0.92**		

Validators

More centralization -> More risk



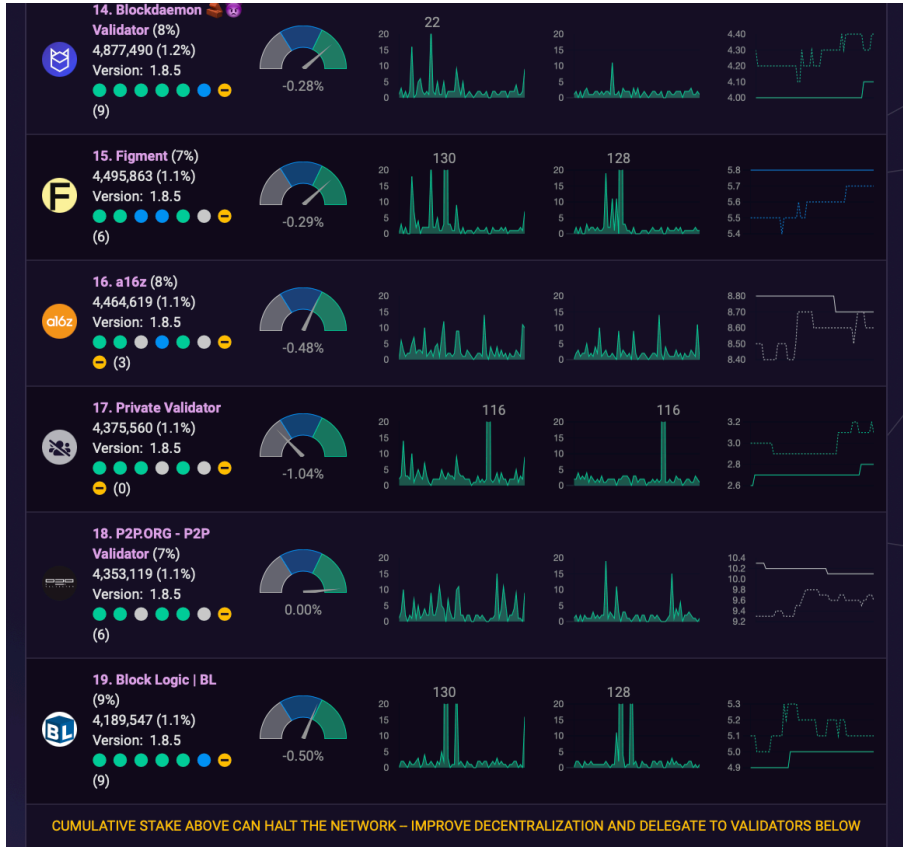
Will the 21 validators in EOS blockchain ever change or will they remain static?

2 Answers

Marius Kramer, No. 1 Cryptocurrency writer on Quora worldwide

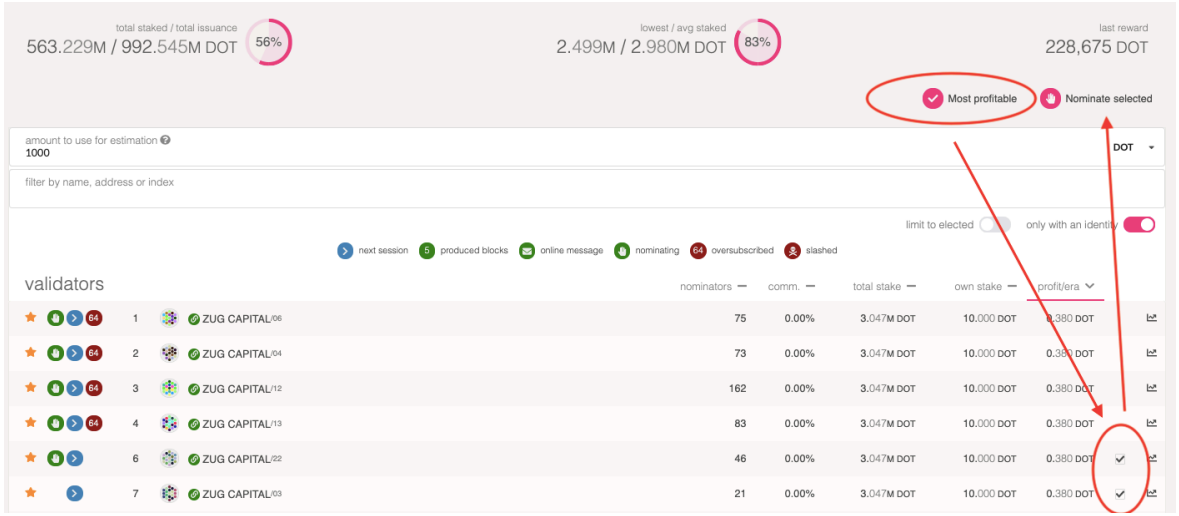
Answered 3 years ago · Author has **1.9K** answers and **175.4M** answer views

Yes they can constantly change based on their performance. However, it seems like the voting isn't working, because Block producers are doing a horrible job and no one cares.



Validators

More centralization -> More risk

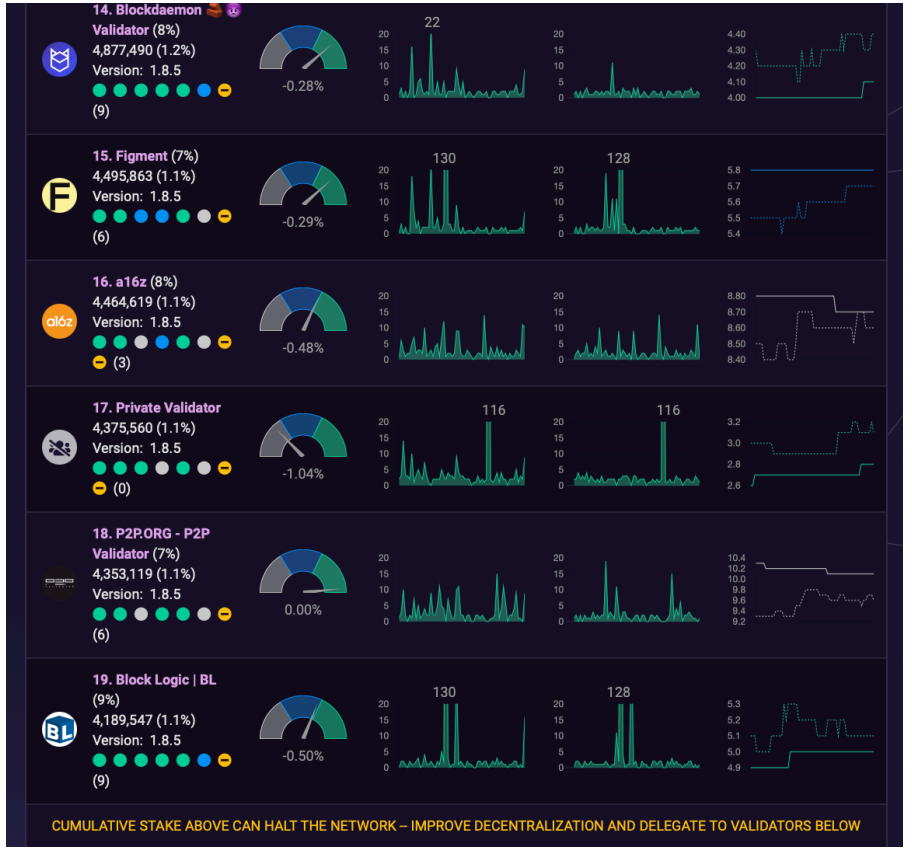


Will the 21 validators in EOS blockchain ever change or will they remain static?

2 Answers

Marius Kramer, No. 1 Cryptocurrency writer on Quora worldwide
Answered 3 years ago · Author has **1.9K** answers and **175.4M** answer views

Yes they can constantly change based on their performance. However, it seems like the voting isn't working, because Block producers are doing a horrible job and no one cares.



Build own System

What challenges you need to solve?

1. Connect peers with each other – Discovery and Bootstrap problem
2. Peers need to communicate with each other: Gossip Protocol
3. You need to deal with unreliable network. Anyone from the world can connect
4. They can run any other protocol
5. You need to safeguard the smart contracts execution
6. Tons of attacks and manipulations possible: Byzantine, Sybils, Eclipse attacks, double-spending attacks etc.

Technical Deep Dive

https://github.com/grimadas/BlockchainEngineering