CONSENSUS PROTOCOLS

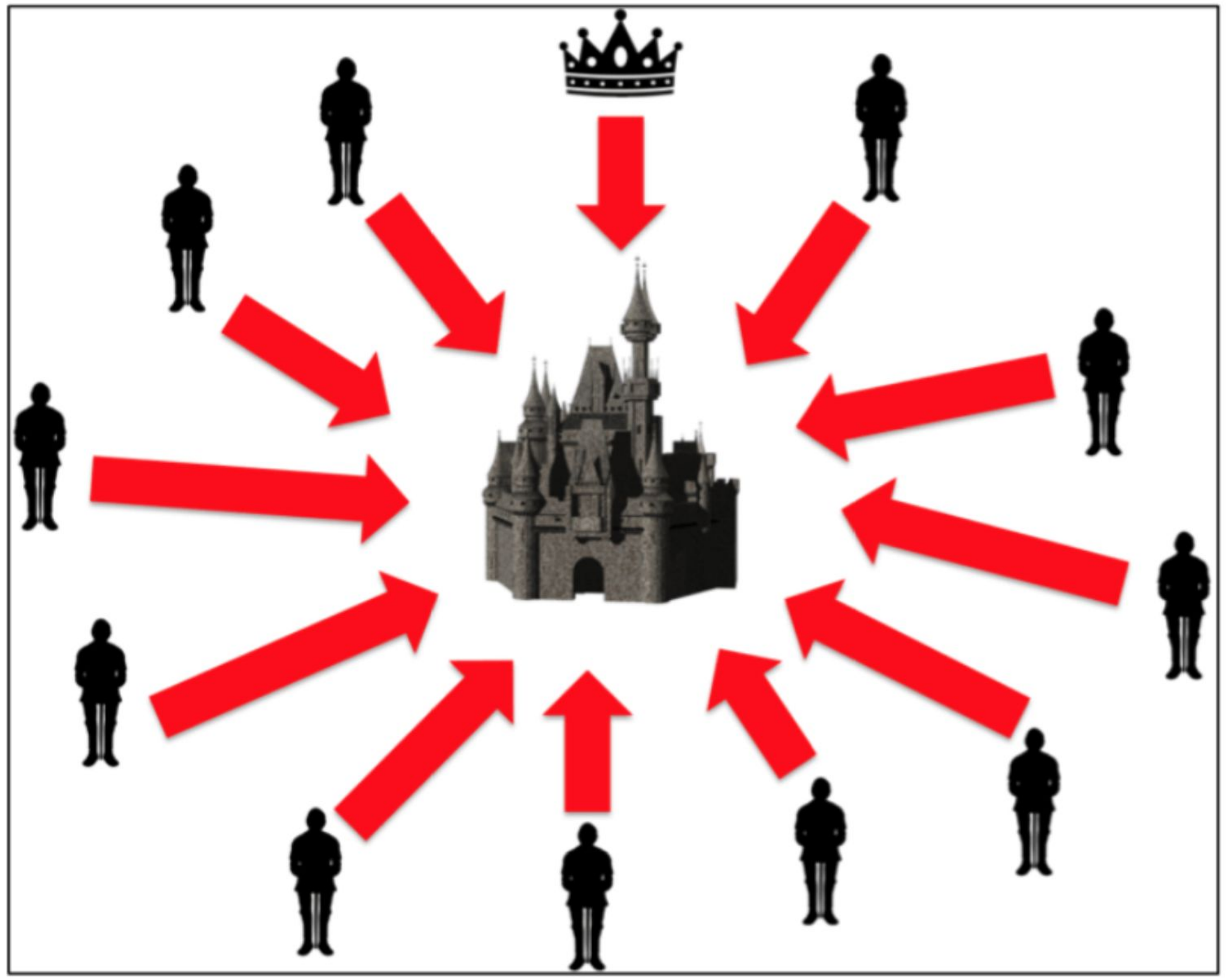
BLOCKCHAIN
@ COLUMBIA

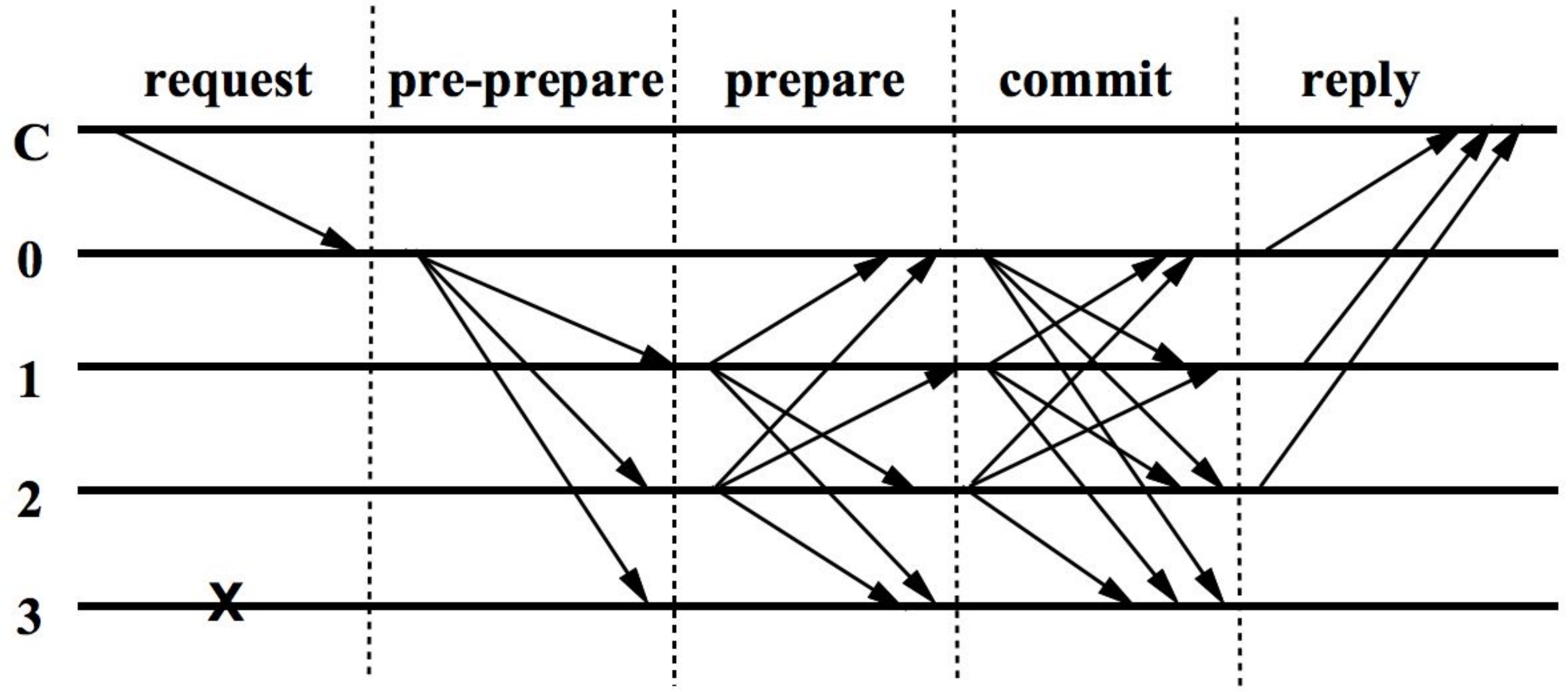
Overview

- Recap
- Proof of Work
- Proof of Stake
- Delegated Proof of Stake
- Other Consensus Mechanisms

Recap | Byzantine Fault Tolerance

- BFT is a systems ability to continue operating in the presence of malicious or faulty nodes and i.e., Byzantine Faults
- Modelled based on the Byzantine Generals Problem (Lamport 1982)
- PBFT: leader-based consensus protocol





BLOCKCHAIN @ COLUMBIA

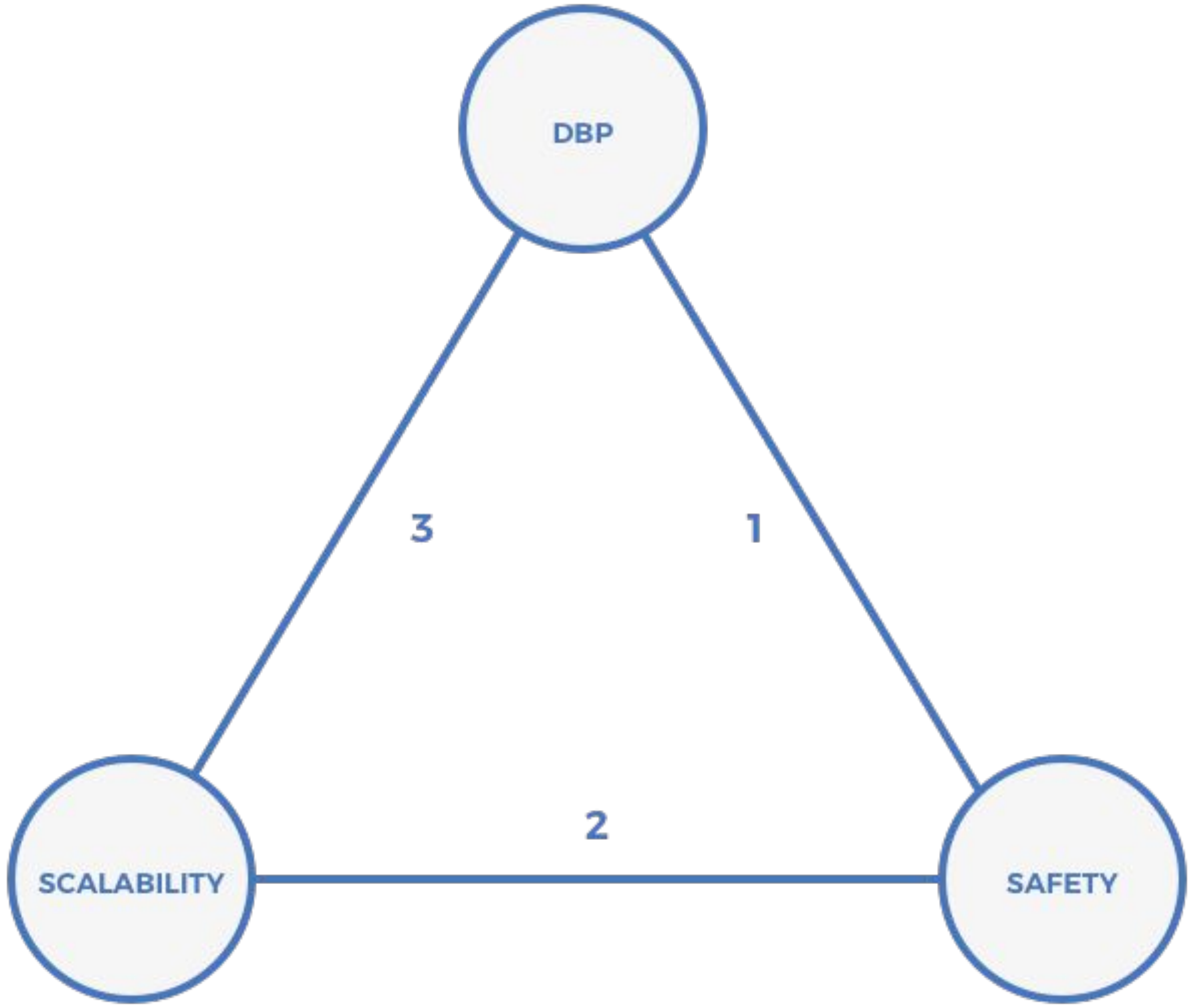
Recap | What is consensus?

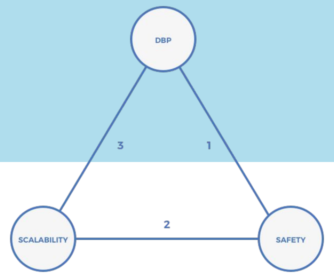
- *Consensus* is reached when all the nodes on the network agree on which block to produce next, and the state of the transaction history
- Consensus is a major bottleneck for decentralization, scalability, and security
- Blockchain consensus protocols must be somewhat resistant to Byzantine faults

Scalability Trilemma

Blockchain consensus protocols face tradeoffs in three core areas:

1. Decentralization of block producers
2. Safety: the relative cost of mounting a Byzantine attack against the network
3. Scalability: the number of transactions per unit time that the network can process





“Miners”

- Other names for miners (Bitcoin, Ethereum, etc.):
  - Forgers (Peercoin)
  - Witnesses (Steemit)
  - Block producers (EOS, Bitshares)
  - Verifiers (Hashgraph)
  - So many more!

Proof of Work | Overview

- Proof of work is a consensus protocol that selects block producers based on CPU power
- Miners earn the right to produce if a block if they find a *nonce* (or number) such that
    - Hash(*nonce* + prev block hash + transactions) < target
        - The target is known as the mining difficulty
- Verifiable that a certain amount of work has been done to create a new block
- Randomization determined by solving math problems

Proof of Work | Advantages

- Security/Finality - PoW provides the best economic finality on a transaction; it would require serious time or money to ‘rebuild’ the Bitcoin blockchain from scratch.
- Time-tested and proven to work
- Inherent value based on computational resources
- More accurate randomness

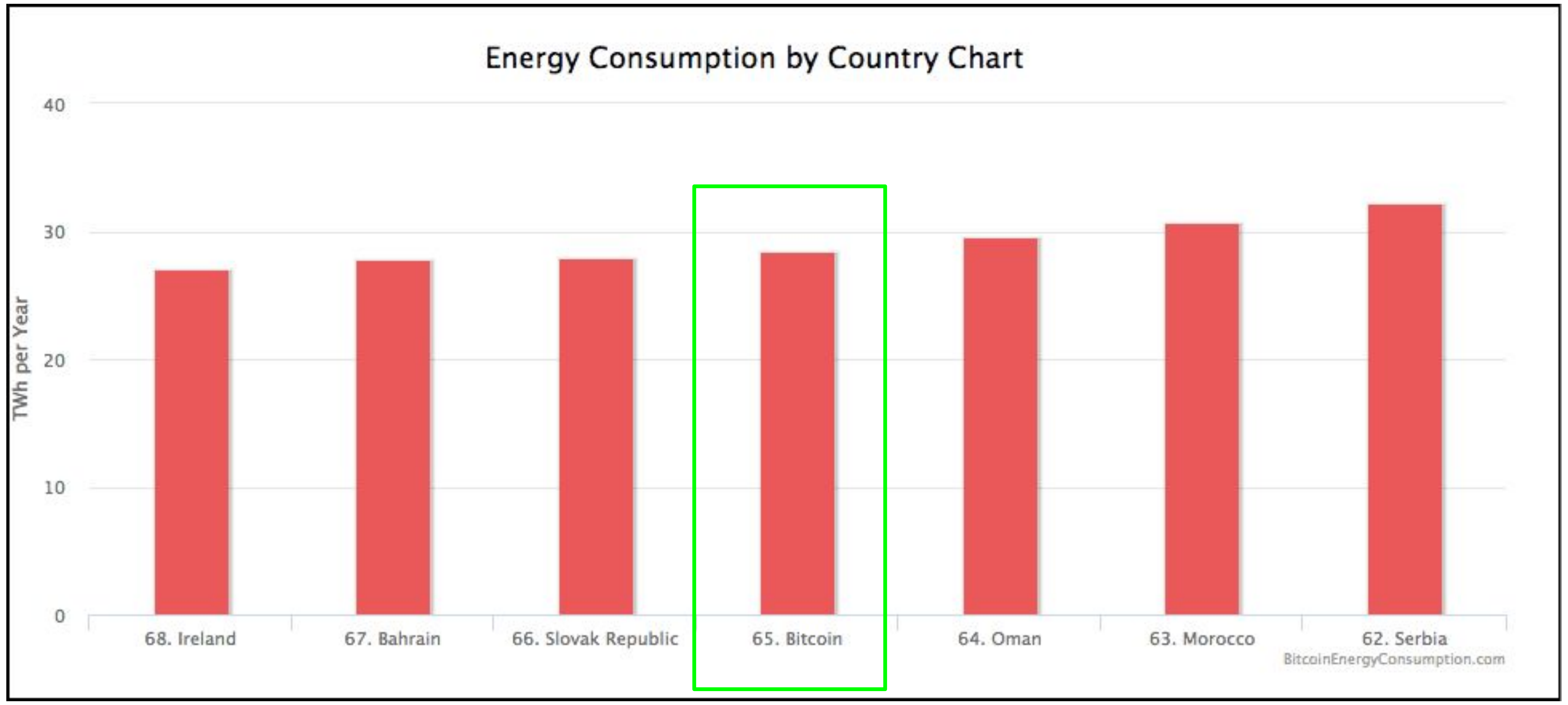
Proof of Work | Disadvantages

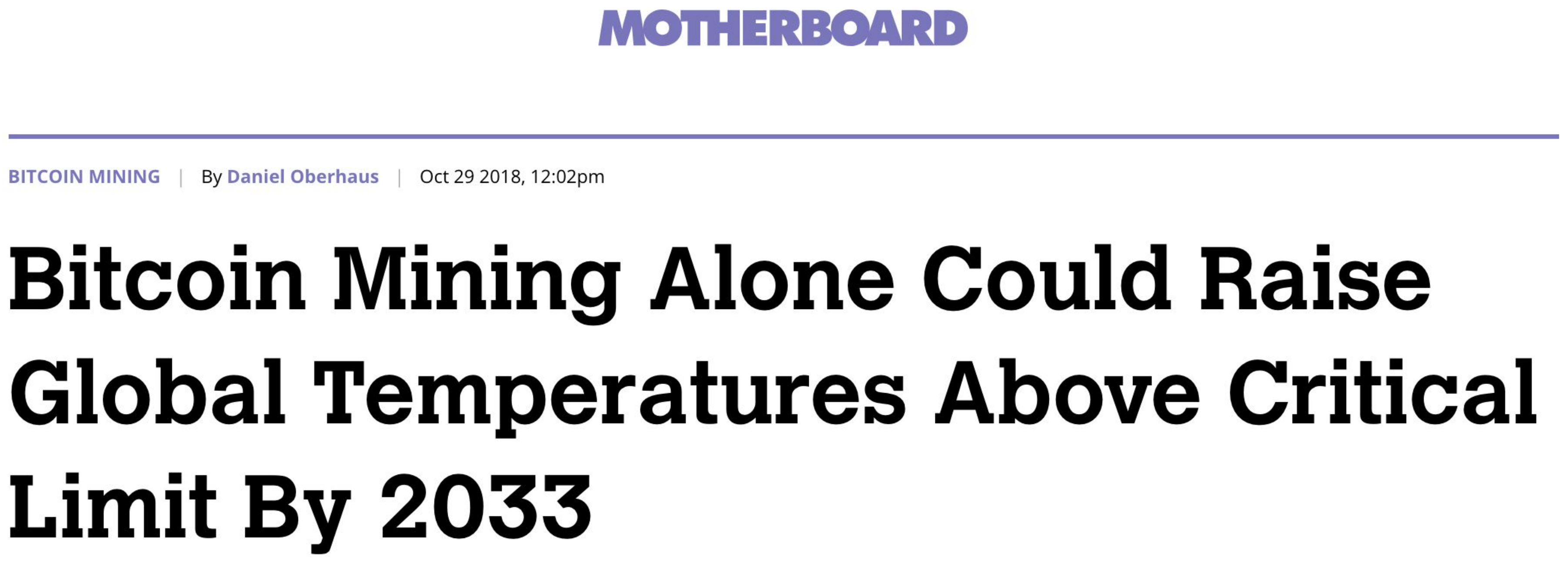
Increasing electricity costs

Scalability -> Slow throughput

Bitcoin: 4-5 tsp
Ethereum:10-15 tps

Wasted computation




MOTHERBOARD

BITCOIN MINING | By Daniel Oberhaus | Oct 29 2018, 12:02pm

Bitcoin Mining Alone Could Raise Global Temperatures Above Critical Limit By 2033

Proof of Stake (PoS) | Overview

- Proof of Stake (2011) is a consensus algorithm that depends on the validator's economic stake in the network
- Rather than using hash power as the scarce resource that prevents sybil attacks, PoS uses the digital currency itself.
- Validators stake tokens to enter into lottery for producing the next block
  - A validators probability of being selected to produce a block is proportional to the number of tokens stake

Original PoS - Peercoin

- Peercoin was the first real implementation of PoS (2013) where *forgers* (miners) would validate transactions in blocks in an order determined by a ‘simple’ proof of work.
    - Coin Age: Forgers have coins for a certain amount of blocks, accruing *age* for their wallet.
        - Age = # of coins * # of blocks since they entered this wallet
    - The greater a wallet’s total coin age, the lower the difficulty, the easier it will be to mine the next block.
    - A minimum coin age is needed to produce a block.

Original PoS - Peercoin

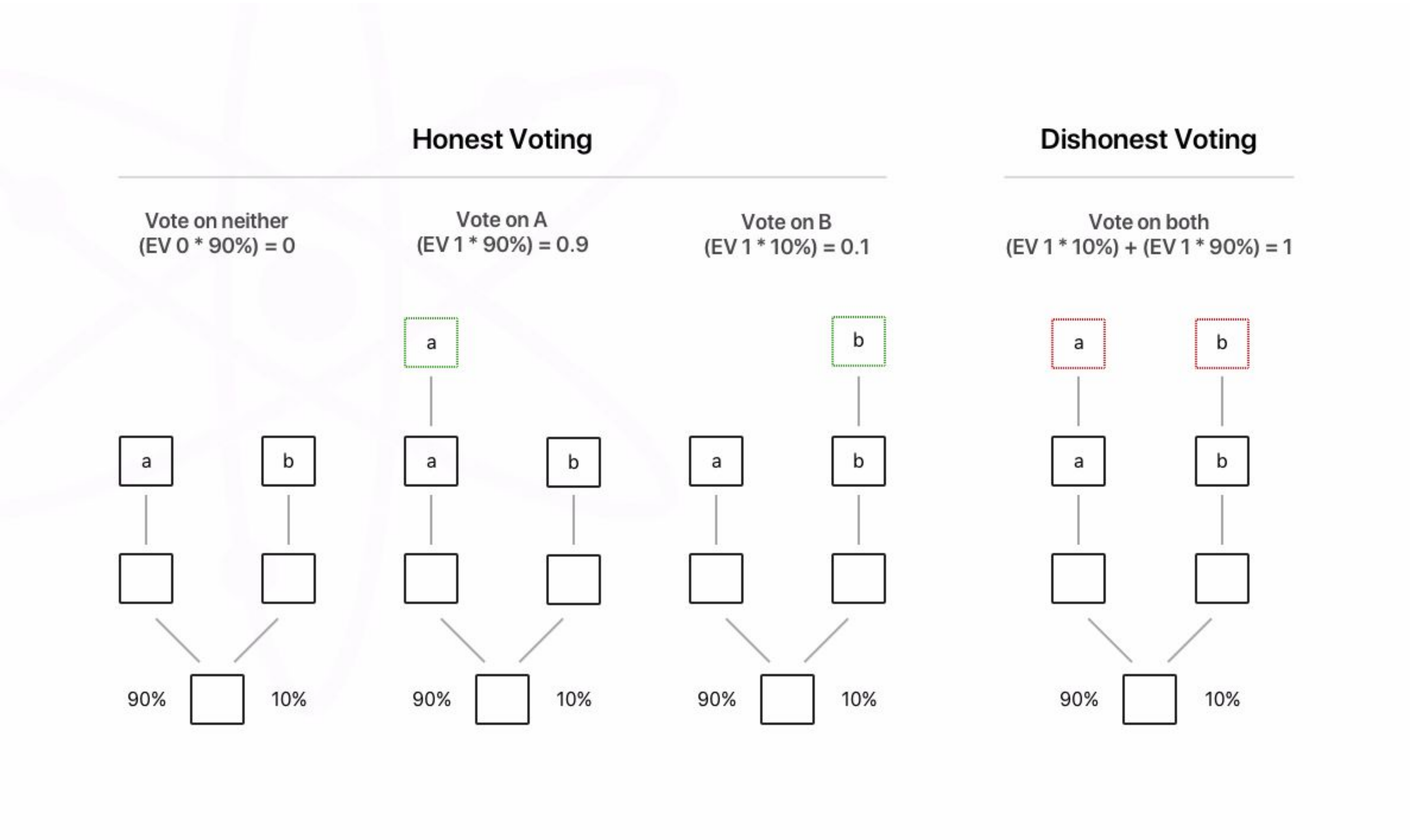
- To mine, a miner:
    - Stakes his coins that make up his coin age
    - Verifies transactions in a block
    - Computes simple PoW
    - Gives himself a block reward
    - Publishes that block to the network

Proof of Stake | Advantages

- Minimizes electricity costs
- Increases the efficiency of the blockchain
  - Ethereum is currently attempting to implement this with Casper 2.0 and sharding
- Allows restructuring of fees
- More consistent block times

The “Nothing at Stake” Problem

- Vanilla PoS systems impose no financial penalty for producing a fraudulent block or staking on multiple conflicting chains
    - In PoW systems there are sunk electricity costs or producing blocks - financially incentives miners to produce blocks that will be accepted by the majority of the network



Solutions to “Nothing at Stake”

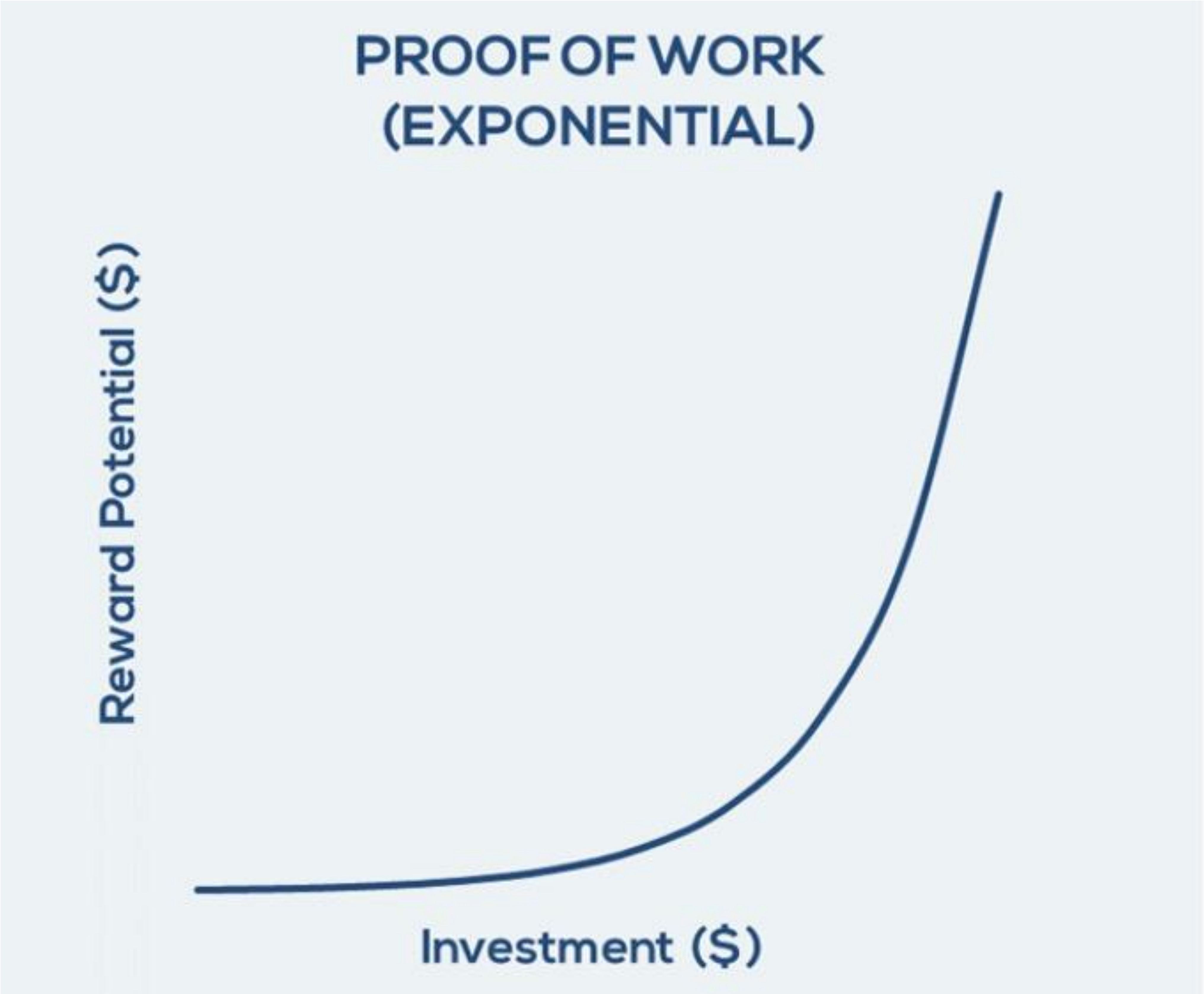
- Casper: Ethereum’s PoS solution
  - Slashing: Confiscate stake for validators who stake on multiple chains or engage in fraudulent activity. See Vitalik’s “Slasher” paper.
  - Sharding: ‘splitting’ byzantine agreement to multiple fragments

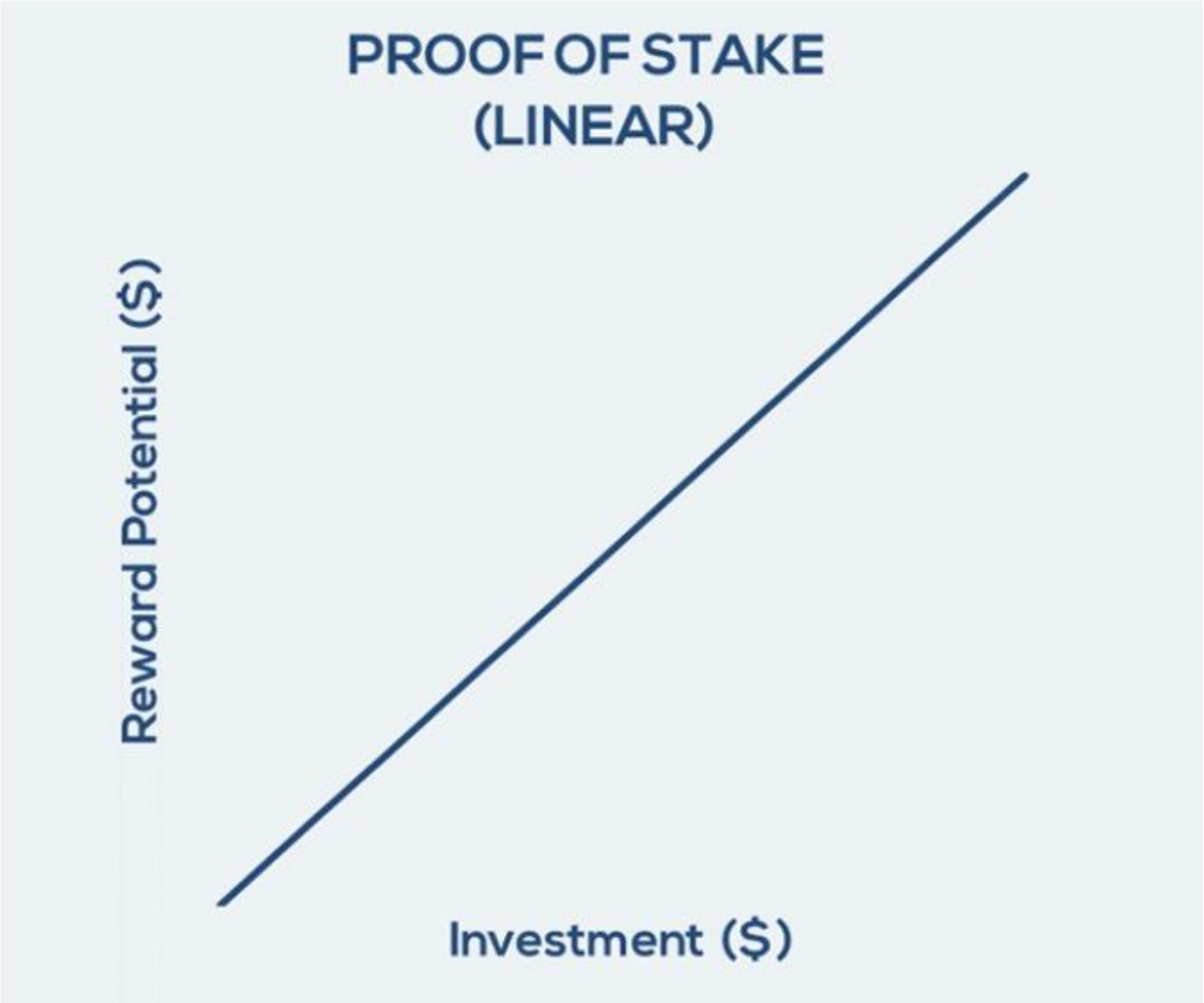
ethereum

Economic Finality Problem

- Because there isn’t a large sum of computational power used to mine each block, ‘rebuilding’ a new version of the blockchain / branch is not that energy consuming.
- Attackers can not only attack the most recent blocks, but could more easily alter the long history of the blockchain.

PoW vs. PoS | Cost and Scalability





https://hackernoon.com/consensus-mechanisms-explained-pow-vs-pos-89951c66ae10

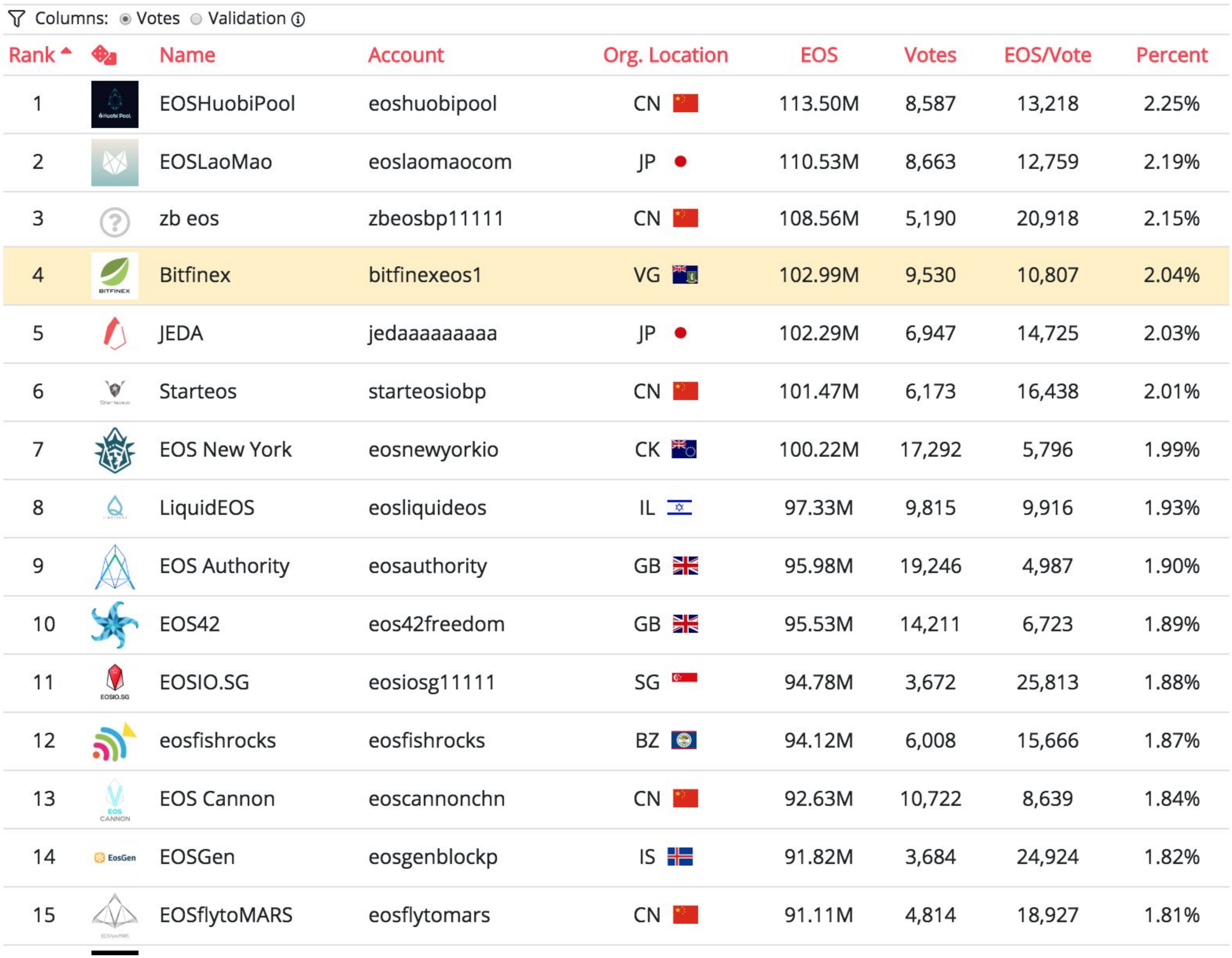
Delegated Proof of Stake | Overview

- Invented by Dan Larimer in 2014 (EOS, Bitshares, Steemit)
- Holders of network tokens are able to cast votes to elect block producers (miners, witnesses, etc.)
- Voter weight is proportional to the amount of tokens staked
- Tokens can be staked instantly, but require time to unstake (several weeks)
- Block producers run PoS with slashing
- Some protocols incorporate liquid voting, whereby stake can be delegated to other voters as *proxy votes.*
- The amount of processing power each wallet gets to produce on the network depends on number of tokens staked.

Delegated Proof of Stake | Consensus

1. Wallets stake their coins and vote for miners/proxies
2. Miners then:
    a. Get chosen at random to produce block
        i. Indexing smallest units of the staked coins (no age!)
    b. Verify transactions in a block
        i. Verification isn't just ownership, but rights to processing power.
    c. Give themselves a block reward
    d. Publishes that block to the network

Block Producer List (EOS)



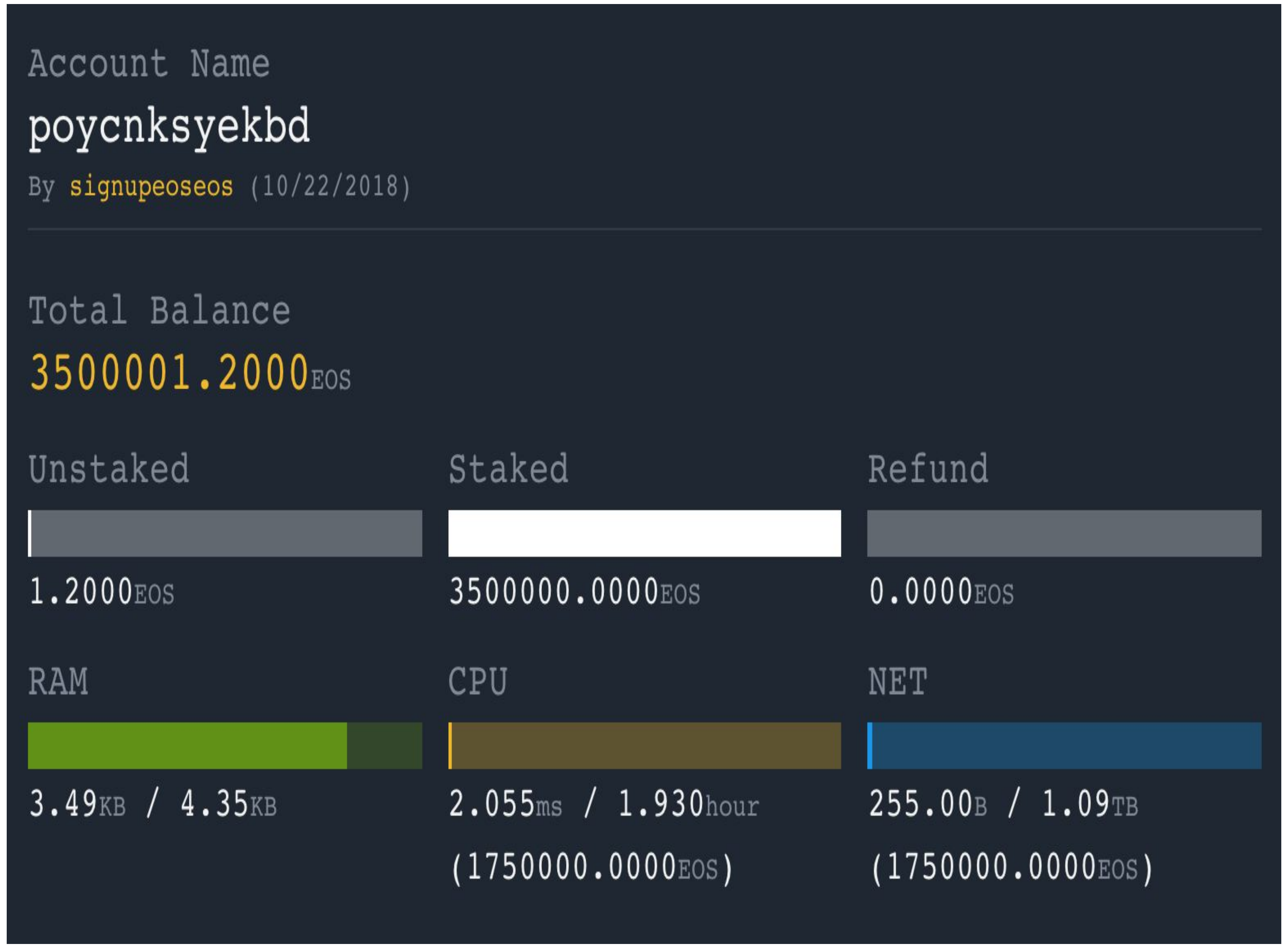
Columns: ● Votes ○ Validation ⓘ

Rank		Name	Account	Org. Location	EOS	Votes	EOS/Vote	Percent
1		EOSHuobiPool	eoshuobipool	CN	113.50M	8,587	13,218	2.25%
2		EOSLaoMao	eoslaomaocom	JP	110.53M	8,663	12,759	2.19%
3		zb eos	zbeosbp11111	CN	108.56M	5,190	20,918	2.15%
4		Bitfinex	bitfinexeos1	VG	102.99M	9,530	10,807	2.04%
5		JEDA	jedaaaaaaaaa	JP	102.29M	6,947	14,725	2.03%
6		Starteos	starteosiobp	CN	101.47M	6,173	16,438	2.01%
7		EOS New York	eosnewyorkio	CK	100.22M	17,292	5,796	1.99%
8		LiquidEOS	eosliquideos	IL	97.33M	9,815	9,916	1.93%
9		EOS Authority	eosauthority	GB	95.98M	19,246	4,987	1.90%
10		EOS42	eos42freedom	GB	95.53M	14,211	6,723	1.89%
11		EOSIO.SG	eosiosg11111	SG	94.78M	3,672	25,813	1.88%
12		eosfishrocks	eosfishrocks	BZ	94.12M	6,008	15,666	1.87%
13		EOS Cannon	eoscannonchn	CN	92.63M	10,722	8,639	1.84%
14		EOSGen	eosgenblockp	IS	91.82M	3,684	24,924	1.82%
15		EOSflytoMARS	eosflytomars	CN	91.11M	4,814	18,927	1.81%

BLOCKCHAIN
@ COLUMBIA

Delegated Proof of Stake | Advantages

- Scalability: More transactions, less electricity
  - EOS: currently >4,000 tps
- ‘Feeless’ transactions
  - Can be paid by user or smart contract



Account Name
poycnksyekbd
By signupeoseos (10/22/2018)

Total Balance
3500001.2000EOS

Unstaked
1.2000EOS

Staked
3500000.0000EOS

Refund
0.0000EOS

RAM
3.49KB / 4.35KB

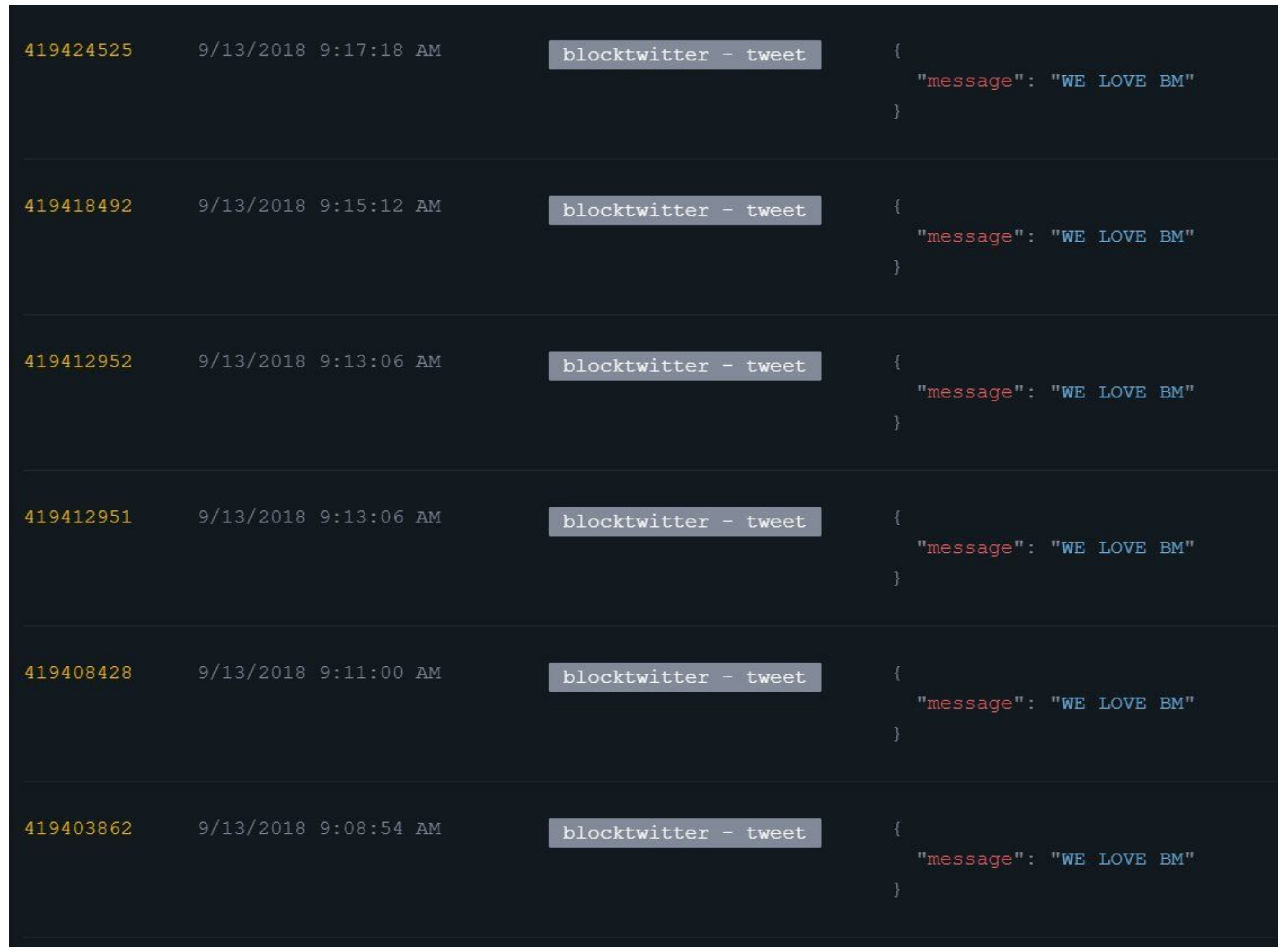
CPU
2.055ms / 1.930hour
(1750000.0000EOS)

NET
255.00B / 1.09TB
(1750000.0000EOS)

BLOCKCHAIN
@ COLUMBIA

Delegated Proof of Stake | Disadvantages

- Network centralization - The rich get richer
- Tragedy of the commons - potential for low voter turnouts
- Collusion among block producers
    - ○ “Vote for me I’ll give you some of my block rewards!”
- Centralized exchanges as block producers
- Spamming



```
419424525    9/13/2018 9:17:18 AM    blocktwitter - tweet    {
                                                               "message": "WE LOVE BM"
                                                             }
419418492    9/13/2018 9:15:12 AM    blocktwitter - tweet    {
                                                               "message": "WE LOVE BM"
                                                             }
419412952    9/13/2018 9:13:06 AM    blocktwitter - tweet    {
                                                               "message": "WE LOVE BM"
                                                             }
419412951    9/13/2018 9:13:06 AM    blocktwitter - tweet    {
                                                               "message": "WE LOVE BM"
                                                             }
419408428    9/13/2018 9:11:00 AM    blocktwitter - tweet    {
                                                               "message": "WE LOVE BM"
                                                             }
419403862    9/13/2018 9:08:54 AM    blocktwitter - tweet    {
                                                               "message": "WE LOVE BM"
                                                             }
```

Top DPoS Blockchains

EOS

CARDANO

NEO
smart economy

Other Consensus Protocols

- Hashgraph
    - DAG with gossip protocol - 39 ‘verifiers’ for now
- Stellar Federated BFT - 80% tokens held by the foundation for now
    - Quorum slices
- Proof of Burn
- Proof of Authority - Gavin Woods, Kovan ETH Testnet