CS578:
Blockchain Technology: A Software Engineering Perspective

Dr. Raju Halder


In order to secure a blockchain ... it's estimated that both Bitcoin and Ethereum burn over $1 million worth of electricity and hardware costs per day as part of their consensus mechanism.
- VITALIK BUTERIN

EDITOR'S PICK | 23,388 views | Apr 19, 2018, 11:09pm

Bitcoin's Energy Consumption Can Power An Entire Country -- But EOS Is Trying To Fix That

Sherman Lee Contributor
I write about deep tech, crypto, and artificial intelligence.

‹ Back to Articles

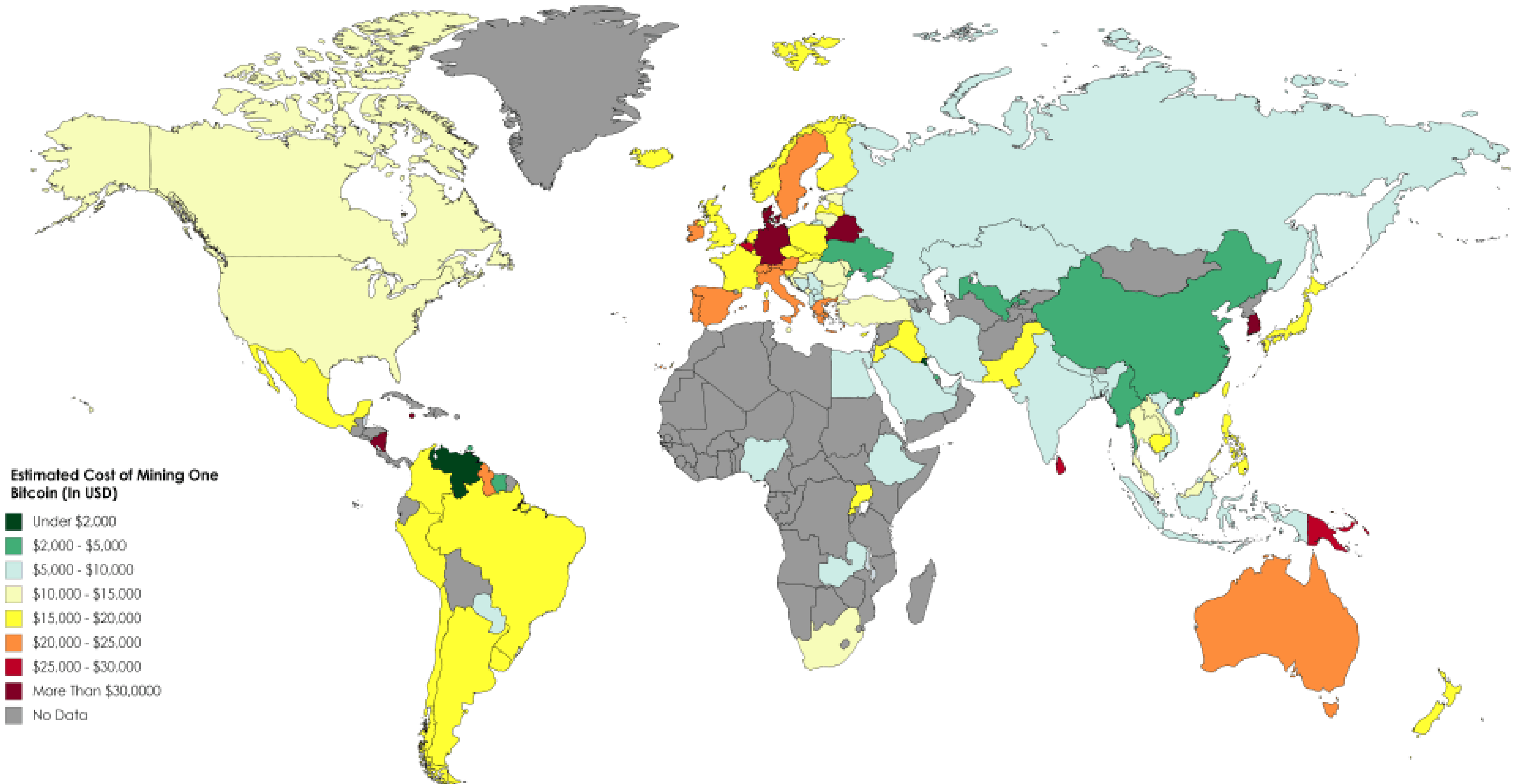
Bitcoins Energy Consumption An Unsustainable Protocol That Must Evolve?

3

3

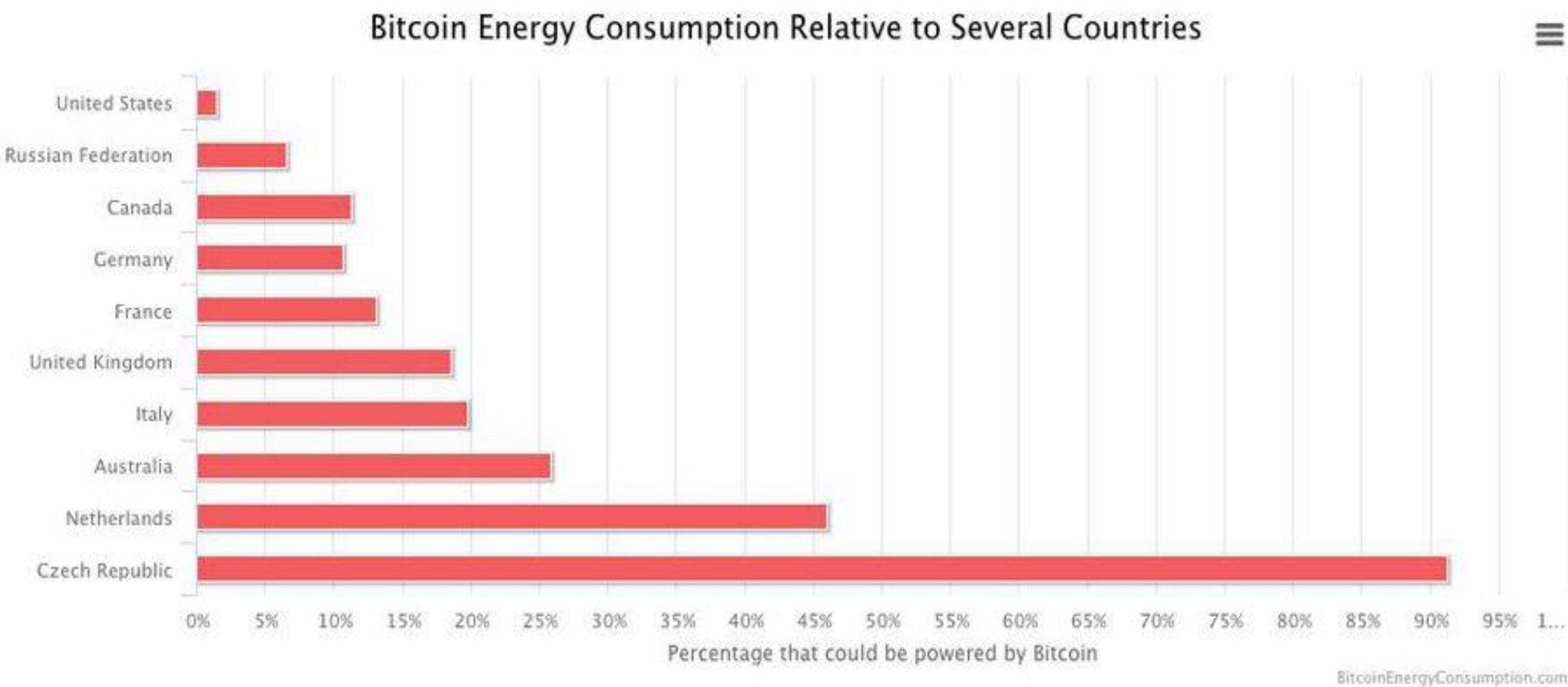
By john lilic #Blockchain 101 #Blockchain for Business #Blockchain for Investors

Estimated Electricity Cost Of Mining One Bitcoin By Country



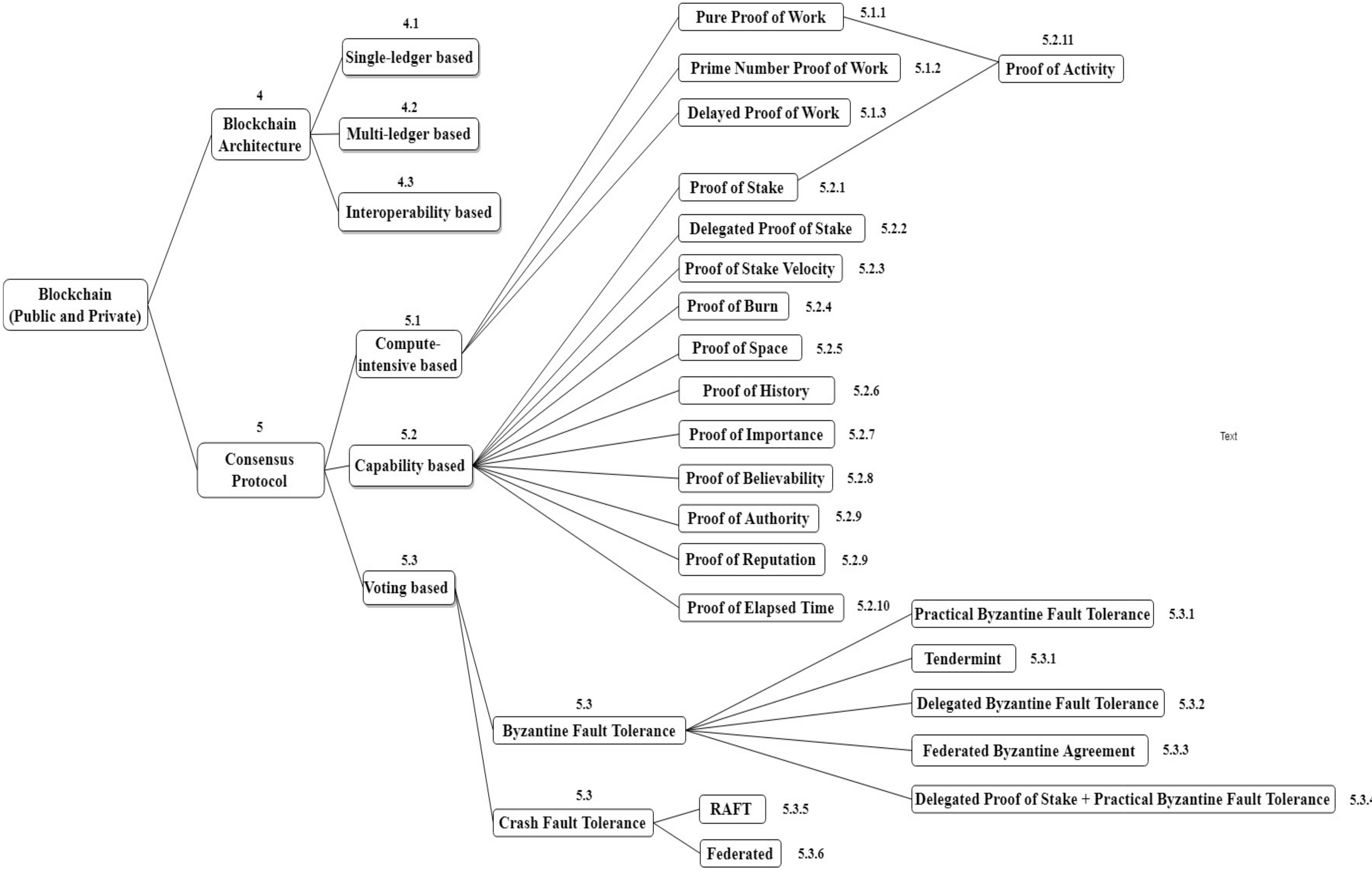
Source: https://powercompare.co.uk/bitcoin-electricity-cost/

The Bitcoin POW mechanism is so costly that it consumes the same amount of electricity it takes to power a country like Switzerland in one year. Bitcoin's current estimated annual electricity consumption is 61.4 TWh, which is also equivalent to 1.5% of the electricity consumed in the United States.



A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions

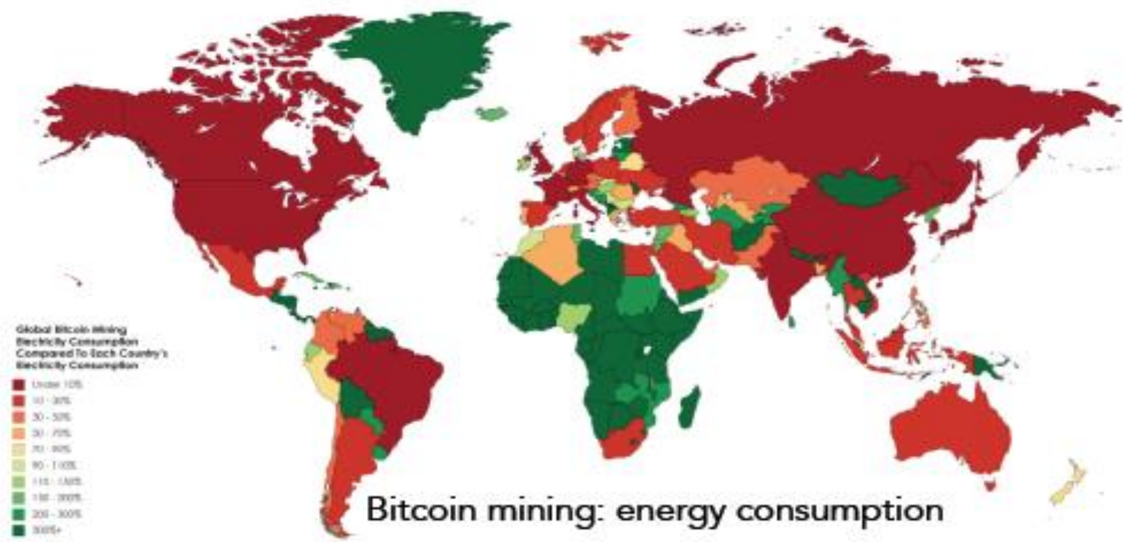
by L. Ismail and H. Materwala (Symmetry 2019, 11, 1198)



Proof of X

Proof of Stake

- And others: Burn, Elapsed time, Capacity



Bitcoin mining: energy consumption

Proof-of-X

- Proof-of-X (PoX) schemes is an umbrella term for systems that replace PoW with more useful and energy-efficient alternatives to Proof-of-Work (PoW).

Proof-of-Stake

Miner/Mining Vs. Validator/Minting or forged

- POS requires people to prove the ownership of a certain amount of currency
  - It is believed that people with more currencies would be less likely to attack the network.
  - If richest person attacks, currency value falls and it may be a loss for the attackers!
- Many blockchains adopt PoW at the beginning and transform to PoS gradually.
  - For instance, Ethereum is planning to move from Ethash (a kind of PoW) (Wood, 2014) to Casper (a kind of PoS) (Zamfir, 2015).

Proof-of-Stake

- PoS alternatives consume less energy and reach higher transactions per second.
- But they have also still to prove their attack-resistance in real open public settings like PoW so far.
- Challenge for proof-of-stake systems is to keep track of the changing stakes of the stakeholders.

Proof-of-Stake

- Selection by account balance would result in undesirable centralization because the single richest member would have a permanent advantage as it gets richer.

- Different versions:
  - random selection,
  - age-based stake selection

Proof-of-Stake: Coin-Age (Peercoin (King and Nadal, 2012)**)**

- Coin-Age=Number of Coins Staked * Number of Days Coins Staked.
- Example: 30 coins hold for 10 days will have coin age of 300 coin days.
- Forger with the maximum value of coin-age is selected to forge the block.
  - In order to participate in the process of forging, the coins must be staked for a minimum of 30 days (to avoid repetitive selection of a forger with a greater number of coins).
  - A malicious user may increase its probability of forging a block by holding the stake for a long period of time. To prevent this, the stake-holding period is capped at the maximum of 90 days.
- Once a block is created by a forger, the coin-age value of the coins staked by that forger becomes zero.

Proof-of-Stake: Randomized block selection method (Blackcoin (Vasin, 2014))

- A forger with a specific **hit value** is selected for forging the next block.
- Each forger encrypts the hash of the previous block using its private key. The encrypted value is hashed, and the first 8-bytes of the hashed output are converted into a number known as **hit value**.
- The forger with the hit value below a target value is selected for the process of forging. **Target** = $T_b * S * B_e$
  - T_b is the base target value calculated by multiplying the previous block target value and the amount of time that was required to forge that block,
  - S is the time elapsed since the last block forged and
  - B_e is the coins at stake.
- To make the selection based on the capability of miner, target value computation involves the number of coins staked by the miner.

Proof-of-Stake: Randomized block selection method (Blackcoin (Vasin, 2014))

- If the hit value of more than one forger is below the target value, then the forger with a high value of cumulative difficulty is selected

$$D_{cb} = D_{pb} + \frac{2^{64}}{T_b}$$

- where D_{pb} is the previous block's difficulty (the level of effort to create the previous block).

Delegated Proof-of-Stake

- The major difference between POS and DPOS is that POS is a direct democratic while DPOS is representative democratic.
- In DPoS, a group of nodes known as witnesses (also called delegates) are elected by the stakeholders based on a voting process (voting power is proportionately weighted based on the stake).
- The first N witnesses with the highest votes are then selected. N is selected such that 50% of the nodes have voted for these many witnesses.
- Each witness in the group mines a block in a round-robin fashion. Once all the witnesses in the group have had their turn, the list of witnesses is shuffled, and the round-robin continues.
- Users can also delegate their voting power to another user who will vote on their behalf.

Delegated Proof-of-Stake

- Higher Throughput: With significantly fewer nodes to validate the block, the block could be confirmed quickly, making the transactions confirmed quickly.

- Dishonest delegates could be voted out easily.

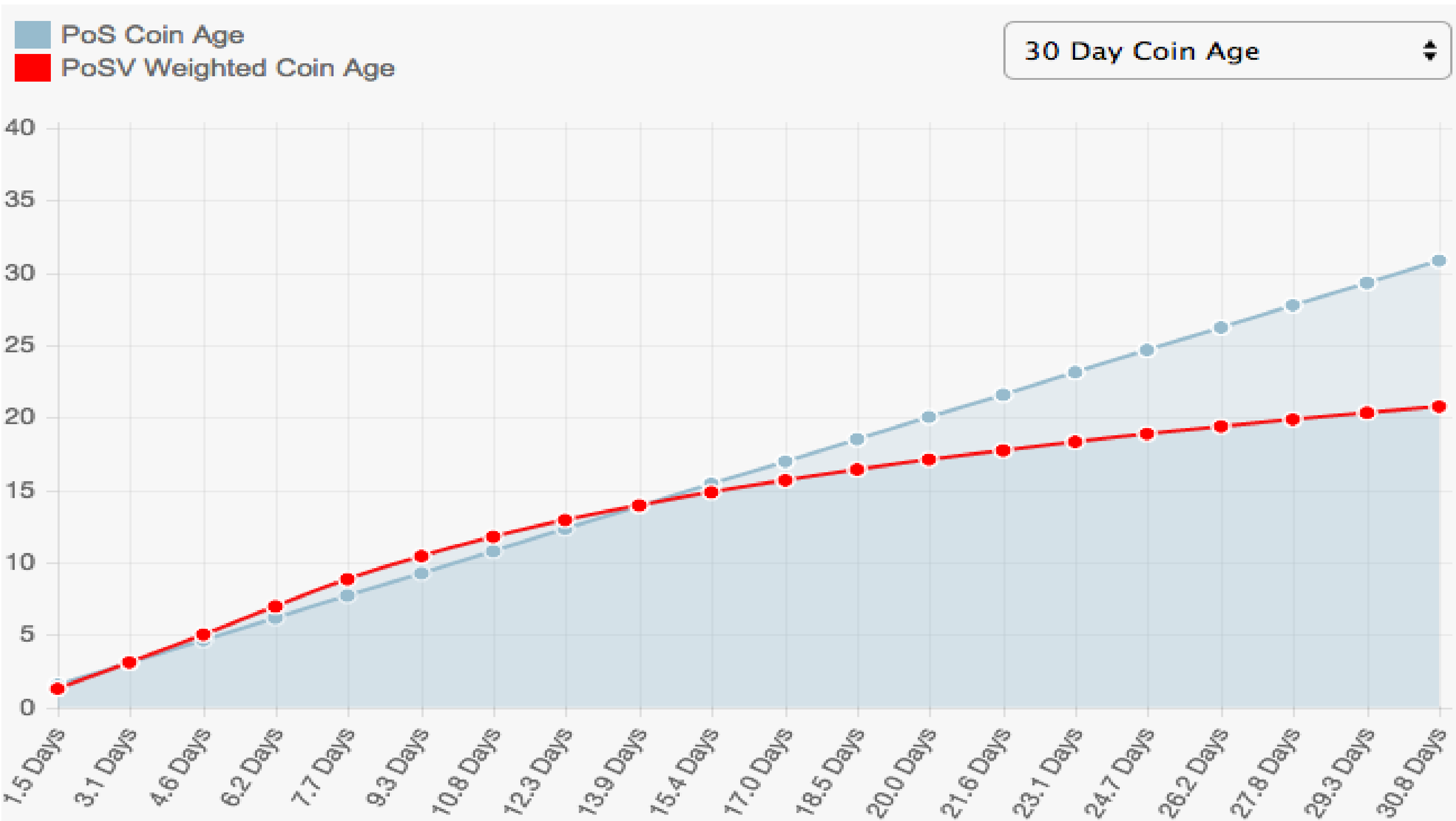
- Examples: Steem, BitShares, Cardano, Nano

Proof of Stake Velocity

- In PoS, coins held over time accumulate Coin Age linearly.
- PoSV introduces a non-linear coin-aging function in which Coin Age is accumulated more quickly in the first few days and weeks after a transaction than in later weeks.
- People who use their coins to stake regularly and sign blocks every 2 weeks or less are thereby able to earn up to 20% more rewards than people who keep their wallets offline for extended periods of time.
- This extra incentive to maintain an active wallet in turn increases the security by ensuring that larger numbers of coins are being actively staked.
- Reddcoin network by Larry Ren

Proof of Stake Velocity

- A trinomial function for the first 7 days of Coin Age accumulation, followed by an logarithmic function (exponential decay function) rate beyond 7 days.



Proof-of-Space

- Dziembowski et al. proposed proof of space (PoSpace) also known as proof of capacity.
- A miner with enough disk space wins the right to generate the next block in the chain.
- For example, Spacecoin, Chia, and Burstcoin.
- Two steps: *plotting* (generation of data blocks which is one time process) and *mining*

Proof-of-Space

- PoSpace consumes less energy than PoW.
- Does not favor the rich always as in case PoS.
- Can be prone to malware attacks as the plot of hashes stored in the hard disk can be easily attacked and tampered with.

Proof-of-Deposit

- Miners ‘lock’ a certain amount of coins, which they cannot spend for the duration of their mining.
- One such system is Tendermint, where a miner’s voting power is proportional to the amount of coins they have locked.
- Deposit could be revoked if they misbehaved.

Proof-of-Activity

- To combine the benefits of POW and POS, proof of activity (Bentov et al., 2014) is proposed.
- In proof of activity, a mined block (based on PoW) needs to be signed by N validators (PoS) to be valid.
- In that way, if some owner of 50% of all coins exists, he/she cannot control the creation of new blocks on his/her own.
- Since POA marries POW and POS, it draws criticism for its partial use of both.

Proof of Authority

- leverages identity instead of coins
- the PoA consensus algorithm is usually reliant upon:
  - valid and trustworthy identities: validators need to confirm their real identities.
  - difficulty to become a validator: a candidate must be willing to invest money and put his reputation at stake. A tough process reduces the risks of selecting questionable validators and incentivize a long-term commitment.
  - a standard for validator approval: the method for selecting validators must be equal to all candidates.
- Kovan and Rinkeby, the two Ethereum testnets, also use PoA as a consensus mechanism. Microsoft Azure is another example where the PoA is being implemented.

Proof-of-Burn

- Method for distributed consensus and an alternative to Proof of Work and Proof of Stake.
- Miners prove that they have destroyed a quantity of coins, for example by sending them to a irretrievable address, known as eater address
- Eater has a public key associated with no private key making it impossible to retrieve the coins from that account.
- Slimcode implemented this approach in 2014 but has recently been discontinued.

Proof-of-Burn

- Once the transactions are recorded, a burn hash for each transaction is calculated using SHA-256, and the miner with the least value of burn hash wins the mining right.

$$Burn\ hash = (Internal\ hash) \times Multiplier$$

- The internal hash is calculated by hashing together the burned transaction hash value, the time elapsed after burning the coins and the current block number.
- The multiplier is inversely proportional to the burned coins, increasing the probability of a miner burning more coins to be selected.

$$Multiplier = \frac{e^{\frac{T_b}{T_d}}}{Burned\ coins}$$

- where T_b is the time elapsed from the time the coins were burned and T_d is the time after which the coin will decay.

Proof-of-Elapsed-Time

- Often used on the permissioned blockchain networks.
- Each node in the blockchain network generates a random wait time and goes to sleep for that specified duration.
- The one to wake up first – that is, the one with the shortest wait time – wakes up and commits a new block to the blockchain, broadcasting the necessary information to the whole peer network
- The same process then repeats for the discovery of the next block.

Proof-of-Elapsed-Time

- The POET network consensus mechanism needs to ensure two important factors:
  - First, that the participating nodes genuinely select a time that is indeed random and not a shorter duration chosen purposely by the participants in order to win, and
  - Second, the winner has indeed completed the waiting time.

Proof-of-Elapsed-Time

- The POET concept was invented during early 2016 by Intel.

- It offers a readymade high tech tool to solve the computing problem of "random leader election."

Hyperledger Fabric : PBFT

- Practical byzantine fault tolerance (PBFT) is a replication algorithm to tolerate byzantine faults (Miguel and Barbara, 1999).

- Hyperledger Fabric (hyperledger, 2015) utilises the PBFT as its consensus algorithm since PBFT could handle up to 1/3 malicious byzantine replicas.

Ripple

- Ripple (Schwartz et al., 2014) is a consensus algorithm that utilises collectively-trusted subnetworks within the larger network.
- In the network, nodes are divided into two types: server for participating consensus process and client for only transferring funds.
- In contrast to that PBFT nodes have to ask every node in the network, each Ripple server has a Unique Node List (UNL) to query.

Ripple

- UNL is important to the server. When determining whether to put a transaction into the ledger, the server would query the nodes in UNL.
- If the received agreements have reached 80%, the transaction would be packed into the ledger.
- For a node, the ledger will remain correct as long as the percentage of faulty nodes in UNL is less than 20%.

Consensus: A Comparison

Table 2 Typical consensus algorithms comparison

Property	*PoW*	*PoS*	*PBFT*	*DPOS*	*Ripple*	*Tendermint*
Node identity management	Open	Open	Permissioned	Open	Open	Permissioned
Energy saving	No	Partial	Yes	Partial	Yes	Yes
Tolerated power of adversary	$< 25\%$ computing power	$< 51\%$ stake	$< 33.3\%$ faulty replicas	$< 51\%$ validators	$< 20\%$ faulty nodes in UNL	$< 33.3\%$ byzantine voting power
Example	Bitcoin	Peercoin	Hyperledger Fabric	Bitshares	Ripple	Tendermint

A COMPARISON OF SOME WELL-KNOWN BLOCKCHAIN SYSTEMS

Platform	Network Type	Purpose	Prog. Language	Consensus Mechanism	Hash Functions	Signatures	Application
Bitcoin	Public/ Private permission -less	B2B,B2C operations	Golang, C++	PoW	SHA256, RIPEMD160	ECDSA, Multi-Signature	Government, financial, audit trails etc.
Ehereum	Public/ Private permission -less	B2C business	Solidity, Serpent ,LLL	PoW(PoS- in future)	SHA256, Ethash, RIPEMD160	ECDSA	banking, commodity trade finance, supply chain mang., insurance etc.
Hyperledger Fabric	Private, permission ed	B2B business	Golang, Chaincode written in Kotlin, Java	PBFT	SHA 2	ECDSA	Supply chain for pharmaceuticals, trade financing, smart energy etc.
MultiChain	Private, permission ed	B2B operations	Python, C#, JavaScript, PHP,Ruby	PBFT	SHA256	ECDSA	Financial transactions, e-commerce etc.
Litecoin	Public/ Private permission -less	B2B,B2C operations	Golang, C++	PoW	SHA-256, SCrypt	ECDSA, Multi-Signature	Banking, financial services etc.
BigchainDB	Public/ Private permissionl ess	B2B operations	SQL, NoSQL	BFT, federation with voting permissions	SHA3-256	Ed25519, EdDSA	Intellectual property, human resources, identity verficatio, supply chain, land registry etc.
Quorum	Private permission ed	B2B operations	Golang, Solidity	Majority voting, on-demand creation	SHA3-512	ECDSA	Banking, financial, insurance services etc.

Proof of X: Attacks

- nothing-at-stake attack: A miners are incentivized to extend every potential fork. Since it is computationally cheap to extend a chain, in the case of forks, rational miners mine on top of every chain to increase the likelihood of getting their block in the right chain.
- grinding attack: A miner re-creates a block multiple times until it is likely that the miner can create a second block shortly afterwards.
- long-range attack: An attacker can bribe miners to sell their private keys. If these keys had considerable value in the past, then the adversary can mine previous blocks and re-write the entire history of the blockchain.