GLOBAL X ETFs RESEARCH

Proof of Work vs. Proof of Stake: Why Their Differences Matter

Authored by:
Roberto de Isidro
Research Analyst
& Erik Anderson
Research Analyst

Date: October 5, 2022
Topic: Digital Assets

Editor's Note: Please see the glossary at the end for all terms highlighted in **sea green** found in the order that they appear.

The consensus method is arguably the most crucial building block of distributed ledger networks because it defines how individuals reach agreement in a global and permissionless system. A key component of consensus is the Sybil resistance mechanism, as it protects the network against attacks. Proof of Work (PoW) and Proof of Stake (PoS) are the biggest Sybil resistance mechanisms.

While they serve the same purpose, PoW and PoS have significant differences in design that dictate a network's throughput, security characteristics, level of decentralisation and energy consumption. In this report, we break down why a PoW network might be more challenging to attack than a PoS network, but also why PoS offers higher scalability, adequate security, and potentially a more compelling economic model.

Key Takeaways

- Coordination of distributed ledger network participants and ensuring confidence in network security falls to consensus mechanisms, where majority rules.
- PoW and PoS are not consensus mechanisms, but they are important components of how a network derives consensus. They play a key role in determining a network's security, decentralisation, and scalability.
- In our view, PoW can offer more robust security, whereas PoS' scalability makes it more suitable for powering an asset as a medium of exchange, giving it the potential to provide a superior economic model for users and investors.

Consensus Mechanisms Coordinate Nodes and Ensure Network Security

Distributed ledger networks like Bitcoin, Ethereum, and Cardano are open for anyone to join, and have no overarching authoritative figure. However, these networks still need a system to ensure they are functioning properly and that they remain trustworthy. This system is manifested in consensus mechanisms, which coordinate the thousands of decentralised machines operating on the network to ensure that the shared ledger is secure.

Consensus ensures that all participants share an identical copy of the ledger. This is made possible by establishing rules that govern how a blockchain's nodes determine the validity of transactions and blocks on the network. Consensus mechanisms are fundamental to a blockchain's security because they reconcile the differences between honest participants and bad actors.

CONSENSUS RECONCILES THE DIFFERENCES BETWEEN PARTICIPANTS
Source: Global X ETFs.

Double spending, a risk unique to digital currencies, is the most common issue that illustrates the importance of consensus to a blockchain's security. As the name implies, double spending occurs when an individual attempts to use a coin or token more than once. This scenario is problematic because it creates inconsistencies between transactional records and account balances on the shared ledger, rendering the token in question valueless.

Consider the example of a user who owns 1 bitcoin (BTC) and attempts to spend it. The transaction goes into a pool of unconfirmed transactions which miners compete to arrange into a block. Once a block is proposed and a majority of the miners in the network agree that its component transactions are valid, the block is posted to the blockchain. Time-stamped and inextricably linked to all previous blocks and transactions, the ledger is updated and cryptographically secured. If the user attempts to spend the same 1 BTC in a second transaction, the miners in the network would immediately identify the transaction as invalid, recognising that a majority of the network already came to consensus on the validity of first transaction.

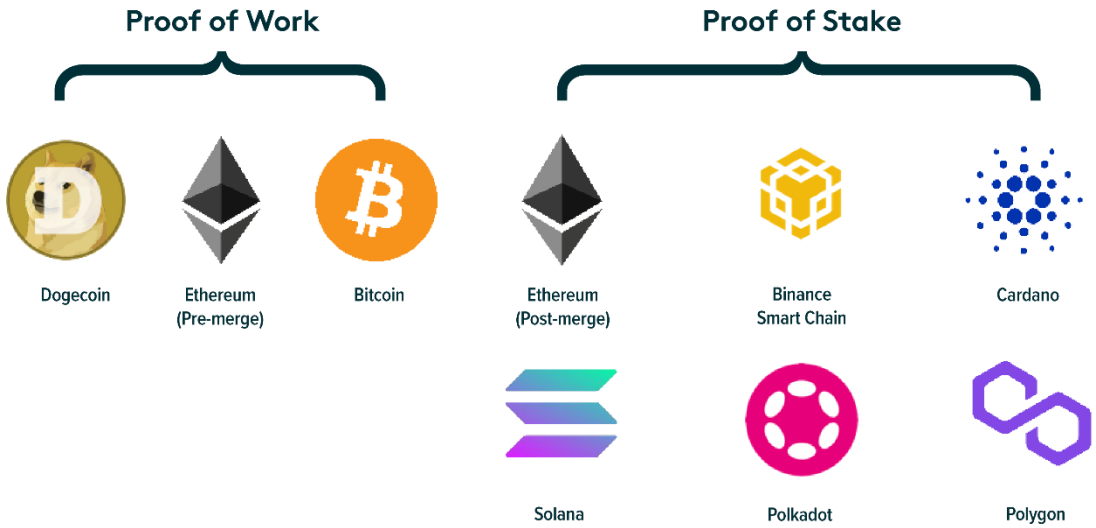
PoW and PoS Breakdown: The Leading Sybil Resistance Mechanisms

Consensus mechanisms are composed of numerous features, **including information propagation algorithms**, **chain selection algorithms**, and Sybil resistance mechanisms. Proof of Work and Proof of Stake are types of Sybil resistance mechanisms

A Sybil resistance mechanism protects the network against Sybil attacks in which an attacker seeks to gain control over the network by amassing a majority of the network's voting power. With that power, the attacker would be able to censor transactions and even potentially bring the network to a halt. To prevent Sybil attacks, Sybil resistance mechanisms impose significant logistic and financial hurdles that make attacking a blockchain an extremely expensive and risky endeavour. These hurdles serve as economic incentives that promote compliant behaviour and reprimand malicious activity.

THE SYBIL RESISTANCE MECHANISM SECURING TODAY'S TOP BLOCKCHAINS

Sources: Global X ETFs with information derived from: CoinMarketCap. (n.d.). Top blockchain assets sorted by market cap Accessed on September 20, 2022.



Proof of Work is a mechanism where nodes, called mining rigs, compete to solve a mathematical problem. The solver has the right to propose a block for validation and claim a block reward if the network agrees on the validity of the proposal. For example, the Bitcoin network currently issues 6.25 new BTC per block created, which happens approximately every 10 minutes.[1] Mining rewards are proportional to a user's share of the network's computational power dedicated to solving new blocks, known as the **hash rate.** Miners typically use specialised hardware designed to mine as efficiently and profitably as possible. To incentivise good behaviour, miners risk forfeiting potential rewards and incurring hardware and electricity costs if they propose blocks with invalid transactions.

With Proof of Stake, validators lock up or "stake" assets in a smart contract as an attestation of good intentions when validating transactions and proposing blocks. PoS uses a system where blocks are produced at defined intervals and the right to propose a block is assigned to validators randomly. This means that a validator's accrual of block rewards is proportional to their share of the network's total staked tokens. Bad actors risk having their staked tokens slashed or even eliminated, depending on the network's rules. Because participants' voting power depends on their share of the network's total stake, a higher amount of staked tokens by honest actors makes it more expensive for bad actors to accumulate voting power. the result is greater network's security.

SYBIL RESISTANCE MECHANISM OVERVIEW

Source: Global X ETFs with information derived from: CoinMarketCap. Dominance data [Data set]. Accessed on August 30, 2022.

Mechanism	Reward mechanism	Reprimand for malicious actors	Market dominance	Market dominance post-Ethereum merge
PoW	The protocol gives assets to the solver of the mathematical problem. The more mining power, the more likely a user is to solve it.	Energy and logistical costs	60%	40%
PoS	A user locks assets in a smart contract as an attestation of good intentions.	A bad actor's assets may be eliminated.	14%	34%

Note: Tokens built on top of layer 1 blockchains like ERC-20 tokens are not included in market dominance calculations. The Ethereum Merge marked the chain's transition from Proof-of-Work to Proof-of-Stake and was executed on September 15th, 2022.

Security: PoW Tougher to Attack, but PoS Can Be Easier to Recover

We can break down a network's resilience to attacks into two main factors: what it costs to attack the network and the network's ability to respond to an attack effectively. For a PoW chain like Bitcoin, an attacker would need to amass 51% of the network's computing power, which would require aggregating huge amounts of specialised mining hardware and electricity. For a PoS network, an attacker would have to acquire a large amount of the network's staked tokens. In a rough, back-of-the-envelope calculation, using Bitcoin's current hash rate and market capitalisation, we estimate that the market value of 51% of tokens is roughly 5 times greater than the value of the hardware and electricity generating 51% of the Bitcoin networks hashpower.[2]

However, attacking a PoW network presents significant logistical challenges that PoS does not, as the attacker would have to find a way to acquire and power a majority of the network's devices. In Bitcoin's case, the network currently consumes 0.42% of the world's annual electricity production; therefore, an attacker would need access an amount of energy comparable to Pakistan's energy consumption to power the mining hardware.[3] It is impossible to say with complete certainty, but it's logical to assume that the hurdles associated with amassing mining hardware and finding enough electricity would make attacking a PoW network of this scale more challenging despite the higher base cost of attacking a PoS network.

In the unlikely scenario that an attacker was able to amass a majority of the voting power in a PoW system, however, recovering the network would be an incredibly demanding undertaking. Because a successful attack would allow the attacker to censor all transactions, honest miners would no longer accrue block rewards. Without these rewards, miners would be economically disincentivised from using electricity to run their mining rigs. By turning off their now unprofitable miners, the attacker's share of the networks hashpower would inflate, cementing the attacker's control. To regain control of more than 50% of the network's hash power, a new contingent of honest miners would need to come online while potentially operating at a loss. Due to the scale of social coordination, logistical complexity, altruism required and the difficulty to identify the attacking party, recovering the network from a Sybil attack would be a significant challenge.

Conversely, PoS chains derive their security from within the network, meaning the staked tokens used to secure the network are registered to the network and are visible to all participants. This feature makes it comparatively easier to identify an attacker, arrest control of the network from them, and punish them financially for acting maliciously. As an added security measure, it is possible to **fork** a chain to create a

new one, where the attacker wouldn't hold any tokens and where normality can be restored. While this solution would go against the no-intervention ethos of cryptocurrency, it can be an effective last-resort option in a black swan event.

SECURITY OVERVIEW

Source: Global X ETFs .

Mechanism	Where it derives security from	Cost of attack	Recovery upon attack	Targeted node attacks
PoW	Hash power from mining hardware	Hardware, energy, and logistical hurdles	Needs social coordination, energy and hardware.	Less vulnerable
PoS	From the assets locked in a smart contract.	A large percentage of the total assets staked.	Easier to recover the network upon attack because it is possible to fork the chain and slash the attacker.	May have undesirable consequences, such as stake being slashed.

Decentralisation: There's No Clear Winner, but PoS Is More Accessible

Decentralisation is critical because it imparts blockchains with trustlessness, censorship resistance, and equal access. It refers to how dispersed the decision-making power is in a network, but it is not an exact science, and it can be tricky to quantify. Decentralisation is largely a product of the number of nodes a network has and how equal the playing field is to run those nodes.

PoW networks typically have no limit on how many users can participate in mining. Among them, large entities can amass a significant amount of the mining hash rate, which can make the barrier to entry prohibitive. Economies of scale have a significant effect on PoW mining. To run a node profitably, mining rewards must exceed operating costs, and if profitability is great enough, large mining operations become attractive undertakings. This is because enterprise-scale mining operations are able to minimise their average energy cost per miner, partner with suppliers of the most advanced and competitive mining hardware and purchase this hardware at much lower prices than the average hobbyist miner.

Compared to PoW networks, PoS networks impose higher barriers to run validating nodes. PoS networks may enforce a minimum amount of staked collateral, limit the number of validators, or have prohibitively expensive hardware requirements to participate in validation. However, depending on the network, individuals can still accrue staking rewards without running a node by delegating their coins to a validator. Delegating requires little technical knowledge and is accessible to anyone. In exchange for running a node, validators usually charge a small fee of 10% or less on staking rewards. Over time, we expect these costs to decrease as validator services become more competitive.

Contributing to a PoS network's security and benefiting from its rewards is widely accessible, and generally allows more people to participate profitably. It is important to note, however, that accessibility does not guarantee decentralisation, at it will depend on each individual network's architecture. For example, after Ethereum transitions to PoS it will have the most nodes with more than 422,000.[4] Conversely, a chain like Solana has under 2,000 validators.[5] While these chains both rely on PoS, Ethereum is much more decentralised than Solana.

Perhaps PoS' greatest concern about decentralisation is the following theoretical scenario. Over a long enough time horizon, large players could compound their staking rewards to amass a large percentage

of a network. This could give them an overwhelming influence over the network, or even the ability to take over the network.

DECENTRALIZATION OVERVIEW
Source: Global X ETFs.

Mechanism	How to contribute to consensus	Requirements to run a node	Positive feedback loops that can increase centralization
PoW	Running mining hardware	The initial hardware investment and access to cheap energy	Economies of scale benefit large corporations.
PoS	Running a validator node or delegating assets.	Hardware, minimum stake, and validator cap vary significantly depending on the protocol.	Compounding staking rewards and amassing an increasing percentage of the network's assets.

Scalability: PoS More Efficient in Block Selection and Energy

Block selection in PoS blockchains typically happens at predetermined time intervals, whereas PoW is more random and relies on difficulty adjustment algorithms. The increased predictability in PoS networks means that they can chose validators faster, which can increase throughput. Additionally, PoS blockchains are more suited for scaling solutions such as **shard chains** without sacrificing on security standards.

Energy-wise, PoS is exponentially more scalable than PoW. PoW deters attackers by imposing significant hardware and energy costs. Conversely, PoS' deterrence stems from the network's value, meaning PoS can secure a network with a fraction of the energy that PoW uses. The reason energy is such an important factor in scalability traces back to blockchain security. The cost to attack a distributed ledger network must outweigh the potential benefit of gaining control over the network. To maintain this property in a PoW network, mining power must increase proportionately to the value within the network which means that, the network's energy consumption must increase proportionately as well.

For a PoS chain, the value of staked assets on a PoS chain has the potential to increase proportionately to the value within the network. In other words, as the value of the PoS chain's native token increases, so does the economic security of the network. This property gives PoS a scalability advantage over PoW.

Lower energy requirements also mean that PoS has the potential to offer a superior economic model for the regular investor. Due to PoW miners' continuous expenditures on electricity and advanced hardware, it is significantly cheaper to compensate PoS validators for their services than PoW miners. Miners must sell their coins to offset their high energy costs, resulting in sell pressure. PoS validators do not have to sell their staked assets, as their operating costs are significantly lower. Additionally, investors can offset PoS assets' inflation rates by participating in staking.

After Ethereum transitions to PoS, its issuance rate is predicted to drop by 90%, significantly reducing ETH's inflation rate.[6] The reduction in energy consumption will be even more drastic. The Ethereum Foundation, a non-profit that supports the development of Ethereum, estimates Ethereum's migration to PoS will reduce its energy consumption 2000-fold.[7] For perspective, Ethereum is expected to use 80% of the energy Visa uses per transaction following its transition to PoS.[8] In contrast, Bitcoin uses a million times more energy per transaction than Visa.[9] The high energy costs associated with PoW spurred

regulators worldwide to crack down on certain mining operations, sometimes outright banning their activity, as China did in June 2021.

It is important to note that the PoW's bad-for-the-environment stigma might not be justified. Energy consumption can be measured easily by the hash rate and broad estimates of the energy required to run the hardware. But to determine carbon emissions associated with consumption requires knowing the exact energy mix, which is much difficult to determine given the lack of transparent data. Over the long term, we expect PoW mining's energy flexibility to be viewed as a key advantage that can help mining achieve carbon neutrality. Renewables and nonrival energy are the natural preferred choice for miners, as they are the cheapest sources of energy when available.[10] Added demand for and attention given to renewables from the crypto world might help accelerate the global energy transition, and the renewables industry could benefit from its economies of scale.

Another key energy plus for PoW is that miners can also be highly mobile. This attribute gives miners the ability to utilise energy that would otherwise be wasted. For example, in the U.S., ExxonMobil and Crusoe Energy piloted a program that runs data centres for miners on excess natural gas that would otherwise be released into the atmosphere. Reportedly, diverting this gas to mining "reduces carbon dioxide-equivalent emissions by as much as 63%."[11] In addition, the possibility exists where during periods of high energy demand, miners would be able to sell theirs to the grid, helping to address potential energy shortfalls.[12] Increasing total energy production capacity, and selling energy in periods of high demand can add robustness to an energy grid.

SCALABILITY OVERVIEW
Source: Global X ETFs.

Mechanism	Throughput	Energy consumption	Issuance rate
PoW	Block time depends on computational power, randomness, and a difficulty adjustment algorithm, making it less efficient.	Energy intensive. Security derives from it.	Block rewards must be high enough to encourage miner activity.
PoS	Block time is consistent and predetermined per protocol. More suited for scaling solutions such as shard chains.	Can be optimized to use less energy.	Staking rewards don't have to be as high as block rewards because staking costs are lower.

Conclusion: Pros and Cons to Both, but PoS' Scalability Is an Edge

Proof of Stake offers great scaling potential while possibly being more prone to Sybil attacks due to the absence of logistical hurdles. If under attack, it's easier to recover a PoS network. Certain PoS networks are more decentralised than PoW networks and vice versa. PoW mining has no entry requirements to run nodes other than hardware and energy costs, whereas PoS protocols can have prohibitive validator requirements. Participating in a PoW network's security may not be as accessible due to economies of scale, whereas anyone can delegate a PoS asset and participate in consensus. In the end, PoW and PoS have trade-offs, but PoS's edge is scalability.

In our view, PoS' scalability makes it a better choice to power a medium of exchange. To onboard a growing number of users, blockchains require sufficient throughput to meet transactional demand and energy consumption that doesn't bottleneck growth. PoS can also offer a more favourable economic model and it's more accessible to participate in network security. For investors, it's important to remember that the performance of a blockchain's native asset will depend on several factors beyond

their Sybil resistance mechanism. For additional information about what to consider when investing in digital assets please see The Case for Digital Assets in a Portfolio, and An Investor's Guide to Smart Contract Blockchains.

Footnotes

1. Gavinandresen, Jgarzik, & Sipa. (n.d.). *Bitcoin code.* Source Forge. Accessed on September 20, 2022 from https://sourceforge.net/p/bitcoin/code/1/tree//trunk/main.cpp
2. Cost of attacking a PoS chain as a % of market cap / Cost of attacking a PoW chain as a % of market cap.; Cost of attacking a PoS chain = % coins staked (assuming 60%, a mid-point between Polkadot and Solana) Ignores the price increase effect buying a token majority would have.; Cost of attacking a PoW chain as a % of market cap = Cost per device * worker number)/share of the pool = $27 Billion ≈ 6% of the market cap of BTC Calculation based on the stats of https://slushpool.com/en/stats/btc/.; Cost per device approximated from https://minerdaily.com/2021/how-much-does-it-cost-to-mine-a-bitcoin-update-may-2021/
3. University of Cambridge Judge Business School. (2022). *Cambridge Bitcoin Electricity Consumption Index*. Cambridge Centre for Alternative Finance. Accessed on September 8, 2022 from https://ccaf.io/cbeci/index/comparisons
4. Beaconcha.in. (n.d.). *Open source Ethereum explorer.* Accessed on September 8, 2022 on from https://beaconcha.in/
5. Solana. (n.d.). *Validators.* Accessed on September 8, 2022 from https://solana.com/validators
6. Ultra Sound Money. (n.d.) *Merge soon.* Accessed on September 8, 2022 from https://ultrasound.money/
7. Beekhuizen, C. (2021, May 18). Ethereum's energy usage will soon decrease by ~99.95% [Blog post]. *Ethereum Foundation Blog.* https://blog.ethereum.org/2021/05/18/country-power-no-more
8. Platt, M., Sedlmeir, J., Platt, D., Xu, J., Tasca, P., Vadgama, N., & Ibañez, J. I. (2021). Discussion paper series: Energy footprint of blockchain consensus mechanisms beyond proof-of-work. *University College London Centre for Blockchain Technologies.* http://blockchain.cs.ucl.ac.uk/wp-content/uploads/2021/11/UCL_CBT_DPS_Q32021_updated-2.pdf
9. Ibid.
10. Lazard. (2020, October). *Lazard's levelized cost of energy analysis – version 14.0.* https://www.lazard.com/media/451419/lazards-levelized-cost-of-energy-version-140.pdf
11. Wright, T. (2022, March 24). ExxonMobil is using excess natural gas to power crypto mining: report. *Cointelegraph.* https://cointelegraph.com/news/exxon-mobil-is-using-excess-natural-gas-to-power-crypto-mining-report
12. Wright, T. (2022, August 3). Riot Blockchain's Bitcoin mining productivity dropped 28% yoy amid record Texas heat. *Cointelegraph.* https://cointelegraph.com/news/riot-blockchain-s-bitcoin-mining-productivity-dropped-28-yoy-amid-record-texas-heat

Glossary

Information propagation Algorithm: The algorithm a distributed ledger uses to broadcast information such as transactions and blocks through the nodes in the network to update the ledger.

Chain Selection Algorithm: An algorithm used to decide which chain is the "correct" chain. Ethereum and Bitcoin currently use the "longest chain" rule, which means that whichever blockchain is the longest will be the one the rest of the nodes accept as valid and work with.

Hash rate: An estimate for the total computational power securing a PoW network at a point in time. It is measured as the number of hashes per second that all the miners in the network are computing in aggregate. The Bitcoin network hash rate reached a peak of approximately 180 quintillion hashes per second in 2021.

Fork: A blockchain that has been split into two versions with a shared history due to a disagreement or protocol upgrade.

Shard chains: A data architecture solution that consists of multiple chains of data. The computational and/or storage load of a network with shard chains is spread between the shards.

This document is not intended to be, or does not constitute, investment research as defined by the Financial Conduct Authority.

The value of an investment in ETFs may go down as well as up and past performance is not a reliable indicator of future performance.

Trading in ETFs may not be suitable for all types of investors as they carry a high degree of risk. You may lose all of your initial investment. Only speculate with money you can afford to lose. Changes in exchange rates may also cause your investment to go up or down in value. Tax treatment depends on the individual circumstances of each client and may be subject to change in the future. Please ensure that you fully understand the risks involved. If in any doubt, please seek independent financial advice. Investors should refer to the section entitled “Risk Factors” in the relevant prospectus for further details of these and other risks associated with an investment in the securities offered by the Issuer.