Proof-of-Work vs. Proof-of-Stake

Securing the chain

August 2022

Table of contents

1.

Introduction

At the heart of every blockchain lies a protocol that defines how pseudonymous individuals reach consensus in a globally distributed network. Arguably the most critical component of a blockchain's consensus method is its Sybil resistance mechanism, such as Proof-of-Work (PoW) or Proof-of-Stake (PoS). As its name implies, Sybil resistance mechanisms protect blockchain networks against Sybil attacks, including spam nodes and 51% attacks. These mechanisms also regulate the selection of a block author and incentivize network nodes to behave honestly.

A rivalry exists between PoW and PoS among crypto communities that surfaces key questions of network security, sustainability, barriers to entry, and decentralization. Though many claim absolutely which Sybil resistance mechanism is best for blockchain networks, the reality is not black and white. Neither Sybil resistance mechanism is perfect. Instead, it is essential to understand the trade-offs between each before concluding on the optimal choice for a particular blockchain network.

This report examines the nuances behind consensus methods and their Sybil resistance mechanisms, describes trade-offs between PoW- and PoS-based systems, and compares key metrics for both mechanisms. Moreover, it makes the case that a given blockchain's utility – hard money or smart contracts, for example – determines which characteristics a network should optimize for. The design choice is often referred to as the "blockchain trilemma," which argues that a blockchain network must balance trade-offs between decentralization, scalability, and security. A highly scalable network, for example, is said to optimize scalability at the expense of decentralization and network security. These choices also impact which Sybil resistance mechanism a particular protocol should utilize. Though other Sybil resistance mechanisms exist, including Proof-of-Authority and Proof-of-Spacetime, this note solely focuses on PoW and PoS. Currently, PoW and PoS make up the lion's share of the major Layer-1 (L1) blockchain networks by market capitalization.

2.

The anatomy of blockchain protocols

Every blockchain follows an underlying protocol that determines its block selection process, how network nodes validate transactions, transaction finality characteristics, supply issuance, supply distribution, and what determines the “true” state of the network. Furthermore, the blockchain protocol provides an incentive structure for network participants to behave honestly with each other while discouraging bad actors.

The Sybil resistance mechanism establishes a cost that disincentivizes a bad actor from maliciously taking over as the sole arbiter of consensus. The consensus method describes how nodes coordinate to agree on the validity of transactions and the state of the network. Examples of consensus methods include Nakamoto consensus and Byzantine Fault-Tolerance.

Sybil resistance mechanism

Sybil resistance mechanisms are compatible with various consensus methods, such as Nakamoto consensus and Practical Byzantine Fault-Tolerance (PBFT), but they are not sole descriptors for consensus. Instead, these mechanisms establish rules that nodes must follow to append data to a blockchain. One of their core functions is to deter Sybil attacks.

A Sybil attack is an exploit against an online network whereby a small number of entities (as few as one) attempt to take control of the whole network by leveraging multiple accounts, nodes, or computers. On social media platforms, a user can generate multiple accounts and spam the network, effectively "taking over" the conversation. On a blockchain, bad actors might run multiple nodes to achieve an overwhelming influence on the network.

In Sybil attacks, dishonest nodes try to out-vote honest nodes on the network by creating enough “Sybil identities.” The word "Sybil" comes from a case study about a woman named Sybil Dorsett, a pseudonym for Shirley Ardell Mason, who received treatment for dissociative identity disorder, or multiple personality disorder.[1] Once an attacker creates enough Sybil identities to disproportionately influence a crypto network, they can refuse to receive or transmit blocks, effectively preventing other users from the network.

The most commonly-known Sybil attack in the crypto space is the "51% attack," where attackers take over most of the network computing power, commonly referred to as “hash rate.” In such cases, they may theoretically influence the ordering of transactions, prevent the confirmation of new transactions, and double-spend their cryptoassets. Resistance to these attacks is essential for a well-functioning, decentralized blockchain.

PoW and PoS are economic deterrents to Sybil attacks because they require users to expend energy or lock-up collateral to participate in network validation. The crux of a Sybil resistance mechanism is that it requires each validator or miner to have "skin-in-the-game" to participate in a decentralized, cryptographic system. Sybil resistance mechanisms are also known as “block author selectors” because they designate a validator or miner to add a block to the chain.[2] Readers should note that these mechanisms are not cures against Sybil attacks; instead, they make it impractical for an attacker to carry out a Sybil attack successfully by:

a. *Encouraging participants to reach a consensus on the state of the blockchain through a competitive process, such as mining or staking;*

b. *Punishing bad actors that try to stall the network from reaching a consensus; and*

c. *Rewarding some or all participants for behaving honestly and coming to a consensus (e.g., block subsidies, transaction fees).*

Figure 1

Sybil Resistance Mechanism Overview

Sybil Resistance Mechanism	Competition	Method	Penalty for Misbehavior	Market Dominance
Proof-of-Work (PoW)	Computational work	Solve mathematical puzzles using computational hardware	Proposing an invalid block results in wasted time, energy, and money	58%
Proof-of-Stake (PoS)	Financial stake	Lock up funds in a smart contract	The protocol can destroy a validator's stake or bar them from participating in consensus if they fail to step up when called upon or sign invalid blocks	12%
Other*	-	-	-	30%
Non-PoW/PoS Sybil resistance mechanism examples, including but not limited to:				
Proof-of-Authority (PoA)	Reputation	Validators undergo authentication to participate	The protocol can exclude nodes that cheat or go offline from consensus and the consortium of approved validators can impose other penalties	
Proof-of-Space (PoSp)	Disk space	Solve mathematical puzzles by dedicating disk space	The protocol can destroy a validator's stake or bar them from participating in consensus if they fail to step up when called upon or sign invalid blocks	
Proof-of-Elapsed Time (PoET)	Fair lottery	Each node must wait for a randomly chosen period; the first to complete the designated waiting time wins the new block	Since PoET is designed for permissioned blockchains, the protocol's leaders can boot any misbehaving nodes from the network	
Proof-of-Burn (PoB)	Coin burn	Burn coins to win the right to propose a block	Proposing an invalid block results in wasted time and money	

Source: Kraken Intelligence, CoinGecko
*Note: The market dominance figure for "other" includes tokens, which are cryptoassets built on top of existing L1 blockchains. Tokens do not have their own native blockchain and must follow the protocol rules of the chain they operate on.

Consensus method

Blockchain consensus methods mitigate the challenge of achieving consensus in a globally distributed, digital world by enabling users to validate entries into the blockchain ledger, help synchronize data, and bolster the network's security. Such methods must ensure that all network participants can agree on a single source of "truth," even if some nodes fail; put differently, they must be Byzantine Fault Tolerant (BFT). The concept of BFT derives from the Byzantine Generals' Problem, a game theory problem that describes the difficulty decentralized parties have in achieving consensus without relying on a trusted central party. Initially conceived in 1982 as a logical dilemma, a group of Byzantine generals must perfectly coordinate an attack with the added challenge that they cannot directly communicate with each other.

A Byzantine army is besieging an enemy city and has the territory surrounded. The army splits into several divisions, each commanded by a different general. After observing the enemy, they must agree on a joint action plan. The generals can win if they all attack simultaneously but will lose if they strike at different times. However, the generals can only communicate with each other by messenger. Some of the generals may be traitors, or any messages sent or received could have been intercepted or deceptively sent by the enemy to prevent the honest generals from reaching a consensus. Thus, the Byzantine Generals Problem highlights a common problem among distributed networks: *can independent participants of a distributed network form an agreement?*[3]

In other words, the consensus method allows network participants to propose and confirm transactions and agree on the state of the distributed ledger in near real-time. PoW and PoS choose a block author and defend against Sybil attacks but do not, in and of themselves, describe a blockchain's consensus method. Instead, a consensus method combines a Sybil resistance mechanism with a chain selection rule, which decides which is the valid version of the blockchain.

Many L1 blockchains, including Bitcoin and Cardano, use the "longest chain" rule, known as Nakamoto-style consensus, meaning that nodes will accept whichever blockchain is the longest as the true state of the transaction ledger. For PoW chains, the chain's total cumulative PoW determines the longest chain. Conversely, PoS chains define the true state of the network as the chain with the most votes. Another common chain selection rule used by L1 blockchains, including Ethereum and Conflux, is the "heaviest chain rule," a variation of the longest-chain rule that includes **orphan blocks** or blocks that were previously authored within the blockchain network but were not accepted at the time. This rule allows a peer-to-peer network of distributed nodes to achieve BFT because each node unambiguously agrees to follow a source of truth derived from a verifiable set of records.

Before Bitcoin, distributed cryptographic systems could only achieve up to 33% fault tolerance utilizing a BFT-style consensus method. Transactions achieve finality in BFT-style, distributed networks when 66% of the aggregate financial stake in the network reaches an agreement. In other words, anyone that can accumulate more than 33% of the total value staked on the network can prevent users from finalizing transactions, reaching a consensus, and censor users.

Depending on the consensus method of the network, this could result in the network ceasing to produce blocks until it gets 66% agreement on the block or continuing to produce blocks but not reaching a final agreement on the content of the blocks. Satoshi's invention of Nakamoto-style consensus incentivized network participants to act honestly in the absence of trust and increased the theoretical fault tolerance of distributed systems from 33% to 50%, effectively deterring Sybil attacks that could lead to double-spending.

Transactions finality is always "probabilistic" on Nakamoto-style consensus protocols because nodes come to a consensus around the longest chain. The node that proposes the transactions that go into a particular block is not predetermined like in BFT-style protocols, meaning it is never 100% guaranteed that a transaction is irreversible as a longer chain could exist. It is considered "probabilistic" because the probability of a transaction reversal decreases as a chain gets longer, providing near certainty in the transaction's irreversibility after a certain period has passed. For instance, most network participants typically wait for 40-60 confirmations for probabilistic finality on Dogecoin and six

confirmations for Bitcoin. Confirmations on a blockchain refer to the validation of blocks, meaning that a transaction receives another confirmation every time miners add a block to the chain. In these networks, this amount of confirmations makes it improbable to reorganize the blockchain, but it is never theoretically impossible.

On the other hand, transactions on BFT-style networks are "deterministic" because rules determine who can vote on a transaction and exactly how many votes are needed before everyone can agree the transaction is 100% final. Once a transaction achieves finality, there is no way a longer chain can exist, as there is no uncertainty in the process.

The success of Bitcoin and its pioneering PoW-based Nakamoto consensus method showed that decentralized networks could work and accrue value for users and network stakeholders by solving fundamental problems such as the Byzantine Generals Problem, Sybil resistance, and economic incentivization. Since then, thousands of blockchain networks have launched using similar mechanisms to deter Sybil attacks and achieve a consensus.

Figure 2

Blockchain Consensus Method Examples

Consensus Method (Examples)	Sybil Resistance Mechanism	Block Validation	Information Propagation	Chain Selection Rule	Transaction Finality	Incentive Structure	Fault-Tolerance
Nakamoto (Bitcoin, Litecoin)	PoW	PoW verification	Gossip	Longest-chain	Probabilistic	Block subsidy and transaction fees	50% computational power
Nakamoto-style, GHOST (Ethereum)	PoW (Ethash)	PoW verification	Gossip	Heaviest-chain	Probabilistic	Block subsidy and transaction fees	50% computational power
Nakamoto-style, chain-based PoS (Peercoin, Nxt, PoAct)	PoS	PoS verification	Gossip	Longest-chain	Probabilistic	Block subsidy and transaction fees	50% financial stake
Nakamoto-style, committee-based PoS (Ouroboros, Praos, CoA, Snow White)	PoS-based committee election	Proposer eligbility verification	Broadcast among committee	Longest-chain	Probabilistic	Block subsidy	50% financial stake
BFT-style PoS—Alogrand (Alogrand)	PoS-based committee election	Proposer eligibility verification	Broadcast among committee	BFT (adapted Byzantine agreement)	Deterministic	Block subsidy	33% financial stake
BFT-style PoS—Tendermint (Cosmos Hub)	PoS-based round robin	Proposer eligibility verification	Broadcast among committee	BFT (adapted distributed ledger system)	Deterministic	Block subsidy	33% financial stake

Source: Kraken Intelligence, Protocol whitepapers

At a high level, some popular blockchains utilize the following consensus methods:

- **Cardano**—Ouroboros, the blockchain protocol **implemented** on Cardano, utilizes Nakamoto-style consensus similar to Bitcoin, where nodes follow the "longest chain rule." However, unlike Bitcoin's PoW mechanism that uses hash power or energy to create a new block, Ouroboros implements PoS, which uses the network's native coin (i.e., ADA) to influence how often the block selection mechanism chooses a validator node to create a new block. Cardano's use of Nakamoto consensus and PoS differentiates it from other major 3rd-generation protocols, which often combine PoS with BFT-style consensus protocols. Instead of following the longest-chain rule, BFT-style consensus protocols come to a consensus in a quorum vote, where a ⅔ majority is required to confirm a block.
- **Ethereum**—The Ethereum blockchain's consensus method also uses Nakamoto-style consensus combined with Ethash, the blockchain's modified version of PoW. The Ethash PoW algorithm depends on generating and analyzing a large, frequently accessed dataset, known as a directed acyclic graph (DAG). Ethereum's chain selection rule is known as Greedy Heaviest Observed Subtree (GHOST), or the "heaviest chain rule."[5]
- **Ethereum 2.0**—The ETH 2.0 Beacon Chain uses a PoS-based consensus method called Casper the Friendly Finality Gadget.[6] Casper is a partial consensus method combining PoS and BFT-style consensus. The method inherited its core design from the PBFT consensus method while adding new mechanisms and simplifying several rules. This consensus method is similar to Nakamoto Consensus in that it defines the "true" chain as the chain with the most attestations.
- **Solana**—Tower BFT is the consensus method Solana utilizes on top of the innovative Proof-of-History (PoH) timing mechanism in conjunction with PoS. Because nodes in a distributed network cannot trust the timestamp on messages received from other nodes, distributed networks cannot form a consensus on the time and order in which events happen. Solana uses PoH to overcome this problem by establishing a cryptographically safe source of time throughout the network. PoH is a sequence of computations that provides a digital record to prove that an event occurred on

the network at any given time. At a high level, Tower BFT works in that when a node votes on a specific fork, they agree to lock themselves out of voting on an opposing fork for a period. As they continue to vote on the same fork, the time they are locked out rises exponentially until they reach a maximum lockout of 32 votes for the same fork. When nodes on the network hit this maximum vote lockout, they will earn inflation incentives.[7]

Though many blockchains have developed unique methods of achieving consensus and BFT, readers should carefully note the difference between a Sybil resistance mechanism and a consensus method. This understanding is critical in determining whether PoW or PoS is a superior model for blockchain design. Sybil resistance mechanisms work with a chain selection rule to form the consensus method that supports a functional blockchain. Furthermore, these Sybil resistance mechanisms have significant trade-offs that result in different desired outcomes for the functionality of a blockchain.

3.

Trade-offs

Proof-of-work (PoW): bridging the physical to the digital

One of the most popular Sybil resistance mechanisms used in crypto networks is PoW, a cryptographic proof in which one party (the miner) proves to other network participants (nodes) that they have solved a sufficiently complex problem that requires computational effort. Introduced in the 1990s to mitigate email spam, PoW involves the exertion of computational power to solve a moderately difficult and random "puzzle" to gain access to the resource, thus preventing frivolous use.[8,9] At the time, the goal of PoW was to require computers to perform a small amount of "work" before sending an email. This work would require trivial computing power for someone sending a legitimate email while creating high computational costs for those sending mass emails.

In PoW blockchains, miners must gather information and try to guess a solution to a cryptographic puzzle. Once miners solve the puzzle, they share their results with other nodes to verify their "work" before adding the block to the chain. Because miners must consume energy in the PoW process and nodes can easily verify any block's validity, malicious miners who try to add an invalid block waste time, energy, and resources. Conversely, the protocol rewards honest miners that successfully mine a valid block.

This mechanism incentivizes honest nodes to act in good faith while discouraging bad actors on the network. In short, PoW networks consume energy to maintain the continued functionality of the distributed blockchain ledger and fairly distribute the cryptoasset's supply without a centralized overseer. This PoW competition among miners comes with several benefits and considerations.

PoW Benefits

- PoW blockchains are battle-tested at scale since crypto protocols implemented the Sybil resistance mechanism throughout most of crypto history, securing billions of dollars worth of value for nearly a decade. Still, readers should note that PoW blockchains are not automatically impervious to hacks as smaller PoW blockchains, including Vertcoin, Verge, and Ethereum Classic, have experienced several successful attacks.
- Carrying out a 51% attack on an established PoW blockchain network, such as Bitcoin, Ethereum, Litecoin, or Dogecoin, requires so much computing power that it is meaningfully expensive; any attacker would spend more than they could earn to attack the network. This financial cost disincentivizes bad actors from behaving maliciously on the network and secures the blockchain.

Figure 3

Theoretical Requirements for 51% Attack on PoW Blockchains Using Bitmain ASICs

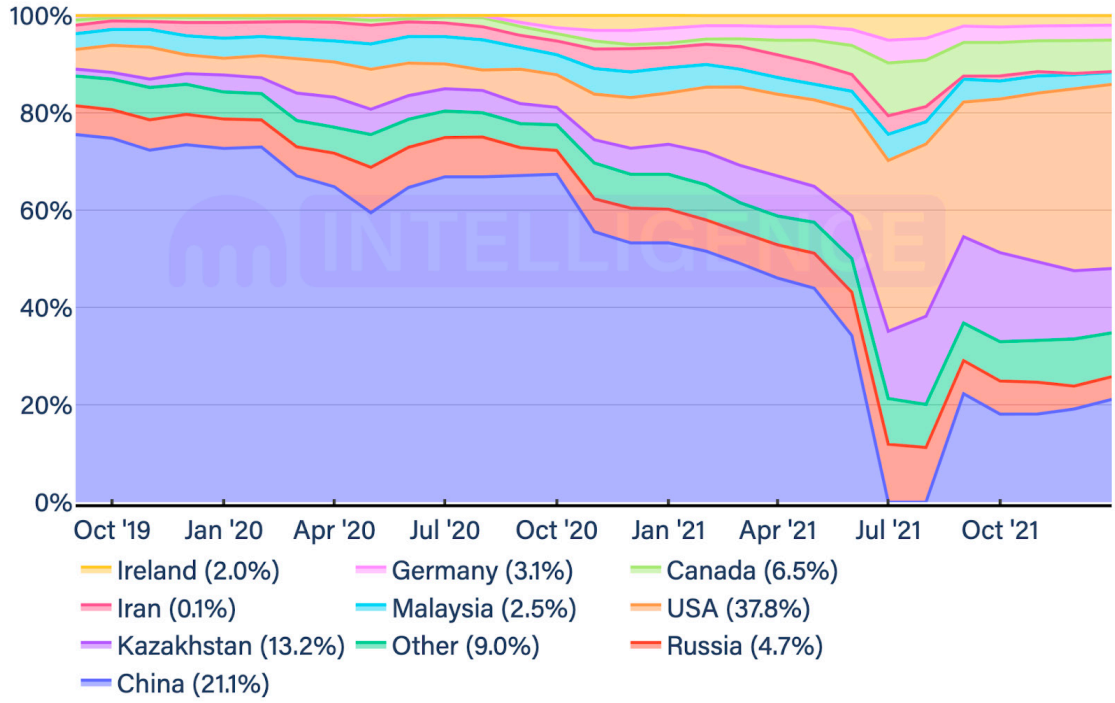
Individual Mining Equipment Specifications	**ASIC Model**	Bitmain Antminer S19				Antminer L7		Antminer Z15	Antminer D7	Antminer DR3
	Hashing Algorithm	SHA-256				Scrypt		Equihash	X11	Blake256r14
	Equipment Hashrate	95 TH/s				0.00905 TH/s		0.0000004 TH/s	1.286 TH/s	7.580 TH/s
	Equipment Cost	$3,990				$13,999		$7,999	$1,778	$1,999
	Power Consumption	3,250W				3,260W		1,510W	3,148W	1,410W
	Electricity Cost/Day*	$9.18				$9.21		$4.27	$8.89	$3.98
Cryptoasset Specifications	**Cryptoasset**	BTC	BCH	BSV	XEC	LTC	DOGE	ZEC	DASH	DCR
	Market Capitalization	$384.8B	$2.2B	$1.2B	$715.4M	$3.7B	$8.3B	$816.4M	$496.6M	$325.5M
	Hashrate	205 EH/s	1.15 EH/s	0.65 EH/s	0.32 EH/s	379 TH/s	329 TH/s	0.00897 TH/s	3,107 TH/s	95,178 TH/s
	Hashrate (%share)	98.93%	0.55%	0.31%	0.15%	0.00018%	0.00016%	0.000000004%	0.0015%	0.046%
51% Attack Requirements	**Hashrate**	207.2 EH/s	1.16 EH/s	0.66 EH/s	0.323 EH/s	382 TH/s	333 TH/s	0.00906 TH/s	3,138 TH/s	96,130 TH/s
	ASICs	2.16M	12.1K	6.8K	3.4K	42.3K	36.8K	21.6K	2.4K	12.7K
	Hardware Cost	$8.6B	$48.3M	$27.3M	$13.6M	$591.7M	$514.5M	$172.5M	$4.3M	$25.4M
	Electricity Cost/Day*	$19.8M	$111.1K	$62.8K	$31.2K	$389.2K	$338.5K	$92.0K	$21.7K	$50.5K

Source: Kraken Intelligence, Bitmain, Newegg
*Note: Energy costs assume a fixed cost of 11.77 cents per kWh, the average electric price a business customer in the U.S. pays for electricity as of June 2022.[10]

- Large intermediaries may have less influence on the governance of PoW-based cryptoassets, as evidenced by the failure of SegWit2x on Bitcoin in 2017.[11] Though most of the large exchanges and custodians supported the movement at the time, nodes did not implement the software upgrade due to a lack of network-wide consensus.[12] Should a similar situation emerge today on one of the larger PoS networks, custodians with large amounts of coin supply may influence protocol governance.
- PoW incentivizes miner operations to distribute geographically and organizationally, decentralizing PoW cryptoassets as a whole. This incentive stems from the fact that electricity, miners' highest variable cost, varies in price depending on location. Because miners constantly pursue lower energy costs and cheap energy exists in remote locations across the globe, mining operators also distribute their operations worldwide. Bitcoin, which houses most of the hash power of all PoW blockchains, is a fine example of this incentive structure. Figure 4 shows that this incentive structure caused a geographic centralization of mining on the network in its early years as China was abundant with cheap electricity. Nonetheless, miners have increasingly distributed internationally in recent years in search of cheaper options. Critics may argue that this decentralization of hash power was solely due to China's ban on mining in May 2021; however, data suggests the distribution began long before the crackdown. From September 2019 to May 2021, China's hash power dominance dropped from 76% to 44%. Since the ban, that figure has dipped further to 21%.

Figure 4

Distribution of Bitcoin Mining Hash Power by Country



Source: Kraken Intelligence, Cambridge Centre for Alternative Finance

- Incentive structure includes measures to prevent constant forking, while forking is not automatically discouraged by PoS systems. The "nothing at stake" problem occurs when a validator signs off on both sides of a fork to earn rewards on both blockchains, afflicting PoS protocols. In a PoS fork, pre-fork holders are presented with a financial incentive to stake the same amount of coins on both the original blockchain and the forked blockchain to increase their total returns. PoW networks like Bitcoin correlate security with hash power, so a fork would not necessarily maintain the hash power of the original network, and thus neither the security. This feature provides a high cost to forking on PoW systems that strongly discourages such an endeavor. Critics may argue that the existence of

merge mining, the process of mining two blockchains that use the same hashing algorithm at the same time, introduces the equivalent problem on PoW as nothing-at-stake does for PoS.[13] However, because a new PoW blockchain created from a hard fork would need to retain the same algorithm as the original blockchain for merge mining capabilities, the issue does not always arise. For instance, Bitcoin Gold and Ethereum Classic did not retain their respective SHA-256 and Ethash hashing algorithms following their respective 2017 hard forks.[14,15] Moreover, PoW blockchain forks that retain the same hashing algorithm as the original blockchain typically fall behind significantly in terms of hash power, as evidenced by historic blockchain forks such as Bitcoin Cash and Bitcoin SV. While Bitcoin Cash is one of the most successful Bitcoin hard forks ever, its hashrate of 1.12 EH/s falls -99.45% behind the 204.6 EH/s on its original chain, Bitcoin, and Bitcoin SV's hashrate of 0.66 EH/s is -41.1% behind Bitcoin Cash.[16]

- It is debatably harder to perform bribery attacks on PoW than on PoS due to the nothing-at-stake problem, which gives PoS validators a greater incentive to behave dishonestly. Bribery attacks rely on a bad actor successfully bribing enough validators or miners to work on specific blocks or forks so the colluding miner(s) or validator(s) can present arbitrary transactions as valid and have dishonest nodes paid to verify them. In a bribery attack, a bad actor sends a transaction, discretely builds an alternative chain based on the prior block until the transaction receives enough confirmations and the attacker's chain is longer than the valid chain, and then publishes the invalid chain as the new valid blockchain to reverse the transaction.[17,18] In a PoW system, a similar attack would require the attacker to bribe the majority of miners by hash rate. Since miners lose resources spent on computations if the attack fails, there are strong assumptions that the number of bribes is prohibitively high. Though bribery attacks are theoretically harder to conduct on an established PoW network, it is also impractical to conduct on a PoS network large enough to make it extremely expensive to attain enough validator votes for such an attack.

PoW Considerations

- Requires energy consumption to achieve Sybil resistance. This feature has spurred a debate on the carbon footprint of cryptocurrency networks.
- Smaller PoW blockchains with low hash power have low security and thus are prone to 51% attacks. Some larger PoW projects that have experienced 51% attacks in the past include Ethereum Classic, Verge, Bitcoin Gold, and Vertcoin.[19,20,21,22,23]
- Some argue that it is difficult for individual miners to continuously upgrade their hardware to compete effectively, eventually leading to a centralization of mining towards corporate players. Data shows that the top three mining pools in Bitcoin control over 52% of the current hash rate, suggesting a group effort among these organizations could theoretically attack the network successfully.[24] The pool selects transactions to put in the blocks that everyone in the pool is working on, receives the pool's mining rewards, and holds the assets until individual hardware operators withdraw them. However, it is worth noting that individual miners could stop contributing power to pools that show any sign of wrongdoing since it is not in their best interest, suggesting arguments for the dangers of mining pool centralization are theoretically unsound. Moreover, mining pool operators have a long-term stake in the Bitcoin network and little incentive to attempt an attack as they have a financial incentive to behave honestly. However, this is equally true in PoS networks as validators must hold the blockchain's native cryptoasset to stake.
- Since nodes can operate anonymously, blocking a malicious miner from participating in the network is impossible, and there is no way to confiscate their mining equipment for misbehaving. Bad actors on PoW networks only waste time, energy, and the funds used to attempt the attack, while the same attack on PoS can cause hackers to lose their stake and bar them from the validation process.
- PoW systems that follow Nakamoto-style consensus could encounter "selfish mining attacks," a deceitful endeavor where a miner or group of miners finds a new block and withholds it from the blockchain. First identified by Cornell researchers Emin Gün Sirer and Ittay Eyal in a 2013 paper, selfish mining attacks create a blockchain fork,

which the malicious miner(s) work on to get ahead of the original blockchain.[25] If the blockchain fork becomes longer than the original blockchain, the miner can introduce its newest block to the network and effectively overwrite the original blockchain with the blockchain fork. This attack alters the blockchain to allow the malicious miners to steal cryptoassets from other users or double-spend funds. Still, selfish mining attacks are theoretical as they have not occurred on a live blockchain.

- Some critics contend that PoW's trial-and-error architecture naturally entails a delay in block production, meaning that fees rise in times of congestion. However, this critique fails to understand what drives throughput. Block size and the number of bytes (and hence, transactions) that can fit into a block, primarily determines throughput, not the time between blocks. For example, a blockchain designed to produce one block per second with 1,000 transactions per block could have the same throughput as a blockchain that produces one block per minute that is large enough to fit 60,000 transactions. Moreover, the same critics may argue that material blockchain fees are unhealthy for a scalable network; instead, cryptoassets with zero transaction fees are preferable. Having fees is arguably healthy for a public blockchain system because it eliminates the spam and DDoS problem by making it costly to insert junk data. Fees also promote a competitive environment among validators, making it prohibitively expensive for single parties to attack a network successfully. Spam and DDoS attacks have historically plagued zero- and low-fee networks like Nano and Solana due to low barriers to entry when conducting a transaction, causing network nodes to lose synchronization.[26,27] These spam attacks have caused user transactions to fail while significantly decreasing overall transaction throughput. Furthermore, such events could cause users to lose confidence in projects with said vulnerabilities, causing an outflow of users and negative selling pressure on the cryptoasset.

Proof-of-stake (PoS): earning in a digital world

In PoS systems, the native coin stores value and voting power rather than just value as in PoW systems. Peercoin first implemented PoS in 2012 to create a blockchain network that achieved Sybil resistance in a BFT way while consuming a fraction of the energy.[28] Rather than relying on computers racing to generate the appropriate hash, the act of locking up coins, or staking, determines participation in a PoS protocol. This mechanism attempts to reduce the computational cost of PoW schemes by selecting validators in proportion to their quantity of staked holdings in the associated cryptoasset. Using a set of factors determined by the protocol, the PoS mechanism pseudo-randomly selects a validator node actively staking to propose the next block to the blockchain. When the mechanism elects a validator node, the node must verify the validity of the transactions within the block, sign it, and propose the block to the network for further validation. PoS-based blockchains come with notable benefits and considerations that differ from PoW.

PoS Benefits

- Achieving Sybil resistance requires virtually no energy consumption. For reference, Ethereum developers estimate that its transition to a PoS system will reduce energy consumption by more than 99.9%.[29] Moreover, thanks to the low energy requirement, less native coin issuance is required to incentivize participation in the validation process.
- PoS eliminates the need for validators to purchase and upgrade hardware continuously.
- Honest validators could decide to forcibly remove attackers from the network and destroy their staked cryptoassets, providing economic defenses against a 51% attack. For example, the Ethereum 2.0 protocol includes a "correlation penalty" where validators forfeit ETH rewards if they fail to participate when called upon, and the protocol destroys, or "slashes," their existing stake if they propose multiple blocks in a single slot or submit contradictory votes. The amount of ETH slashed depends on how many dishonest validators the protocol slashes around the same time. This penalty can result in the slashing of roughly 1% of a validator's stake if they are

penalized on their own or 100% of the validator's stake during a mass slashing event. The protocol imposes the penalty halfway through a forced exit period that begins with an immediate penalty (up to Ξ0.5) on day 1, the correlation penalty on day 18, and finally, ejection from the network on day 36. Furthermore, the dishonest node receives minor attestation penalties daily because they are present on the network without submitting votes.[30] However while PoS protocols such as Ethereum 2.0, Polkadot, Solana, and Cosmos, enforce a "slashing" penalty, some PoS protocols, including Cardano, Avalanche, and Algorand, do not include a slashing feature.

- The time it takes for PoS blockchains to choose a validator is faster and has less block variance than PoW mining competition, allowing for increased efficiency.
- Lower barrier to entry since the protocol only requires funds to participate in the block validation process, rather than warehousing, energy contracts, and specialized hardware as is required in PoW.

PoS Considerations

- Not as extensively tested as PoW, which has secured billions of dollars worth of value for nearly a decade. Particular implementations of PoS could introduce black swan attack vectors, decreasing the overall security of the blockchain.
- The initial supply distribution in PoS systems can introduce voter concentration depending on the free market accessibility to initial supply distributions.
- PoS blockchains using BFT-style consensus reduce fault tolerance from 50% to 33%, as Nakamoto-style consensus is critical in resisting 51% attacks. Suppose a validator or a coordinated set of validators own more than 33% of the financial stake in these blockchains. In that case, they can attack the network by reverting transactions, censoring transactions, or stopping network participants from reaching a consensus.

- PoS is potentially more vulnerable to centralization than PoW because capital ownership determines network control, which is more centralized than labor and cheap energy. In a BFT-style PoS network worth $100 billion, where users stake 10% of tokens, any party able to allocate more than $33 billion (>33%) can take over the network by locking their assets in a staking contract. In a PoW network using Nakamoto-style consensus, attacks require most of the mining equipment and labor. Attacking a network with $10 billion of security would require acquiring specialized hardware, space, and energy contracts to mine at a larger scale than the entire network and deploy the labor to execute the attack. If such an attack were underway, the entire network would likely become aware of the immense demand for mining equipment and electricity ahead of time. Because carrying out a 33% attack on a PoS network requires holding 33% of staked tokens, those with large amounts of coins, such as early adopters, exchanges, and custodians, can overwhelmingly influence the rules of the network. They can also accumulate more of the coin via staking, causing a positive feedback loop that can increase centralization. There are already examples of exchanges used to influence PoS networks, including when Tron founder Justin Sun worked with several exchanges to obtain influence on the Steem network by voting with their user funds in favor of his proposal.[31] The figure below analyzes some major blockchain's and the minimum number of validators required for a 33% attack within those networks, suggesting that the requirements to halt PoS-based networks such as Solana, Algorand, Avalanche, and Cosmos Hub, are costly but only require collaboration among a small set of validators.

Figure 5

Minimum Number of Validators Required for a 33% Attack

	Solana		Algorand		Avalanche		Cosmos Hub	
Validator	Stake ($)/ Share (%)	Cumulative Stake/Share	Stake ($)/ Share (%)	Cumulative Stake/ Share	Stake ($)/ Share (%)	Cumulative Stake/Share	Stake ($)/ Share (%)	Cumulative Stake/Share
1	$322M (2.56%)	$322M (2.56%)	$32.5M (3.15%)	$32.5M (3.15%)	$49.0M (1.22%)	$49.0M (1.22%)	$84M (6.30%)	$84M (6.30%)
2	$266M (2.11%)	$589M (4.67%)	$26.8M (2.61%)	$59.3M (5.76%)	$49.0M (1.22%)	$98.0M (2.45%)	$77M (5.73%)	$161M (12.03%)
3	$262M (2.08%)	$851M (6.75%)	$26.4M (2.56%)	$85.7M (8.32%)	$49.0M (1.22%)	$147.0M (3.67%)	$76M (5.63%)	$237M (17.66%)
4	$232M (1.84%)	$1.1B (8.58%)	$26.2M (2.54%)	$111.9M (10.86%)	$49.0M (1.22%)	$196.0M (4.90%)	$72M (4.60%)	$299M (22.26%)
5	$196M (1.56%)	$1.3B (10.14%)	$26.2M (2.54%)	$138.0M (13.40%)	$49.0M (1.22%)	$245.0M (6.12%)	$61M (4.54%)	$360M (26.80%)
6	$196M (1.56%)	$1.5B (11.695)	$23.3M (2.27%)	$161.3M (15.67%)	$48.7M (1.22%)	$293.7M (7.34%)	$57M (4.23%)	$416M (31.03%)
7	$178M (1.41%)	$1.7B (13.10%)	$23.3M (2.26%)	$184.6M (17.93%)	$48.6M (1.22%)	$342.3M (8.56%)	$48M (3.57%)	$464M (34.60%)
8	$177M (1.41%)	$1.8B (14.51%)	$21.9M (2.13%)	$206.5M (20.05%)	$48.1M (1.20%)	$390.5M (9.76%)	$47M (3.47%)	$511M (38.07%)
9	$169M (1.34%)	$2.0B (15.85%)	$21.9M (2.13%)	$228.4M (22.18%)	$48.1M (1.20%)	$438.6M (10.96%)	$47M (3.47%)	$557M (41.54%)
10	$166M (1.32%)	$2.2B (17.17%)	$17.6M (1.71%)	$246.0M (23.89%)	$46.8M (1.17%)	$485.4M (12.13%)	$44M (3.49%)	$602M (44.83%)
11	$149M (1.18%)	$2.3B (18.35%)	$16.2M (1.58%)	$262.2M (25.46%)	$46.6M (1.17%)	$532.0M (1.30%)	$40M (3.01%)	$642M (47.85%)
12	$149M (1.18%)	$2.5B (19.53%)	$15.6M (1.52%)	$277.8M (26.98%)	$46.2M (1.16%)	$578.3M (14.46%)	$40M (2.99%)	$682M (50.84%)
13	$147M (1.17%)	$2.6B (20.70%)	$15.4M (1.50%)	$293.3M (28.48%)	$45.0M (1.12%)	$623.3M (15.58%)	$34M (2.52%)	$716M (53.36%)
14	$144M (1.14%)	$2.8B (21.84%)	$14.9M (1.45%)	$308.2M (29.93%)	$43.7M (1.09%)	$666.9M (16.67%)	$29M (2.16%)	$745M (55.52%)
15	$141M (1.12%)	$2.9B (22.96%)	$14.9M (1.44%)	$323.1M (31.37%)	$43.1M (1.08%)	$710.0M (17.75%)	$26M (1.96%)	$771M (57.48%)
16	$135M (1.07%)	$3.0B (24.03%)	$14.1M (1.36%)	$337.1M (32.74%)	$42.5M (1.06%)	$752.6M (18.81%)	$26M (1.91%)	$797M (59.39%)
17	$132M (1.05%)	$3.2B (25.07%)	$14.0M (1.36%)	$351.1M (34.09%)	$42.5M (1.06%)	$795.1M (19.87%)	$21M (1.60%)	$818M (60.98%)
18	$126M (1.00%)	$3.3B (26.07%)	$13.9M (1.35%)	$365.0M (35.44%)	$42.3M (1.06%)	$837.4M (20.93%)	$18M (1.32%)	$836M (62.30%)
19	$115M (0.91%)	$3.4B (26.99%)	$13.9M (1.34%)	$378.8M (36.79%)	$42.2M (1.06%)	$879.7M (21.99%)	$17M (1.24%)	$853M (63.54%)
20	$108M (0.86%)	$3.5B (27.84%)	$13.7M (1.33%)	$392.5M (38.12%)	$41.4M (1.03%)	$921.1M (23.02%)	$15M (1.08%)	$867M (64.62%)
21	$105M (0.83%)	$3.6B (28.67%)	$13.6M (1.32%)	$406.1M (39.44%)	$40.4M (1.01%)	$961.5M (24.03%)	$14M (1.08%)	$882M (65.70%)
22	$104M (0.83%)	$3.7B (29.50%)	$13.5M (1.31%)	$419.6M (40.75%)	$39.7M (0.99%)	$1.0B (25.03%)	$14M (1.07%)	$896M (66.77%)
23	$102M (0.81%)	$3.8B (30.31%)	$13.5M (1.31%)	$433.1M (42.06%)	$39.5M (0.99%)	$1.0B (26.02%)	$14M (1.02%)	$910M (67.79%)
24	$102M (0.81%)	$3.9B (31.12%)	$13.3M (1.29%)	$446.4M (43.35%)	$39.5M (0.99%)	$1.1B (27.00%)	$13M (1.00%)	$923M (68.79%)
25	$99M (0.78%)	$4.0B (31.90%)	$13.1M (1.28%)	$459.5M (44.62%)	$39.5M (0.99%)	$1.1B (27.99%)	$13M (0.98%)	$936M (69.78%)
26	$97M (0.77%)	$4.1B (32.67%)	$13.1M (1.27%)	$472.6M (45.89%)	$39.2M (0.98%)	$1.2B (28.97%)	$13M (0.97%)	$949M (70.74%)
27	$96M (0.76%)	$4.2B (33.44%)	$13.1M (1.27%)	$485.6M (47.16%)	$38.8M (0.97%)	$1.2B (29.94%)	$13M (0.94%)	$962M (71.68%)
28	$94M (0.75%)	$4.3B (34.18%)	$13.0M (1.26%)	$498.6M (48.42%)	$38.6M (0.96%)	$1.2B (30.91%)	$12M (0.91%)	$974M (72.59%)
29	$93M (0.74%)	$4.4B (34.92%)	$12.9M (1.25%)	$511.5M (49.67%)	$37.7M (0.94%)	$1.3B (31.85%)	$11M (0.85%)	$985M (73.44%)
30	$93M (0.73%)	$4.5B (35.66%)	$12.7M (1.24%)	$524.3M (50.91%)	$36.9M (0.92%)	$1.3B (32.77%)	$11M (0.81%)	$996M (74.25%)
31	$93M (0.73%)	$4.6B (36.39%)	$11.8M (1.14%)	$536.0M (52.05)	$36.5M (0.91%)	$1.3B (33.68%)	$11M (0.80%)	$1B (75.04%)

Source: Kraken Intelligence, Block Explorers, CoinGecko

- Stakes can turn rogue and validate incorrect transactions. However, some protocols have implemented incentive mechanisms to deter this from happening. For instance, Ethereum, as part of their planned transition to PoS, designed the "Casper" protocol where such rogue validators are punished by confiscating their staked cryptocurrencies and barring them from staking again.
- Some PoS protocols may require a large initial investment of the native token to qualify as a validator, which depends on the size of the network. Thus, PoS network design may impact centralization depending on how costly it is to partake in governance. For example, partaking in Ethereum 2.0 governance without a third party requires an individual to purchase and stake a minimum Ξ32 (about $35,000 as of publication) to become a validator, Whereas Cardano allows people to delegate their stake and participate with as little as 2.17 ADA.[32,33]

Figure 6

PoS Blockchain Validator Node Specs

PoS Bloackchain	Capped Validator Set	CPU Cores	Ram (GB)	Storage	Min. Stake (Native)	Min. Stake (USD)	Slashing Penalty
Ethereum 2.0	-	4 pCPU	8	500 GB, SSD	Ξ32	$38,207	✓
Cosmos	125	4 pCPU	32	2 TB, SSD	37,801 ATOM*	$340,133	✓
Polkadot	297	8 pCPU	64	500 GB, SSD	1.85M DOT*	$12,425,525	✓
BSC	21	8 pCPU	16	1 TB, SSD	614,846 BNB*	$146,187,997	✓
Solana	-	12–16 pCPU	128–256	2 TB, SSD	34 SOL	$1,238	✓
Algorand	-	2–4 vCPU	4–8	100–200 GB, SSD	0.1 ALGO	$0.03	
Avalanche	-	8 pCPU	16	1 TB, SSD	2,000 AVAX	$39,420	

Source: Kraken intelligence, protocol white papers, block explorers

- The trade-off for eliminating the need for validators to purchase and continuously upgrade hardware is that staked assets on PoS networks present an opportunity cost requiring a participant to own the native asset to stake.
- Forking is not automatically discouraged by PoS systems as it is in PoW due to the nothing-at-stake problem. However, PoS protocols have mitigated these vulnerabilities by destroying the stake of dishonest validators and barring them from the validation process. Still, readers should take such considerations into account since some PoS networks, including Algorand and Avalanche, do not include slashing penalties.[34,35]

The Debate: PoW vs. PoS

The rivalry between PoW and PoS surfaces key questions of network security, sustainability, barriers to entry, and achieving decentralization. A series of trade-offs between scalability, decentralization, and network security, commonly known as the "blockchain trilemma," plague every blockchain. For example, an increase in throughput typically comes at the expense of decentralization or security. Neither Sybil resistance mechanism is perfect; it is essential to understand the way we clearly define these trade-offs before discussing an optimal design for a blockchain network:

- **Decentralization**—retaining low barriers to entry for participation and a sufficiently distributed voting system.
- **Security**—ability to conduct attacks against or manipulate the network.
- **Scalability**—transaction efficiency and ability to adapt to a growing, global audience.

Considering these definitions, it is our take that PoW tends to offer better security and decentralization guarantees, sacrificing scalability in the process. On the other hand, PoS typically offers better scalability in exchange for security and decentralization.

Figure 7

The Blockchain Trilemma–PoW vs. PoS

Criteria	PoW	PoS
Decentralization	✓	
Security	✓	
Scalability		✓

Source: Kraken Intelligence

However, the optimal choice ultimately depends on a given blockchain's use case and how developers implement its Sybil resistance mechanism. Some blockchains are better suited for PoS, while others should use PoW.

Blockchain networks should generally adhere to a PoW mechanism if they want to retain the ethos of crypto: decentralization and security. PoW is generally more secure than PoS in that it is more extensively vetted, has fewer potential attack vectors (e.g., bribery attacks), requires the use of both capital and labor to misbehave on the network, and discourages constant forking (i.e., nothing-at-stake). The mechanism is also more decentralized than PoS in that it inherently encourages miners to distribute globally in search of cheap energy sources. Furthermore, voting power is theoretically less susceptible to falling in the hands of the wealthiest cryptoasset holders due to the requirement of hardware in authoring new blocks.

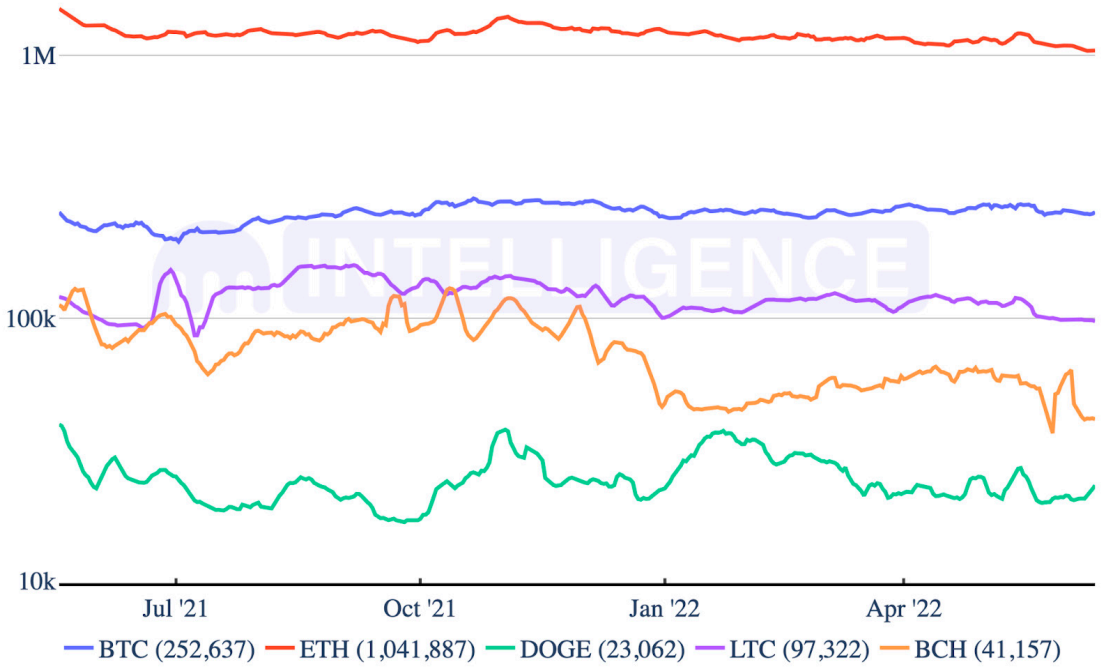
Imagine a scenario where a mining pool operator acts maliciously and the mining pool contributors opt to leave the pool. At worst, the malicious mining pool operator could keep the contributor's earnings. However, they could not continue to utilize their hash power for malicious purposes because the individual miners could turn off their mining equipment. Conversely, suppose a similar situation emerges where hackers target a third-party custodian and utilize the stolen funds to gain an overwhelming influence over a PoS network. Unlike PoW, in this hypothetical situation, the customers of the compromised custodian could not withdraw their contributions, losing both their funds and voting power.

Thus, for use cases such as hard money, PoS likely is undesirable because the possibility of the wealthiest network participants gaining an overwhelming share poses significant problems for an asset whose value derives from its decentralization, security, and scalability, among others.

PoS-based blockchains have more potential to scale because block production does not consume energy, honest nodes can bar dishonest nodes from the validation process, and the lack of mining allows for a faster validation process with less block variance. For use cases including mediums of exchange or smart contract platforms, PoW is potentially less desirable than PoS because network efficiency and scalability are paramount. Suppose these blockchains were to prioritize decentralization and security. In that case, they might become vulnerable to long-term scaling issues critical for a network that requires high transaction throughput to scale for a global audience. Solana is a fine example of this. Solana processes an average of 2,700 transactions per second (TPS), per the Solana explorer, with an upper peak of over 710,000 TPS.[36,37] Despite the immense transaction throughput on this blockchain network, some argue that running a Solana node is infeasible for consumers, leading to a centralized network. The high barrier to entry for participation means anyone interested in running a Solana node needs data center-grade hardware, including at least 128-256 GB of RAM, 2 TB of storage on an SSD, and 16 CPU cores.[38] Furthermore, the high throughput has caused security concerns because the protocol has broken down during times of high congestion.[9]

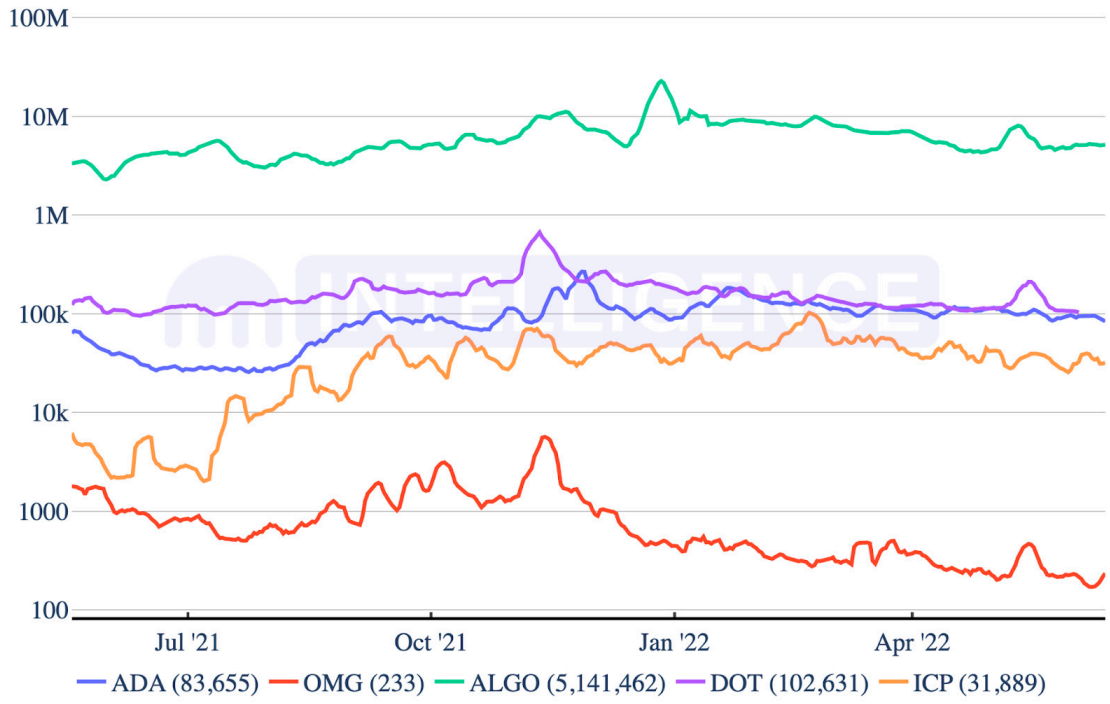
Figure 8

PoW (Top) vs. PoS (Bottom)—Transaction Count (7-Day Moving Average)



Daily Transaction Count (PoW)

PoW Asset	Jun 20, 2021	Jan 1, 2022	Jun 13, 2022	YoY	YTD
BTC	222.3K	241.7K	252.6K	14%	5%
LTC	93.3K	100.4K	97.3K	4%	-3%
DOGE	23.8K	22.5K	23.1K	-3%	3%
ETH	1.2M	1.2M	1.0M	-10%	-15%
BCH	92.8K	47.3K	41.2K	-56%	-13%
Total	**1.6M**	**1.6M**	**1.5M**	**-8%**	**-11%**



Daily Transaction Count (PoS)

PoS Asset	Jun 20, 2021	Jan 1, 2022	Jun 13, 2022	YoY	YTD
ICP	2.9K	32.2K	31.9K	984%	-1%
ADA	27.5K	39.5K	83.7K	205%	112%
ALGO	3.4M	12.7K	5.1K	51%	-59%
DOT	107.4K	179.7M	102.6M	-4%	-43%
OMG	0.7K	0.4K	0.2K	-66%	-48%
Total	**3.5M**	**12.9M**	**5.4M**	**52%**	**-59%**

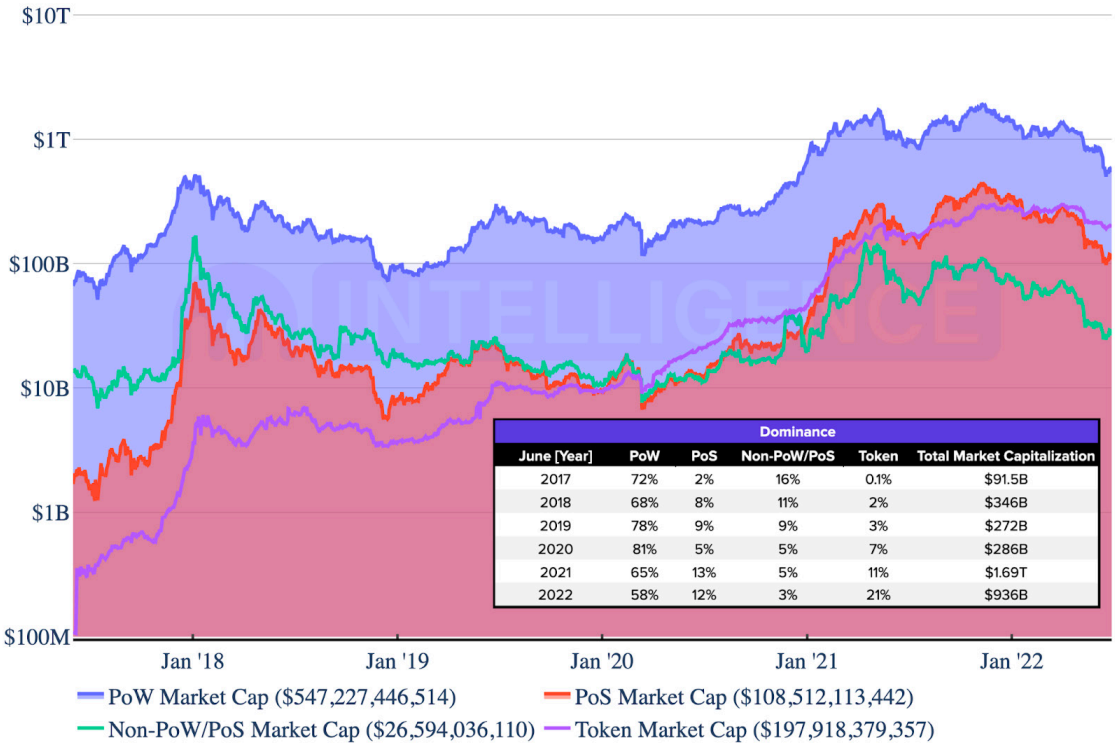
Source: Kraken Intelligence, Coin Metrics

Data suggests PoS cryptoassets are gaining traction as a medium of exchange as they outperformed PoW cryptoassets in transaction count on an annual basis. However, PoS cryptoassets have underperformed compared to PoW on a relative basis so far in 2022. Demand for on-chain value transfer has grown, as evidenced by BTC's transaction growth on both a YoY and YTD period, and LTC's YoY rise. ALGO's poor performance primarily drove the -60% YTD decline posted in the PoS camp. Because ETH alternatives like ADA and ALGO saw network activity rise while ETH saw activity fall, this provides further evidence of rising demand for smart contract platforms with low fees.

Furthermore, PoW cryptoassets have lost significant market dominance while token and PoS dominance has grown over the last five years. PoS cryptoassets have consumed considerable market dominance, but PoW still makes up roughly 58% of total market dominance. Still, PoS cryptoassets are on track to eventually outgrow the market capitalization of PoW cryptoassets should this pace continue. Moreover, readers should note that once Ethereum undergoes the Merge, its transition from PoW to PoS, about 12% dominance will leave the PoW camp for the PoS camp, meaning PoW assets will constitute about 46% of market dominance. In comparison, PoS will make up about 24%.

Figure 9

PoW vs. PoS Market Capitalization and Dominance



Dominance

June [Year]	PoW	PoS	Non-PoW/PoS	Token	Total Market Capitalization
2017	72%	2%	16%	0.1%	$91.5B
2018	68%	8%	11%	2%	$346B
2019	78%	9%	9%	3%	$272B
2020	81%	5%	5%	7%	$286B
2021	65%	13%	5%	11%	$1.69T
2022	58%	12%	3%	21%	$936B

Source: Kraken Intelligence, CoinGecko, Project websites
Note: The readings in figure 6 track nearly 115 different cryptoassets (~0.85% of cryptoassets), making up more than 94% of the total crypto market capitalization as of June 2022.

The choice between PoW and PoS is not black and white; however, there are apparent differentiating factors that could help determine which Sybil resistance mechanism is preferable for a given blockchain. Readers should interpret these comparisons as a rule of thumb rather than an objective fact applicable across all blockchains. Every blockchain still requires a deep understanding of the protocol's measures to defend against Sybil attacks, achieve a consensus on the state of the network, and how its measures balance the trade-offs within the blockchain trilemma.

4.

Conclusion and outlook

A blockchain's consensus method, paramount for verifying the authenticity of distributed blockchain platforms, is the process of building agreement among a network of mutually distrusting participants. Maintaining BFT within an open and distributed network as grand as Bitcoin requires a specific set of rules and mechanisms that rely on cryptography and game theory mechanics to create the trustless environment necessary to facilitate decentralized consensus across a value transfer network. The Sybil resistance mechanism is arguably the most critical feature of a blockchain's consensus method since distributed networks cannot otherwise reach a consensus in a BFT way. The two main Sybil resistance mechanisms to maintain BFT in a large distributed system like Bitcoin or Cardano are PoW and PoS, each with their trade-offs.

The rivalry between PoW and PoS confronts key questions of network security, sustainability, barriers to entry, and decentralization. Understanding the trade-offs between each is essential before concluding the optimal choice for a given blockchain network. It is our take that PoW generally offers better security and decentralization guarantees, exchanging scalability in the process. Conversely, PoS typically offers better scalability in exchange for security and decentralization. However, the best choice ultimately depends on a given blockchain's use case.

Blockchains should adhere to a PoW mechanism if they want to retain the ethos of cryptoassets: decentralization and security. For use cases such as hard money, PoS is likely less desirable because the possibility of the wealthiest users gaining an overwhelming share poses significant problems for an asset whose value derives from its decentralization, security, and scalability, among others. Decentralization and security should take precedence in these blockchains if they are to scale globally.

For use cases including mediums of exchange or smart contract platforms, PoW is potentially less desirable than PoS because network efficiency and scalability are paramount if these types of blockchains are to resist long-term scaling issues. Thus, the choice between PoW and PoS is not black and white. It requires a nuanced understanding of the two and their trade-offs to determine which Sybil resistance mechanism is better suited for a particular blockchain.

Footnotes

1. https://en.wikipedia.org/wiki/Sybil_(Schreiber_book)
2. https://ethereum.org/nl/developers/docs/consensus-mechanisms/
3. https://dl.acm.org/doi/10.1145/357172.357176
4. https://cypherpunks-core.github.io/ethereumbook/14consensus.html
5. https://arxiv.org/abs/2203.01315
6. https://arxiv.org/abs/1710.09437
7. https://www.leewayhertz.com/solana-blockchain-using-poh/#:~:text=Solana%20runs%20a%20consensus%20mechanism,out%20of%20voting%20on%20an
8. https://link.springer.com/chapter/10.1007/3-540-48071-4_10
9. https://link.springer.com/chapter/10.1007/978-0-387-35568-9_18
10. https://www.saveonenergy.com/electricity-rates/#:~:text=The%20average%20residential%20electricity%20rate,kilowatt%2Dhour%20(kWh).&text=The%20average%20electric%20price%20a,is%2011.77%20cents%20per%20kWh.
11. https://bitcoinmagazine.com/technical/now-segwit2x-hard-fork-has-really-failed-activate
12. https://bitcoinmagazine.com/technical/no2x-hard-fork-suspended-due-lack-consensus
13. https://bitcoin.stackexchange.com/questions/273/how-does-merged-mining-work
14. https://en.wikipedia.org/wiki/Bitcoin_Gold
15. https://www.coindesk.com/markets/2017/11/08/ethereum-security-lead-hard-fork-required-to-release-frozen-parity-funds/
16. https://coin.dance/blocks/hashrate
17. https://link.springer.com/chapter/10.1007/978-3-662-53357-4_2
18. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8653269
19. https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month/
20. https://www.ccn.com/privacy-coin-verge-succumbs-to-51-attack-again/
21. https://blockexplorer.com/news/third-times-a-charm-verge-suffers-51-attack-yet-again/
22. http://fortune.com/2018/05/29/bitcoin-gold-hack/
23. https://www.ccn.com/vertcoin-hit-by-51-attack-allegedly-lost-100000-in-double-spending/

24. https://btc.com/stats/pool

25. https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf

26. https://www.coindesk.com/tech/2021/03/11/nanos-network-flooded-with-spam-nodes-out-of-sync/

27. https://cointelegraph.com/news/solana-hit-with-another-network-incident-causing-degraded-performance

28. https://www.peercoin.net/#:~:text=Efficient%20Security&text=The%20key%20innovation%20of%20Peercoin,a%20costly%20limited%20resource%3A%20electricity.

29. https://blog.ethereum.org/2021/05/18/country-power-no-more/

30. https://arxiv.org/pdf/2003.03052.pdf

31. https://decrypt.co/21108/did-binance-just-help-take-over-steem-network-justin-sun

32. https://ethereum.org/en/staking/

33. https://www.reddit.com/r/Cardano_ELI5/comments/lg70t3/comment/gn6o7rl/

34. https://twitter.com/el33th4xor/status/1304204689198723073?lang=en

35. https://medium.com/blockchain-at-berkeley/the-need-for-an-incentive-scheme-in-algorand-6fe9db45f2a7

36. https://explorer.solana.com/

37. https://docs.solana.com/introduction

38. https://docs.solana.com/running-validator/validator-reqs

39. https://www.coindesk.com/tech/2022/05/03/heres-why-solana-ceased-block-production-for-seven-hours-on-saturday/#:~:text=Solana%20processes%20an%20average%20of,network%2C%20as%20per%20developer%20documents.

We appreciate your feedback!

Please visit **here** to participate in a brief survey. For all future Kraken Intelligence content, sign up **here**. For comments, suggestions, or questions related to this article or future topics you'd like to learn more about, you may also direct your communication to **intel@kraken.com** or to your account manager.

Kraken provides access to 196 crypto assets spanning 601 markets with advanced trading features, industryleading security, and on-demand client service. With the acquisition of Crypto Facilities, Kraken now offers seamless access to regulated derivatives on 5 cryptocurrencies with up to 50x leverage. Sign up for a free account in minutes at **www.kraken.com/sign-up**. We look forward to welcoming you.

For multi-exchange charting, trading, portfolio tracking, and high resolution historical data, please visit **https://cryptowat.ch**. Create a free Cryptowatch account today at **https://cryptowat.ch/account/create**.

For OTC-related execution services or inquiries, please direct your communication to **otc@kraken.com** or to your account manager.

Disclaimer