

If you have spent any time reading about cryptocurrency, you have likely seen lengthy articles bemoaning the large quantity of electricity consumed by crypto networks. What's the benefit of decentralised financial systems if they come with a side effect of increasing climate change? Expending electricity – Proof of Work, which we'll explain in more detail – is how the majority of blockchains validate transactions, but it's not the only way.

Smart people trying to get around the electricity consumption issues came up with a new way of validating transactions on a blockchain network – Proof of Stake. So how do these two systems compare?

Consensus mechanisms

How does a blockchain determine that a new block of the chain is valid? A majority of nodes in the blockchain network must agree on a block's validity, reaching a **consensus**. The method of reaching the consensus is known as a **consensus mechanism**. This controls how a blockchain verifies a transaction, and how it releases new coins to the network. Proof of stake and proof of work are both consensus mechanisms.

With **Proof of Work**, nodes of the network – known as **miners** – compete with each other to solve complex mathematical puzzles using computational power. The puzzles are hard to solve, but easy for other nodes to verify the validity. The miner node to solve the puzzle is rewarded with cryptocurrency, while all of the energy expended by the other miners is wasted. With proof of work, miners are financially rewarded for verifying the validity of transactions in the blockchain.

With **Proof of Stake**, nodes of the network – known as **validators** – each 'stake' a certain amount of cryptocurrency, which acts as a security deposit. A validator is selected to create a new block – called '**minting**' or '**forging**' – and validate a transaction. As a reward, the validator receives the transaction fee – validators with larger stakes are more likely to be selected and rewarded.

Comparing Proof of Work and Proof of Stake

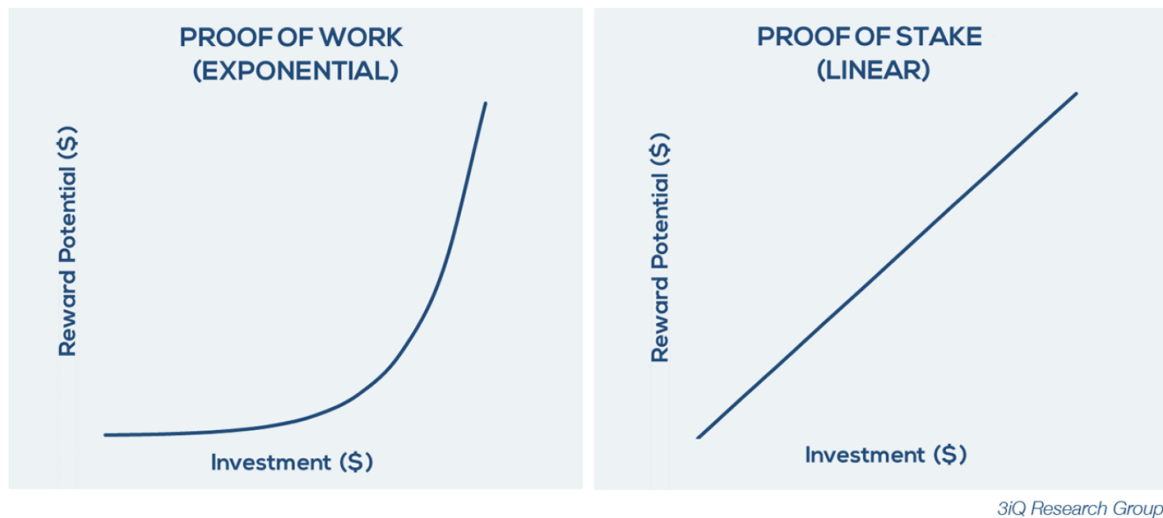
Fairness

In a proof of stake network, validators are selected to mint a new block pseudo-randomly according to the size of their stake. The chances of being selected increase linearly – a validator with a stake of \$20 000 is ten times more likely to be selected than a validator with only \$2000 staked.

This builds inequality into the network – those with the most money invested are most likely to win the transaction fee reward for new blocks, increasing their stake, and further increasing their chances of winning.

However, this proof of stake is MORE fair than proof of work. Miners in a proof of work network must pay for equipment and electricity, and those who invest the most increase their

chances of being rewarded exponentially. Multiple groups of miners pool their resources together to further increase their chances.



[\(Source\)](#)

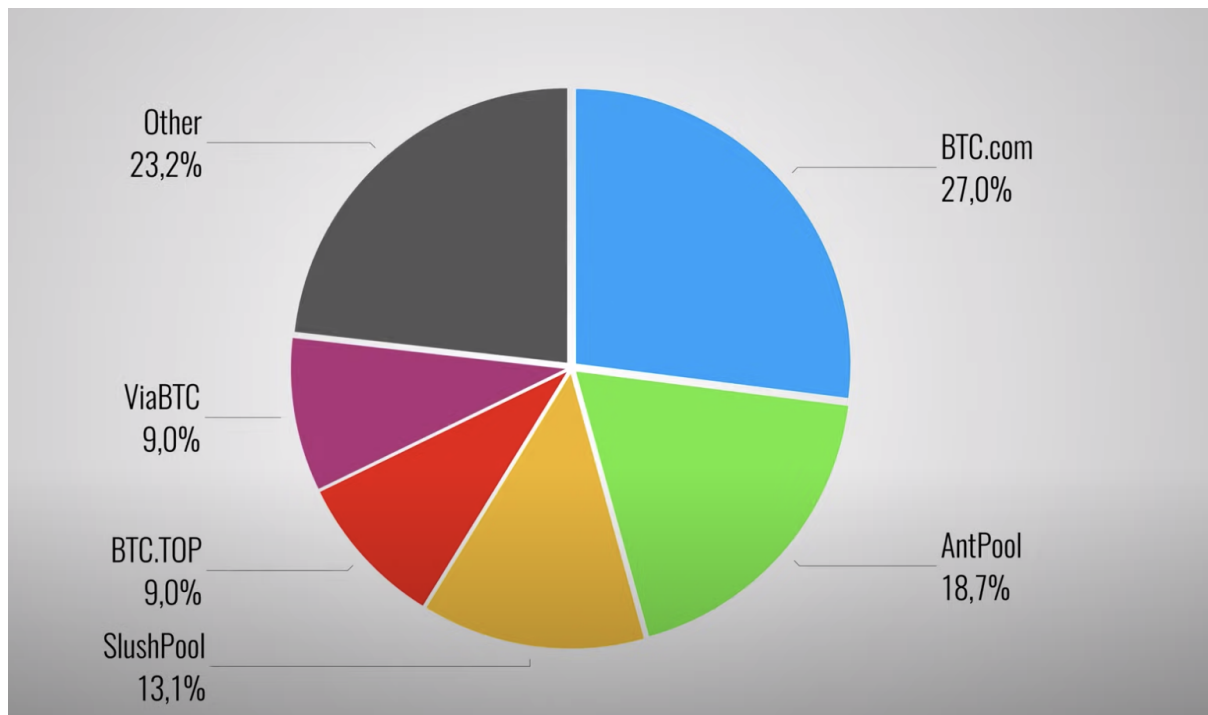
Security

Every node of a blockchain owns a full copy. When a node adds a new block to the blockchain, each node then compares their copy against the new copy to check its validity. Blocks that have been tampered with will mean the blockchain copies do not match, and the new block will be rejected.

In a proof of work network, the only penalty for creating a fraudulent block is the wasted energy spent solving the computational puzzle. In a proof of stake network, however, the network takes a financial penalty from the validator's stake. Incentive and punishment are built into the blockchain algorithm in proof of stake.

If a node stops being a validator, their stake and accumulated transaction fees are released after a period of time. The time delay is necessary because the network still needs to be able to punish validators if fraudulent blocks are found.

Fraudulent blocks could be added to the blockchain if a bad actor controls 51% of the nodes. For Bitcoin, the largest proof of work blockchain, miners pool their resources to increase their rewards. 76.8% of the BitCoin blockchain network is controlled by just five mining pools – further pooling could quite easily give one group a majority. Gaining 51% of a proof of stake network, however, involves owning 51% of the currency. This is possible, especially for a smaller cryptocurrency, but would be prohibitively expensive for established cryptos like Ethereum or BitCoin.



[\(source\)](#)

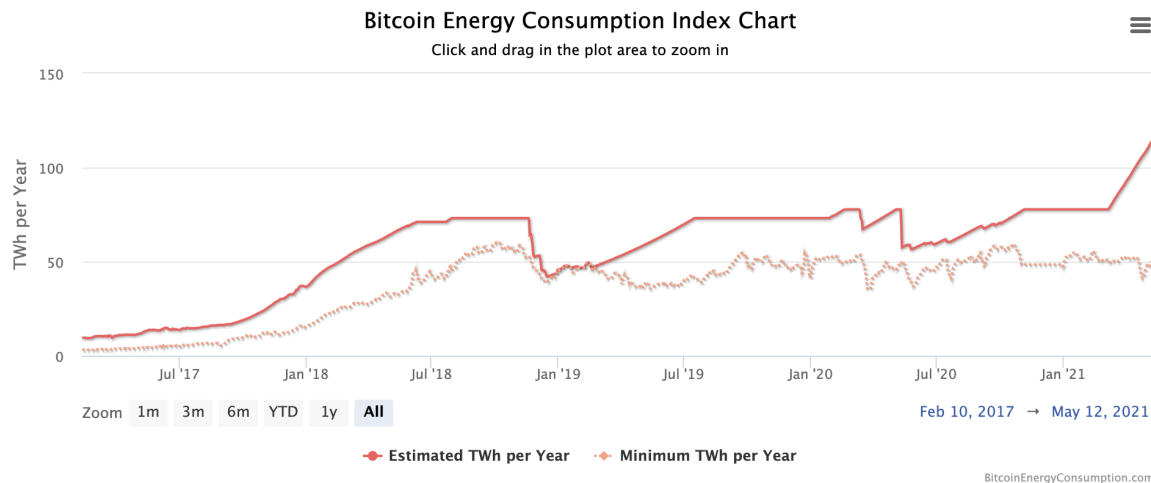
Proof of stake is also a consensus mechanism. The creator of a new block is chosen from a pool of users that have 'staked' a certain amount of crypto. No puzzle, no reward, but the miners take a fee for transaction. Penalty for trying to harm the network is losing your stake. A bad actor would need to control 51% of the cryptocurrency. Greener and cheaper. Proof of stake has validators. Mint or forge not mine.

Decentralisation

More nodes in a network increases the security of a blockchain. Becoming a miner in a proof of work blockchain requires plenty of computing equipment and a place to run it. As proof of stake only requires a financial transaction, the barrier for entry to be a validator is lower, increasing the amount of nodes.

Energy consumption

BitCoins ever-climbing energy consumption has been touted as a major limiting factor, as well as absurdly wasteful. Due to the nature of the proof of work algorithm, the energy consumption increases as more blocks are added to the chain. With proof of stake, there are no puzzles to solve and thus no energy to expend – this problem is (theoretically) eliminated.



[\(Source\)](#)

While the majority of blockchains still use the proof of work consensus mechanism, there are new blockchain cryptocurrencies that have been established using proof of stake. The second largest cryptocurrency, Ethereum, is planning a much awaited move to proof of stake.

However, proof of work blockchains have been in operation for several years now, which is enough time for the flaws and drawbacks of the system to be made apparent. Proof of stake may sound more workable and appealing so far, but as it has yet to be tested at global scale, will almost certainly come with a new set of problems to solve.