McKinsey & Company

McKinsey Explainers

What is proof of stake?

Proof of stake (PoS) is a consensus protocol in blockchains. It is a way to decide which user or users validate new blocks of transactions and earn a reward for doing so correctly.

January 2023

Blockchain has a reputation—not necessarily deserved—for being complicated and impenetrable. This has a lot to do with the consensus mechanism, which is essentially the way users of a blockchain agree on transaction history, present and future. Here, we demystify the consensus mechanism that seems poised to take over the world of cryptocurrency: proof of stake.

What is a blockchain?

Blockchain is a technology that enables secure sharing of information. Obviously, a database is where data is stored. A ledger is an account book where transactions are recorded. A blockchain is a type of *distributed* database or ledger—one of today's top tech trends—which means the power to update it is distributed between the nodes of a public or private computer network. This is known as distributed ledger technology, or DLT. The network provides incentives for nodes to make updates to blockchains in the form of digital tokens or currency.

What is a consensus protocol?

Cryptocurrencies, which have no physical note or coin exchange, are decentralized systems. That means there's no bank or other central authority to keep track of how much money is in each account and whether transactions are valid or fraudulent. Everyone participating in the network, or every node, needs another way to keep on top of ledgers and transactions.

For the blockchain to work, every node needs access to the same, continually updating database. That's why it's important that all nodes on a blockchain come to a consensus on any changes to the record.

When new data is added to the network, the majority of nodes must verify and confirm the legitimacy of the new data based on permissions or economic incentives; these are also called consensus mechanisms. When a consensus is reached, a new block is created and attached to the chain. All nodes are then updated to reflect the blockchain ledger.

There are many kinds of consensus protocols. Proof of work is the consensus mechanism that most cryptocurrencies have used until now; in September 2022 Ethereum-based cryptocurrencies transitioned to proof-of-stake protocols in a highly publicized event known as "The Merge."

How does proof of stake work?

A blockchain protocol provides traders with incentives to validate transactions by rewarding them with cryptocurrency for every correct validation. As a safeguard against fraud, proof-of-stake protocols require traders to "stake" some of their cryptocurrency as collateral, which is then locked up in a deposit. If a trader adds a transaction to the blockchain that other validators deem to be invalid, they can lose a portion of what they staked.

There's usually a lower limit to how much validators can stake. After the limit is surpassed, validators can stake as much as they want. In fact, the more a trader stakes, the more likely they are to be chosen by the algorithm. Here's a simple example to illustrate the point: let's say there's a new change to the blockchain that needs verification. Ten nodes volunteer to validate it, and they each stake one cryptocoin for the privilege. That means that they each have an equal 10 percent chance of being awarded the work.

Let's say that one volunteer really wants to win the work. They could up the odds by staking three coins on the deal. If everyone else kept their stake at one coin, they would up their chance of winning the work to 25 percent, while everyone else's chances would go down to 8.3 percent.

In practice, it's a lot more complicated than that. That's because new transactions are grouped together in blocks, sometimes of several hundred or more. Then several blocks are chained together to create a record of all the transactions in order. Another complicating factor is that traders can enter staking pools, where groups of validators can together come up with the lower limit to become a validator. When a staking pool is awarded the work,

the reward is split among the pool's members, with a slightly larger share going to the pool's owner.

What is a proof-of-work consensus protocol?

Currently, most blockchains arrive at consensus via proof of work (PoW). Here's how it works: the first node, or participant, to verify a new data addition or transaction on the digital ledger receives a certain number of tokens as a reward. The verification process requires a participant—who might be called a "miner"—to solve a cryptographic question. The computer that completes the puzzle first is awarded the token. This model provides incentives for miners to act quickly, which increases the speed at which an operation is completed.

Why is proof of stake seen as an upgrade from proof of work?

Many expect that a significant number of cryptocurrencies will migrate to proof of stake. In PoS systems, miners are scored based on the number of coins they have in their digital wallets and the length of time they have had them. The miner with the highest at stake has a greater chance to be chosen to validate a transaction and receive a reward.

Directing the resources of high-powered computers to solve puzzles means using more electricity. Cryptocurrencies that use proof-of-work consensus mechanisms have been criticized for their electricity consumption.

Proof of stake is faster, sidesteps the energy burn, and requires no special computing equipment. For these reasons and others, it's the validation protocol for newer waves of cryptocurrencies and altcoins. For example, Ethereum 1.0 uses proof of work, but Ethereum 2.0 uses proof of stake. Others using proof-of-stake protocols include Tezos, Cardano, Solana, and Algorand. Users like it for its quicker processing returns and the scalability made possible by the lower cost.

Articles referenced include:

— "McKinsey Technology Trends Outlook 2022," August 24, 2022, Michael Chui, Roger Roberts, and Lareina Yee

— "Forward Thinking on tech and the unpredictability of prediction with Benedict Evans," April 6, 2022, Janet Bush and Michael Chui

— "CBDC and stablecoins: Early coexistence on an uncertain road," October 11, 2021, Ian De Bode, Matt Higginson, and Marc Niederkorn

— "Blockchain and retail banking: Making the connection," June 7, 2019, Matt Higginson, Atakan Hilal, and Erman Yugac

— "Blockchain 2.0: What's in store for the two ends—semiconductors (suppliers) and industrials (consumers)?," January 18, 2019, Gaurav Batra, Rémy Olson, Shilpi Pathak, Nick Santhanam, and Harish Soundararajan

— "Blockchain explained: What it is and isn't, and why it matters," September 28, 2018, Brant Carson and Matt Higginson

Designed by McKinsey Global Publishing