VALKYRIE

What is Proof-of-Stake?

Proof-of-Stake (PoS) is a is a consensus mechanism which gives blockchain data verification responsibilities to assigned network nodes that have locked collateral tokens in the network. The collateral used is also often locked for a specific time period, depending on the network.

To select a validator for each block, PoS networks use several different methods and criteria, including; size of stake, age of stake, and random selection. The winning validator is then given the block reward and associated transaction fees, meaning most PoS coins are inherently inflationary forever. As opposed to Proof-of-Work (PoW), Proof-of-Stake requires no specialized external hardware or significant electricity requirements. Depending on the network, validators may or may not be required to store the full or partial history of all transactions on a network node. The idea for PoS consensus was first discussed on the bitcointalk forums in 2011 and the first functioning PoS network was PeerCoin in 2012.

Functionally, PoS rewards act as passive income, comparable to interest payments. Similar to the availability of mining pools on a PoW network, users who do not meet the staking collateral requirements for a validator node, or do not wish to run a node but want to collect a reward, can delegate their stake to a validator node. The validator then collects the network rewards and sends the delegate their reward based on the collateral provided, minus a variable fee. On some networks, validator nodes can require a significant capital investment and are referred to as masternodes, which may also have additional transactional capabilities. Conversely, some networks only require a small fixed amount of collateral to run a validator node. Other networks limit the number of validator nodes to the top eligible delegates based on total coins or tokens staked by the validator, with other validators receiving little to no block reward.

In order to discourage inactivity or malicious validator activity, such as double spending transactions or ledger re-organization, a penalty known as slashing can be enacted on a network validators. A slashing penalty is collected from the staked collateral of the validator and may vary from a fixed token amount or percentage, as well as temporarily or permanently banning the validator from the network. Depending on the network, slashing penalties are collected as a bounty by the reporting entity, sent to a community fund, and/or sent to an unretrievable burn address.

Coin	Ticker	Market Cap (bn)	Staking Reward (%)	Staked Value (bn)	Staking Participation (%)
Ethereum 2.0	ETH	394.60	4.60	34.06	9
Binance Coin	BNB	70.93	7.25	7.81	81
Solana	SOL	40.63	5.86	48.82	76
Cardano	ADA	39.02	5.04	28.25	72
Terra	LUNA	36.70	5.95	31.94	41
Avalanche	AVAX	25.73	9.08	21.27	55
Polkadot	DOT	21.22	14.05	13.26	52
Polygon	MATIC	12.67	5.26	11.28	35
NEAR	NEAR	8.82	10.62	5.59	39
Cosmos	ATOM	8.29	15.20	5.09	60

*Market Cap and Staking values as of April 1st, 2022

	Equipment Requirements	Validating or Mining a Block	Centralization Risk	Network Security	Malicious Attack
Proof-of-Stake (PoS)	Server Grade Hard Drive and RAM	Determined by Size and/or Age of Staked Collateral, or Random Selection	If Significant Collateral Held by Few Validators	Increasingly Secure as Staked Collateral Increases	Single Entity Would Need to Acquire 51% of All Circulating Coins
Proof-of-Work (PoW)	Application-Specific Integrated Circuits (ASICs) and Graphics Processing Units (GPUs)	Capacity of Computing Power Determines Probability of Mining a Block	If Significant Computing Power Held by Few Miners	Increasingly Secure as Computing Power Increases	Single Entity Would Need to Acquire 51% of All Computing Power