title: Frequently Asked Questions description: Frequently asked questions on proof-of-stake Ethereum. lang: en

What is proof-of-stake {#what-is-proof-of-stake}

Proof-of-stake is a class of algorithm that can provide security to blockchains by ensuring that assets of value are lost by attackers who act dishonestly. Proof-of-stake systems require a set of validators to make some asset available that can be destroyed if the validator engages in some provably dishonest behavior. Ethereum uses a proof-of-stake mechanism to secure the blockchain.

How does proof-of-stake compare to proof-of-work? {#comparison-to-proof-of-work}

Both proof-of-work and proof-of-stake are mechanisms that economically disincentivize malicious actors from spamming or defrauding the network. In both cases, nodes that actively participate in consensus put some asset "into the network" that they will lose if they misbehave.

In proof-of-work, this asset is energy. The node, known as a miner, runs an algorithm that aims to compute a value faster than any other node. The fastest node has the right to propose a block to the chain. To change the history of the chain or dominate the block proposal, a miner would have to have so much computing power that they always win the race. This is prohibitively expensive and difficult to execute, protecting the chain from attacks. The energy required to "mine" using proof-of-work is a real-world asset that miners pay for.

Proof-of-stake requires nodes, known as validators, to explicitly submit a crypto asset to a smart contract. If a validator misbehaves, this crypto can be destroyed because they are "staking" their assets directly into the chain instead of indirectly via energy expenditure.

Proof-of-work is much more energy-hungry because electricity is burned in the mining process. Proof-of-stake, on the other hand, requires only a very small amount of energy - Ethereum validators can even run on a low-powered device such as Raspberry Pi. Ethereum's proof-of-stake mechanism is thought to be more secure than proof-of-work because the cost to attack is greater, and the consequences to an attacker are more severe.

Proof-of-work versus proof-of-stake is a contentious topic. Vitalik Buterin's blog and the debate between Justin Drake and Lyn Alden give a good summary of the arguments.

Is proof-of-stake energy efficient? {#is-pos-energy-efficient}

Yes. Nodes on a proof-of-stake network use a tiny amount of energy. A third-party study concluded that the entire proof-of-stake Ethereum network consumes around 0.0026 TWh/yr - about 13,000x less than gaming in the US alone.

More on Ethereum's energy consumption.

Is proof-of-stake secure? {#is-pos-secure}

Ethereum's proof-of-stake is very secure. The mechanism was researched, developed, and tested rigorously over eight years before going live. The security guarantees are different from proof-of-work blockchains. In proof-of-stake, malicious validators can be actively punished ("slashed") and ejected from the validator set, costing a substantial amount of ETH. Under proof-of-work, an attacker can keep repeating their attack while they have sufficient hash power. It is also more costly to mount equivalent attacks on proof-of-stake Ethereum than under proof-of-work. To affect the liveness of the chain, at least 33% of the total staked ether on the network is required (except in the cases of very sophisticated attacks with an extremely low likelihood of success). To control the contents of future blocks, at least 51% of the total staked ETH is required, and to rewrite history, over 66% of the total stake is needed. The Ethereum protocol would destroy these assets in the 33% or 51% attack scenarios and by social consensus in the 66% attack scenario.

- More on defending Ethereum proof-of-stake from attackers

- More on proof-of-stake design

Does proof-of-stake make Ethereum cheaper? {#does-pos-make-ethereum-cheaper}

No. The cost to send a transaction (gas fee) is determined by a dynamic fee market that increases with more network demand. The consensus mechanism does not directly influence this.

More on gas.

What are nodes, clients and validators? {#what-are-nodes-clients-and-validators}

Nodes are computers connected to the Ethereum network. Clients are the software they run that turns the computer into a node. There are two types of clients: execution clients and consensus clients. Both are needed to create a node. A validator is an optional add-on to a consensus client that enables the node to participate in proof-of-stake consensus. This means creating and proposing blocks when selected and attesting to blocks they hear about on the network. To run a validator, the node operator must deposit 32 ETH into the deposit contract.

- More on nodes and clients
- More on staking

Is proof-of-stake a new idea? {#is-pos-new}

No. A user on BitcoinTalk proposed the basic idea of proof-of-stake as an upgrade to Bitcoin in 2011. It was eleven years before it was ready to implement on Ethereum Mainnet. Some other chains implemented proof-of-stake earlier than Ethereum, but not Ethereum's specific mechanism (known as Gasper).

What is special about Ethereum's proof-of-stake? {#why-is-ethereum-pos-special}

Ethereum's proof-of-stake mechanism is unique in its design. It was not the first proof-of-stake mechanism to be designed and implemented, but it is the most robust. The proof-of-stake mechanism is known as "Casper". Casper defines how validators are selected to propose blocks, how and when attestations are made, how attestations are counted, the rewards and penalties given to validators, slashing conditions, failsafe mechanisms such as the inactivity leak, and the conditions for "finality". Finality is the condition that for a block to be considered a permanent part of the canonical chain it must have been voted for by at least 66% of the total staked ETH on the network. Researchers developed Casper specifically for Ethereum, and Ethereum is the first and only blockchain to have implemented it.

In addition to Casper, Ethereum's proof-of-stake uses a fork choice algorithm called LMD-GHOST. This is required in case a condition arises where two blocks exist for the same slot. This creates two forks of the blockchain. LMD-GHOST picks the one that have the greatest "weight" of attestations. The weight is the number of attestations weighted by the effective balance of the validators. LMD-GHOST is unique to Ethereum.

The combination of Casper and LMD_GHOST is known as Gasper.

More on Gasper

What is slashing? {#what-is-slashing}

Slashing is the term given to the destruction of some of a validator's stake and the ejection of the validator from the network. The amount of ETH lost in a slashing scales with the number of validators being slashed - this means colluding validators get punished more severely than individuals.

More on slashing

Why do validators need 32 ETH? {#why-32-eth}

Validators have to stake ETH so that they have something to lose if they misbehave. The reason why they have to stake 32 ETH specifically is to enable nodes to run on modest hardware. If the minimum ETH per validator were lower, then the number of validators and therefore the number of messages that must be processed in each slot would increase, meaning more powerful hardware would be required to run a node.

How are validators selected? {#how-are-validators-selected}

A single validator is pseudo-randomly chosen to propose a block in each slot using an algorithm called RANDAO that mixes a hash from the block proposer with a seed that gets updated every block. This value is used to select a specific validator from the total validator set. The validator selection is fixed four epochs in advance.

More on validator selection

What is stake grinding? {#what-is-stake-grinding}

Stake grinding is a category of attack on proof-of-stake networks where the attacker tries to bias the validator selection algorithm in favour of their own validators. Stake grinding attacks on RANDAO require about half the total staked ETH.

More on stake grinding

What is social slashing? {#what-is-social-slashing}

Social slashing is the ability of the community to coordinate a fork of the blockchain in response to an attack. It enables the community to recover from an attacker finalizing a dishonest chain. Social slashing can also be used against censorship attacks.

- More on social slashing
- Vitalik Buterin on social slashing

Will I get slashed? {#will-i-get-slashed}

As a validator, it is very difficult to get slashed unless you deliberately engage in malicious behavior. Slashing is only implemented in very specific scenarios where validators propose multiple blocks for the same slot or contradict themselves with their attestations - these are very unlikely to arise accidentally.

More on slashing conditions

What is the nothing-at-stake problem? {#what-is-nothing-at-stake-problem}

The nothing-at-stake problem is a conceptual issue with some proof-of-stake mechanisms where there are only rewards and no penalties. If there is nothing at stake, a pragmatic validator is equally happy to attest to any, or even multiple, forks of the blockchain, as this increases their rewards. Ethereum gets around this using finality conditions and slashing to ensure one canonical chain.

More on the nothing-at-stake problem

What is a fork choice algorithm? {#what-is-a-fork-choice-algorithm}

A fork choice algorithm implements rules determining which chain is the canonical one. Under optimal conditions, there is no need for a fork choice rule because there is only one block proposer per slot and one block to choose from. Occasionally, though, multiple blocks for the same slot or late-arriving information leads to multiple options for how blocks near the head

of the chain are organized. In these cases, all clients must implement some rules identically to make sure they all pick the correct sequence of blocks. The fork-choice algorithm encodes these rules.

Ethereum's fork-choice algorithm is called LMD-GHOST. It picks the fork with the greatest weight of attestations, meaning the one that most staked ETH has voted for.

More on LMD-GHOST

What is finality in proof-of-stake? {#what-is-finality}

Finality in proof-of-stake is the guarantee that a given block is a permanent part of the canonical chain and cannot be reverted unless there is a consensus failure in which an attacker burns 33% of the total staked ether. This is "crypto-economic" finality, as opposed to "probabilistic finality" which is relevant to proof-of-work blockchains. In probabilistic finality, there are no explicit finalized/non-finalized states for blocks - it simply becomes less and less likely that a block could be removed from the chain as it gets older, and users determine for themselves when they are sufficiently confident that a block is "safe". With crypto-economic finality, pairs of checkpoint blocks have to be voted for by 66% of the staked ether. If this condition is satisfied, blocks between those checkpoints are explicitly "finalized".

More on finality

What is "weak subjectivity"? {#what-is-weak-subjectivity}

Weak subjectivity is a feature of proof-of-stake networks where social information is used to confirm the current state of the blockchain. New nodes or nodes rejoining the network after being offline for a long time can be given a recent state so that the node can see immediately whether they are on the correct chain. These states are known as "weak subjectivity checkpoints" and they can be obtained from other node operators out-of-band, or from block explorers, or from several public endpoints.

More on weak subjectivity

Is proof-of-stake censorship resistant? {#is-pos-censorship-resistant}

Censorship resistance is currently hard to prove. However, unlike proof-of-work, proof-of-stake offers the option to coordinate slashings to punish censoring validators. There are upcoming changes to the protocol that separate block builders from block proposers and implement lists of transactions that builders must include in each block. This proposal is known as proper-builder separation and helps to prevent validators from censoring transactions.

More on proposer-builder separation

Can Ethereum's proof-of-stake system be 51% attacked? {#pos-51-attack}

Yes. Proof-of-stake is vulnerable to 51% attacks, just like proof-of-work. Instead of the attacker requiring 51% of the network's hash power, the attacker requires 51% of the total staked ETH. An attacker that accumulates 51% of the total stake gets to control the fork-choice algorithm. This enables the attacker to censor certain transactions, do short-range reorgs and extract MEV by reordering blocks in their favor.

More on attacks on proof-of-stake

What is social coordination, and why is it needed? {#what-is-social-coordination}

Social coordination is a last line of defense for Ethereum that would allow an honest chain to be recovered from an attack that finalized dishonest blocks. In this case, the Ethereum community would have to coordinate "out-of-band" and agree to use an honest minority fork, slashing the attacker's validators in the process. This would require apps and exchanges to recognize the honest fork too.

Read more on social coordination

Do the rich get richer in proof-of-stake? {#do-rich-get-richer}

The more ETH someone has to stake, the more validators they can run, and the more rewards they can accrue. The rewards scale linearly with the amount of staked ETH, and everyone gets the same percentage return. Proof-of-work enriches the rich more than proof-of-stake because richer miners that buy hardware at scale benefit from economies of scale, meaning the relationship between wealth and reward is non-linear.

Is proof-of-stake more centralized than proof-of-work? {#is-pos-decentralized}

No, proof-of-work tends towards centralization because mining costs increase and price out individuals, then price out small companies, and so on. The current problem with proof-of-stake is the influence of liquid staking derivatives (LSDs). These are tokens representing ETH staked by some provider that anyone can swap on secondary markets without the actual ETH being unstaked. LSDs allow users to stake with less than 32 ETH, but they also create a centralization risk where a few big organizations can end up controlling much of the stake. This is why solo staking is the best option for Ethereum.

More on stake centralization in LSDs

Why can I only stake ETH? {#why-can-i-only-stake-eth}

ETH is Ethereum's native currency. It is essential to have a single currency in which all stakes are denominated, both for accounting effective balances for weighting votes and security. ETH itself is a fundamental component of Ethereum rather than a smart contract. Incorporating other currencies would significantly increase the complexity and decrease the security of staking.

Is Ethereum the only proof-of-stake blockchain? {#is-ethereum-the-only-pos-blockchain}

No, there are several proof-of-stake blockchains. None are identical to Ethereum; Ethereum's proof-of-stake mechanism is unique.

What is The Merge? {#what-is-the-merge}

The Merge was the moment when Ethereum switched off its proof-of-work-based consensus mechanism and switched on its proof-of-stake-based consensus mechanism. The Merge happened on September 15, 2022.

More on The Merge

What are liveness and safety? {#what-are-liveness-and-safety}

Liveness and safety are the two fundamental security concerns for a blockchain. Liveness is the availability of a finalizing chain. If the chain stops finalizing or users are not able to access it easily, those are liveness failures. Extremely high cost of access could also be considered a liveness failure. Safety refers to how difficult it is to attack the chain - i.e. finalize conflicting checkpoints.

Read more in the Casper paper