title: A more secure Ethereum description: Ethereum is the most secure and decentralized smart-contract platform in existence. However, there are still improvements that can be made so that Ethereum stays resilient to any level of attack far into the future. lang: en image: ../../../assets/roadmap/roadmap-security.png alt: "Ethereum roadmap" template: roadmap

Ethereum is already a very secure, decentralized smart-contract platform. However, there are still improvements that can be made so that Ethereum stays resilient to all kinds of attack far into the future. These include subtle changes to the way Ethereum clients deal with competing blocks, as well as increasing the speed the network considers blocks to be "finalized" (meaning they can't be changed without extreme economic losses to an attacker).

There are also improvements that make censoring transactions much more difficult by making block proposers blind to the actual contents of their blocks, and new ways to identify when a client is censoring. Together these improvements will upgrade the proof-of-stake protocol so that users - from individuals to corporations - have instant confidence in their apps, data and assets on Ethereum.

Staking withdrawals {#staking-withdrawals}

The upgrade from proof-of-work to proof-of-stake began with Ethereum pioneers “staking” their ETH in a deposit contract. That ETH is used to protect the network. However, that ETH cannot yet be unlocked and returned to the users. Allowing ETH to be withdrawn is a critical part of the proof-of-stake upgrade. In addition to withdrawals being a critical component of a fully-functional proof-of-stake protocol, allowing withdrawals is also good for Ethereum security as it allows stakers to use their ETH rewards for other non-staking purposes. This means users that want liquidity do not have to rely upon liquid staking derivatives (LSDs) that can be a centralizing force on Ethereum. This upgrade is scheduled to be completed on April 12, 2023.

Read about withdrawals

Defending against attacks {#defending-against-attacks}

Even after withdrawals there are improvements that can be made to Ethereum'sproof-of-stake protocol. One is known as view-merge - a more secure fork-choice algorithm that makes certain sophisticated types of attack more difficult.

Reducing the time Ethereum takes to finalize blocks would provide a better user experience and prevent sophisticated "reorg" attacks where attackers try to reshuffle very recent blocks to extract profit or censor certain transactions. **Single slot finality (SSF)** is a way to minimize the finalization delay. Right now there are 15 mins worth of blocks that an attacker could theoretically convince other validators to reconfigure. With SSF, there are 0. Users, from individuals to apps and exchanges, benefit from fast assurance that their transactions will not be reverted, and the network benefits by shutting down a whole class of attacks.

Read about single slot finality

Defending against censorship {#defending-against-censorship}

Decentralization prevents individuals or small groups of validators from becoming too influential. New staking technologies can help to ensure Ethereum's validators stay as decentralized as possible while also defending them against hardware, software and network failures. This includes software that shares validator responsibilities across multiple nodes. This is known as **distributed validator technology (DVT)**. Staking pools are incentivized to use DVT because it allows multiple computers to collectively participate in validation, adding redundancy and fault-tolerance. It also splits validator keys across several systems, rather than having single operators running multiple validators. This makes it harder for dishonest operators to coordinate attacks on Ethereum. Overall, the idea is to derive security benefits by running validators as *communities* rather than as individuals.

Read about distributed validator technology

Implementing **proposer-builder separation (PBS)** will drastically improve Ethereum's built-in defenses against censorship. PBS allows one validator to create a block and another to broadcast it across the Ethereum network. This ensures that the gains from professional profit-maximizing block building algorithms are shared more fairly across the network, **preventing stake from concentrating** with the best-performing institutional stakers over time. The block proposer gets to select the most profitable block offered to them by a market of block builders. To censor, a block proposer would often have to choose a less profitable block, which would be **economically irrational and also obvious to the rest of the validators**on the network.

There are potential add-ons to PBS, such as encrypted transactions and inclusion lists, that could further improve Ethereum's censorship resistance. These make the block builder and proposer blind to the actual transactions included in their blocks.

Read about proposer-builder separation

Protecting validators {#protecting-validators}

It is possible that a sophisticated attacker could identify upcoming validators and spam them to prevent them from proposing blocks; this is known as a **denial of service (DoS)** attack. Implementing **secret leader election (SLE)** will protect against this type of attack by preventing block proposers from being knowable in advance. This works by continually shuffling a set of cryptographic commitments representing candidate block proposers and using their order to determine which validator is selected in such a way that only the validators themselves know their ordering in advance.

Read about secret leader election

Current progress {#current-progress}

Security upgrades on the roadmap are in advanced stages of research, but they are not expected to be implemented for some time. The next steps for view-merge, PBS, SSF and SLE is to finalize a specification and start building prototypes.