---

title: Future-proofing Ethereum description: These upgrades cement Ethereum as the resilient, decentralized base layer for the future, whatever it may hold. lang: en image: ../../../assets/roadmap/roadmap-future.png alt: "Ethereum roadmap" template: roadmap

---

Some parts of the roadmap are not necessarily required for scaling or securing Ethereum in the near-term, but set Ethereum up for stability and reliability far into the future.

Quantum resistance {#quantum-resistance}

Some of the cryptography securing present-day Ethereum will be compromised when quantum computing becomes a reality. Although quantum computers are probably decades away from being a genuine threat to modern cryptography, Ethereum is being built to be secure for centuries to come. This means making Ethereum quantum resistant as soon as possible.

The challenge facing Ethereum developers is that the current proof-of-stake protocol relies upon a very efficient signature scheme known as BLS to aggregate votes on valid blocks. This signature scheme is broken by quantum computers, but the quantum resistant alternatives are not as efficient.

The "KZG" commitment schemes used in several places across Ethereum to generate cryptographic secrets are known to be quantum-vulnerable. Currently, this is circumvented using "trusted setups" where many users generate randomness that cannot be reverse-engineered by a quantum computer. However, the ideal solution would simply be to incorporate quantum safe cryptography instead. There are two leading approaches that could become efficient replacements for the BLS scheme: STARK-based and lattice-based signing. These are still being researched and prototyped.

Read about KZG and trusted setups

Simpler and more efficient Ethereum {#simpler-more-efficient-ethereum}

Complexity creates opportunities for bugs or vulnerabilities that can be exploited by attackers. Therefore, part of the roadmap is simplifying Ethereum and removing code that has hung around through various upgrades but is no longer needed or can now be improved upon. A leaner, simpler codebase is easier for developers to maintain and reason about.

There are several updates that will be made to theEthereum Virtual Machine (EVM) to make it simpler and more efficient. These include removing the SELFDESTRUCT opcode - a rarely used command that is no longer needed and in some circumstances can be dangerous to use, especially when combined with other future upgrades to Ethereum's storage model. Ethereum clients also still support some old transaction types that can now be completely removed. The way gas is calculated can also be improved and more efficient methods for the arithmetic underpinning some cryptographic operations can be brought in.

Similarly, there are updates that can be made to other parts of present-day Ethereum clients. One example is that current execution and consensus clients use a different type of data compression. It will be much easier and more intuitive to share data between clients when the compression scheme is unified across the whole network.

Current progress {#current-progress}

Most of the upgrades required for future-proofing Ethereum are still in the research phase and may be several years away from being implemented. Upgrades such as removing SELF-DESTRUCT and harmonizing the compression scheme used in the execution and consensus clients are likely to come sooner than quantum resistant cryptography.

Further reading

- Gas
- EVM
- Data structures