

Ethereum's Roadmap for Post-Quantum Cryptography

Ethereum is a decentralized, public blockchain-based platform conceptualised by Vitalik Buterin in 2015. It enables developers to create decentralized applications (DApps) and deploy smart contracts using its Ether (ETH) cryptocurrency. Also, Ethereum has been integral to the development of non-fungible tokens (NFTs), decentralized finance (DeFi), decentralized autonomous organizations (DAOs), and the Metaverse. Ethereum is often described by its founders and developers as "the world's most programmable blockchain." This is because it has established itself as the only blockchain network that facilitates digital asset transactions and enables the development of a wide range of decentralized applications.

The security of our online communications and digital assets is built on two of the most popular cryptography standards, RSA and ECC, whose foundation is heavily established on the assumption that it's extremely difficult for conventional computers to solve certain complex mathematical problems. However, the advent of quantum computers has brought about the "quantum threat," which means that if and when large-scale quantum computers are built, they can solve these problems and break our current public-key cryptosystems. This would seriously undermine the security, confidentiality, and integrity of our digital communication on the internet and its associated data.

Understanding Post-Quantum Cryptography (PQC)

Post-quantum cryptography, also known as quantum-proof encryption or quantum-resistant encryption, refers to cryptographic schemes or systems that can secure classical computers against attacks by quantum computers. It prepares us for the approaching era of quantum computing by revising the mathematical-based algorithms and standards associated with our existing cryptography standards. Post-quantum cryptography has incorporated an evolution of cryptographic approaches that can be implemented on today's classical computers, which will safeguard them against attacks from tomorrow's quantum computers.

The blockchain, which is the backbone of cryptocurrencies such as Bitcoin and Ethereum, is built on a cryptographic security system called elliptic curve cryptography (ECC). Similarly, the security of our digital communications, specifically via the internet, is founded on another cryptographic system known as RSA (Rivest, Shamir, and Adleman, its creators). Both RSA and

ECC use public key encryption (PKE) algorithms, which ensures that they are not easily compromised based on the fact that classical computers find it difficult to factor very large numbers and compute elliptic curve discrete logarithms.

But after Peter Shor demonstrated in 1992 using a powerful algorithm named after him, Shor's algorithm, how large-scale quantum computers can break our current cryptography systems, cryptographers and researchers around the world began to explore how to implement post-quantum cryptography systems. PQC is critical to the future of our digital security because data that is safe today, based on our current cryptography systems, won't be safe in the quantum computing era, which calls for the implementation of post-quantum cryptography techniques to keep these data safe. Also, PQC is critical to the future of blockchain, as cryptocurrencies and blockchain-based applications require quantum-resistant cryptographic techniques to preserve the integrity of data and assets in these decentralized and immutable ledgers.

Ethereum's Proactive Approach to Quantum Threats

Ethereum uses elliptic curve cryptography schemes, particularly elliptic curve digital security algorithm (ECDSA), for signing transactions and Boneh-Lynn-Shacham (BLS) for signature aggregation and verification. Being an offshoot of ECC, the security of ECDSA is based on the difficulty of solving discrete logarithm problems, which robust quantum computers would do easily. The vulnerability of ECDSA has necessitated the need for it to be replaced with quantum-resistant schemes. Ethereum is aware of the looming threat that quantum computing poses and has taken a major step forward by integrating quantum resistance into its roadmap.

Ethereum 2.0, named Serenity, was fully launched in late 2022 and one of its major upgrades is ditching the former Proof of Work (PoW) consensus mechanism for the Proof of Stake (PoS) consensus mechanism, which is believed to be more resistant to quantum attacks. Ethereum 2.0 also comes with the option of switching to a hash-based quantum-resistant signature scheme, such as the Lamport signature, which research has said is impractical to use because it takes up 231 times more storage than ECDSA. XMSS and PHINCS⁺ are the other hash-based stateful and stateless signature options. Furthermore, Ethereum is planning to implement a hard fork which can be strategically employed to mitigate the impact of a quantum attack by creating a divergence in the blockchain.

Ethereum 3.0 is projected to launch in 2027 and promises more robust quantum-resistant protocols such as Winternitz signature and zero-knowledge STARKs (or ZK-STARKs), which aim to safeguard transactions from quantum attacks by preventing the exposure of users' private keys. The input of Ethereum developers and the community is paving the way for actualizing the roadmap for a quantum-safe Ethereum. They have started working on developing alternative post-quantum cryptographic signature schemes and secure, resilient Ethereum protocol. According to Ethereum.org, “most of the upgrades required for future-proofing Ethereum are still in the research phase and may be several years away from being implemented.”

The Quantum Threat to Ethereum

Some cryptographic methods have been employed on the Ethereum blockchain to secure transactions on the network and preserve the integrity of the distributed ledger. However, these cryptographic methods are at risk of becoming ineffective or even broken due to the potential advancements in quantum computing technology. Ethereum's heavy reliance on ECDSA and BLS opens it up to vulnerabilities in the event of attacks from quantum computers. These vulnerabilities include the ability of malicious actors to decrypt private keys, compromise the integrity of smart contracts, and counterfeit digital signatures, which give them the power to control funds associated with those signatures.

The BLS signature scheme uses bilinear pairings with mathematical operations on elements of an elliptic curve group (BLS12-381), different from ECDSA (secp256k1). However, elliptic curve problems as a whole are vulnerable to quantum attacks. This is because a robust quantum computer with Shor's algorithm is capable of solving these problems, breaking the cryptographic security in the process and revealing sensitive user data on the Ethereum blockchain.

Also, Ethereum uses the KZG (which stands for Kate-Zaverucha-Goldberg – its original authors) commitment schemes to generate cryptographic secrets based on polynomial commitments, which allows binding a value to a commitment (polynomial function) without revealing the value itself. The risks associated with these commitment schemes are that they are inefficient, require trusted setups, and are also vulnerable to quantum computer attacks.

In the meantime, Ethereum is safe from quantum attacks because we don't yet have quantum computers that are robust enough to break the underlying cryptographic security of the

blockchain. However, when quantum computing becomes more powerful than it is today, the potential impacts it could have on Ethereum include breaking its cryptographic algorithm (ECDSA), undermining internet communication between nodes on the blockchain, and rendering transaction signatures that are used to protect assets and value stored in the ledgers useless.

Proposed Quantum-Resistant Solutions

To prepare Ethereum for the gradually approaching era of powerful quantum computing, some quantum-resistant solutions have been proposed. These include hash-based cryptography, lattice-based cryptography, code-based cryptography, multivariate polynomial cryptography, and STARK-based solutions. But out of all of these, only two solutions have gained prominent attention, which are:

- **STARK-based solutions**

ZK-STARKs (Zero-Knowledge Scalable Transparent ARguments of Knowledge) is a cutting-edge cryptography technique that uses a zero-knowledge proof system to create encrypted data that allows for easy verification without revealing any underlying information about such data. STARKs offer significant improvements such as its use of collision-resistant hash functions over the well-known ZK-SNARKSs, which rely on elliptic curves and trusted setups. One of the major benefits of ZK-STARKs is that they are more secure and quantum-resistant, thanks to their use of hash functions. Also, STARKs eliminate the need for trusted setups for its use in a blockchain network like Ethereum. In a show of support for its planned adoption of ZK-STARKs in Ethereum 3.0, the Ethereum Foundation has given a [\\$12 million grant](#) to STARKware, a company focused on developing ZK-STARKs scaling solutions.

- **Lattice-based Cryptography**

Lattice-based cryptography is a post-quantum cryptography technique that is based on the intense difficulty associated with the nearest or shortest vector problem in lattices. In this technique, the public key is generated by encrypting an arbitrary lattice point, while the private key is generated by evaluating the shortest vector in the lattice. Lattice-based cryptographic algorithms are believed by many cryptographers and researchers to be the most promising for securing data and for quantum-resistant encryption because it's based

on the worst-case hardness of calculating the shortest vector of large, multidimensional lattices.

However, with these proposed post-quantum cryptography methods come new challenges. These challenges entail efficiency issues and compatibility with existing blockchain operations. It is necessary to secure Ethereum from quantum attacks while striking a balance between efficiency and compatibility without sacrificing its scalability and performance.

Roadmap to Integration

Current progress in research and development, especially as touching post-quantum cryptography integration in Ethereum, is the implementation of an opcode that would allow users to submit STARK-based proofs, which are based on ZK-STARKs. These proofs will validate a user's knowledge of a private preimage and a public key address generated through approved hash functions, resulting in the replacement of the user's account code with a validation mechanism that is quantum attack-resistant.

Implementing post-quantum cryptography solutions, such as those mentioned above, within Ethereum blockchain is a multifaceted effort that demands complex yet crucial steps from testing to deployment. This is because integrating new cryptographic algorithms is not only about making the blockchain ecosystem more secure, especially against quantum threats, but also more efficient and scalable.

Already and as previously stated, Ethereum 2.0, known as Serenity, was launched in late 2022 and uses Proof of Stake (PoS), which is, to some extent, resistant to quantum attacks. The next upgrade, Ethereum 3.0, is expected to launch in 2027 and promises to come with a more scalable and quantum-resistant protocol, which is STARK-based.

Conclusion

While quantum attacks are currently non-existent and speculative, they constitute potential vulnerabilities that are capable of compromising the security of Ethereum in the near future. The Ethereum community has been proactive in its commitment to making Ethereum more secure and resilient against impending quantum attacks by implementing emergency response measures (such as a hard fork) and setting out a plan to integrate cutting-edge cryptography (STARK-based) solutions into its next upgrade. As advancement in quantum computing

continues, there's a need for ongoing innovation in blockchain security to safeguard the multi-billion-dollar assets that Ethereum harbors. Also, future-proofing Ethereum against quantum threats is important as it is the only programmable blockchain network for digital asset transactions and for creating decentralized applications. To go through Ethereum's official roadmap documentation, see [here](#) and [here](#). BTQ is committed to addressing the different aspects of the "quantum problem" with its four products namely: PQScale, Keelung, Kenting, and QCIM.