Ethereum and the quantum challenge

Source: AI generated

"Q-Day", which is the day quantum computers become capable of breaking current cryptographic standards, could make even the most secure digital systems vulnerable. The Bitcoin community has been debating the threat for over a year, while Ethereum's community appears to be taking its first cautious steps in 2026.

Charles-Henry Monchau, CFA, CAIA, CMT
Chief Investment Officer
charles-henry.monchau@syzgroup.com

Assia Driss
Syz Research Lab Team Coordinator
assia.driss@syzgroup.com

Hugo Morel
Syz Research Lab Team
hugo.morel@syzgroup.com

Syz PRIVATE BANKING

Introduction

Ethereum is a decentralised blockchain platform that enables smart contracts and applications to operate without intermediaries. Since its launch in 2015, it has become one of the core infrastructures of the digital asset ecosystem, supporting thousands of decentralised applications across finance, gaming and digital ownership.

The network experienced its most rapid expansion during the 2021–2022 crypto boom. At the peak, Ethereum processed more than 1.2 million transactions per day, hosted a rapidly growing ecosystem of decentralised finance protocols and NFT platforms, and saw ether rise to around $4,800, pushing its market capitalisation above $500 billion.

Since then, activity has normalised as markets cooled and competition from other blockchain networks intensified. Yet Ethereum remains a critical pillar of the crypto economy. Its operation relies fundamentally on cryptography, which allows transactions to be verified and executed without trusted intermediaries.

Advances in quantum computing, however, are beginning to challenge the long-term assumptions behind this security model. Systems that rely on public-key cryptography, including blockchains, could become vulnerable once sufficiently powerful quantum computers emerge. On Ethereum, where transactions and digital signatures are permanently recorded on-chain, data generated today could potentially be exploited in the future. Wallet addresses, validator approvals, and cryptographic proofs all rely on mathematical problems that quantum algorithms could eventually solve efficiently.

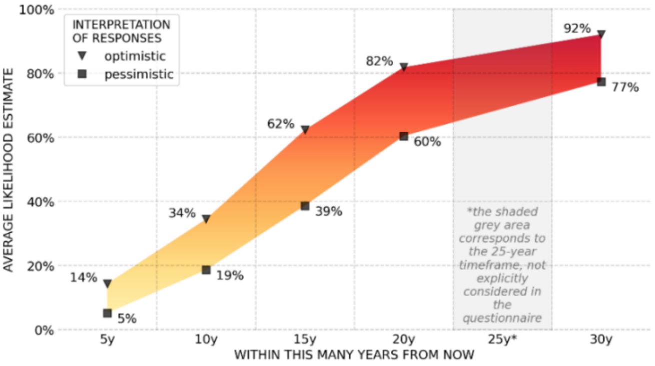
Quantum threats and cryptographic vulnerabilities in Ethereum

Quantum computing introduces a major challenge for digital security by questioning the mathematical foundations of modern cryptography. Traditional computers struggle with problems such as factoring large numbers or solving discrete logarithms, which is why public-key cryptography is considered secure today. Quantum algorithms, however, could solve these problems far more efficiently. For instance, Shor's algorithm demonstrates how a sufficiently advanced quantum machine could break the cryptographic systems that protect digital signatures and key exchanges. Blockchains rely heavily on public-key cryptography to verify ownership and validate transactions, meaning their long-term security could be significantly affected.

Estimates from researchers suggest that the probability of a quantum computer capable of breaking RSA-2048 could increase significantly over the coming decades. Survey results indicate that the cumulative probability may approach about 50% within roughly 15 years and exceed 80% within 30 years.

2024 OPINION-BASED ESTIMATES OF THE LIKELIHOOD OF A DIGITAL QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS, AS FUNCTION OF TIME

Range between average of an optimistic (top value) or pessimistic (bottom value) interpretation of the likelihood intervals indicated by the respondents



Source: Global Risk Institute

Ethereum is structurally exposed to this threat. Its transparency means public keys, signatures, and cryptographic proofs are visible on chain, allowing hackers to collect information now and potentially exploit it later as quantum computing advances. This creates a long-term, systemic vulnerability that is particularly relevant for decentralised networks.

This looming threat is not just theoretical. Ethereum's architecture contains specific components that are especially vulnerable to quantum attacks, and understanding these is key to planning effective defences.

Vitalik Buterin, Ethereum's co-founder, shared a quantum-resistance roadmap on X on 26 February 2026. He identified four main sources of vulnerability: validator signatures involved in the consensus process, Ethereum's data availability mechanisms, user wallet signatures used in daily transactions, and specific zero-knowledge proof employed by applications and layer-2 solutions.

Ethereum's proof-of-stake system uses BLS signatures to aggregate thousands of validator attestations efficiently, finalising blocks every 12 seconds. Because BLS relies on elliptic-curve cryptography, a quantum computer could forge validator signatures. For example, an attacker might simulate most validators, allowing invalid blocks to be confirmed or even triggering a chain reorganisation.

KZG commitments allow validators to check that large batches of transaction data exists without downloading everything, supporting rollups and Ethereum's scalability. Their security depends on mathematical assumptions that quantum computers could break. If compromised, a malicious operator could pretend that transaction data is available when it is not, potentially producing invalid state transitions while validators accept them as valid.

Every Ethereum wallet relies on ECDSA (elliptic curve digital signature algorithm) to control funds and authorise transactions. Once a wallet sends a transaction, its public key is exposed on chain. A quantum attacker could later derive the private key and steal the funds. For instance, large dormant wallets could be targeted years from now with "harvest now, decrypt later" attacks.

Zero-knowledge proofs enable privacy and scalability by verifying computations without revealing data. Many current zk-systems rely on elliptic-curve cryptography. If quantum computers break these assumptions, attackers could forge proofs to falsely validate application states, such as showing fake balances on layer-2 rollups, while validators accept them as legitimate.

Post-quantum security roadmap and technical solutions

Recognising these vulnerabilities, Vitalik Buterin has outlined a roadmap to gradually transition Ethereum toward post-quantum security. The strategy relies on targeted modifications across the protocol's most sensitive cryptographic layers. The goal is to replace vulnerable primitives and to preserve Ethereum's performance and scalability. As quantum-resistant cryptography often introduces higher computational costs, the proposed solutions emphasise efficiency and incremental deployment.

The first step focuses on Ethereum's consensus layer, were validator signatures secure block production and finality. These signatures rely on BLS cryptography, which is vulnerable to Shor's algorithm. Buterin proposes replacing them with hash-based signature schemes, such as variants of Winternitz signatures, which rely only on the security of hash functions and are therefore considered resistant to quantum attacks. To maintain efficiency, these signatures could be aggregated using STARKs (Scalable Transparent Arguments of Knowledge), a class of zero-knowledge proofs that does not depend on elliptic-curve assumptions. In the near term, Buterin also suggests simplifying the structure of consensus by moving toward a "lean available chain," where each slot contains significantly fewer signatures, between roughly 256 and 1,024. Reducing the number of signatures per slot lowers aggregation complexity and allows the network to transition to quantum-safe primitives without sacrificing performance. An important design decision concerns the choice of hash function underpinning the system. Several candidates have been proposed, including Poseidon2 with additional rounds for stronger security, Poseidon1 as a well-tested alternative, or conventional high-performance hashes such as BLAKE3. Selecting the right primitive will be critical to balancing efficiency and long-term security.

Ethereum's data availability layer currently relies on KZG commitments to ensure that rollup data is correctly stored and accessible. While highly efficient, KZG commitments depend on cryptographic assumptions that could be compromised by quantum computers. To address this vulnerability, Buterin proposes replacing KZG commitments with STARK-based proof systems. The transition introduces new challenges, particularly because KZG commitments possess a property called linearity that STARK constructions do not naturally replicate. As a result, additional mechanisms would be required to verify that blobs of transaction data have been constructed correctly. Buterin argues that Ethereum's scaling roadmap does not require overly complex architectures. Maintaining a one-dimensional data availability sampling structure, such as PeerDAS, should be sufficient to achieve Ethereum's throughput objectives. Recursive STARK proofs could then be used to manage proof sizes and verification efficiency. Although the transition would require significant engineering effort, it remains technically feasible and consistent with Ethereum's modular scaling strategy.

Quantum risk also extends to externally owned accounts (EOAs), which currently rely on ECDSA signatures. Once a transaction is sent, the associated public key becomes visible on chain, potentially enabling future quantum attackers to derive the private key. Buterin's solution is to implement native account abstraction, allowing accounts to adopt any signature scheme rather than being locked into ECDSA. Proposals such as EIP-8141 would introduce first-class flexible accounts capable of integrating post-quantum cryptography. The challenge lies in efficiency. Quantum-resistant signatures, whether hash-based or lattice-based, are larger and more computationally expensive to verify. While verifying an ECDSA signature costs roughly 3,000 gas today, post-quantum alternatives could require around 200,000 gas. To mitigate this cost increase, Buterin proposes introducing vectorised mathematical precompiles capable of performing operations such as multiplications, additions, and dot products more efficiently. Over time, protocol-level recursive aggregation of signatures and proofs could further compress verification costs, potentially reducing the overhead to near-negligible levels.

Zero-knowledge systems are another area where quantum-resistant alternatives introduce substantial overheads. Current zk-SNARK verification typically costs between 300,000 and 500,000 gas. Replacing these with STARK-based proofs, while improving security, could increase costs dramatically, potentially reaching 10 million gas per verification. To address this issue, Buterin proposes introducing "validation frames" within the transaction structure as part of the EIP-8141 framework. These frames would allow transactions to carry structured verification data for signatures and proofs. In practice, heavy cryptographic computation would shift away from the chain itself. Instead, nodes in the mempool could aggregate and validate transactions off chain using STARK proofs before submitting them on chain. These aggregated proofs could be produced at short intervals, potentially every 500 milliseconds, allowing the blockchain to verify large batches of transactions with minimal on-chain cost. This architecture preserves scalability while transitioning to quantum-secure cryptography.

The long-term objective is to achieve a quantum-resistant layer-1 architecture before large-scale quantum computers become practical threats. Buterin has suggested that a realistic timeline for completing these upgrades would extend toward the end of the decade, potentially around 2029.

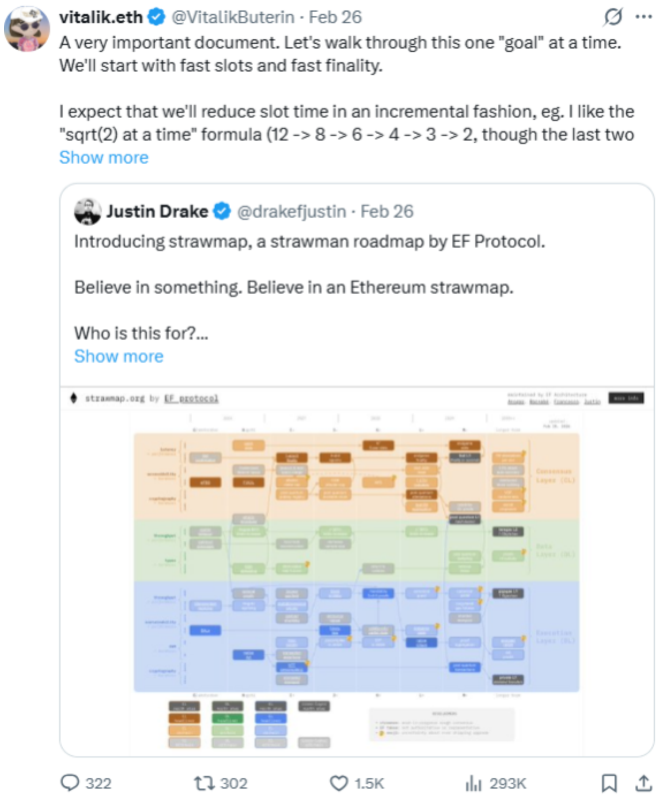
Ethereum long-term network evolution

Post-quantum security is increasingly becoming a strategic priority for Ethereum. Earlier this year, the Ethereum Foundation, the Swiss nonprofit supporting Ethereum's core research and development, formally created a dedicated post-quantum team to coordinate research, tooling and protocol upgrades aimed at strengthening the network's cryptographic foundations.

The initiative builds on several years of internal research and reflects a growing effort to prepare the network well before quantum computers become a practical threat. To accelerate progress, the foundation has begun organising bi-weekly technical discussions among developers focused specifically on quantum security and launched a $1 million incentive program encouraging researchers to improve quantum-resistant cryptography.

However, support from influential figures in the ecosystem such as Vitalik Buterin and from the Ethereum Foundation itself does not automatically translate into protocol changes. Ethereum's governance model is highly decentralised, meaning that major upgrades require broad agreement across developers and stakeholders.

This dynamic was highlighted when researcher Justin Drake published a draft development plan for the network. The document is referred to as a "strawmap", because of "the limits of drafting a roadmap in a highly decentralised ecosystem." According to Drake, in a decentralised ecosystem with many independent contributors, defining a single official roadmap that reflects all participants is effectively impossible. The strawmap therefore represents one coherent scenario among many potential trajectories for Ethereum's future development.



vitalik.eth @VitalikButerin · Feb 26

A very important document. Let's walk through this one "goal" at a time. We'll start with fast slots and fast finality.

I expect that we'll reduce slot time in an incremental fashion, eg. I like the "sqrt(2) at a time" formula (12 -> 8 -> 6 -> 4 -> 3 -> 2, though the last two

Show more

Justin Drake @drakefjustin · Feb 26

Introducing strawmap, a strawman roadmap by EF Protocol.

Believe in something. Believe in an Ethereum strawmap.

Who is this for?...

Show more

322 302 1.5K 293K

Source: Vitalik Buterin on X

Conclusion

Ethereum, just like Bitcoin, faces the challenge posed by quantum computing, but the two networks approach it differently. Bitcoin places a strong emphasis on immutability and broad consensus, favouring slow, stability-focused changes. Ethereum prioritises adaptability and user-level flexibility, allowing faster experimentation and the potential deployment of quantum-resistant solutions at the account level. These structural differences are likely to shape how each network prepares for quantum risks and may ultimately influence how investors, developers, and users engage with them.

Welcome to
Syzerland®

For further information

Banque Syz SA
Quai des Bergues 1
CH-1201 Geneva
T. +41 58 799 10 00
syzgroup.com

Charles-Henry Monchau, CFA, CAIA, CMT
Chief Investment Officer
charles-henry.monchau@syzgroup.com

Assia Driss
Syz Research Lab Team Coordinator
assia.driss@syzgroup.com

Hugo Morel
Syz Research Lab Team
hugo.morel@syzgroup.com

This marketing document has been issued by Bank Syz Ltd. It is not intended for distribution to, publication, provision or use by individuals or legal entities that are citizens of or reside in a state, country or jurisdiction in which applicable laws and regulations prohibit its distribution, publication, provision or use. It is not directed to any person or entity to whom it would be illegal to send such marketing material.

This document is intended for informational purposes only and should not be construed as an offer, solicitation or recommendation for the subscription, purchase, sale or safekeeping of any security or financial instrument or for the engagement in any other transaction, as the provision of any investment advice or service, or as a contractual document. Nothing in this document constitutes an investment, legal, tax or accounting advice or a representation that any investment or strategy is suitable or appropriate for an investor's particular and individual circumstances, nor does it constitute a personalized investment advice for any investor.

This document reflects the information, opinions and comments of Bank Syz Ltd. as of the date of its publication, which are subject to change without notice. The opinions and comments of the authors in this document reflect their current views and may not coincide with those of other Syz Group entities or third parties, which may have reached different conclusions. The market valuations, terms and calculations contained herein are estimates only. The information provided comes from sources deemed reliable, but Bank Syz Ltd. does not guarantee its completeness, accuracy, reliability and actuality. Past performance gives no indication of nor guarantees current or future results. Bank Syz Ltd. accepts no liability for any loss arising from the use of this document.