

Quantum Computing and Bitcoin: Why 'Q-Day' Is Not an Existential Threat

Recent advances in quantum computing raise long-term concerns for Bitcoin's security, but the threat is not immediate. Experts estimate that vulnerable cryptography could be phased out between 2029 and 2035 through protocol upgrades and new cryptographic standards. Migration will require careful coordination, but Bitcoin can adapt without risking instant failure. Overall, quantum risk is a future issue related to governance and timing, not an urgent crisis.

April 22, 2026 at 08:51 AM By **David Zaslowsky**



cryptocurrency bitcoin crime

Recent advances in quantum computing have reignited a persistent concern: that Bitcoin's cryptographic foundation could one day be compromised. "Q-Day" is the hypothetical point in time

when a sufficiently powerful quantum computer becomes capable of breaking widely used public-key encryption systems. A recent Google paper suggesting Q-Day might be closer than previously believed has understandably captured the attention of investors and fiduciaries. The reality, however, is more nuanced.

This article examines which parts of the Bitcoin network are potentially vulnerable to quantum attacks, which are not, why the issue is best understood as a conventional technological transition rather than an existential crisis, and what fiduciaries should be thinking about in light of Q-Day.

The Quantum Countdown: A Growing Institutional Consensus

For fiduciaries, the most critical question is not the precise date of a hypothetical “quantum break,” but how much time remains to execute a safe and orderly transition. While some technologists continue to debate whether a sufficiently powerful quantum computer is an “if” rather than a “when,” major regulatory and technology institutions have begun planning on the assumption that the threat will eventually materialize.

That emerging consensus generally views the timeline through three practical lenses.

1. The “Harvest Now, Decrypt Later” Risk (Current)

We are already in a phase in which adversaries may be collecting cryptographic targets today with the expectation that they could be exploited years in the future, once quantum capabilities mature.

For Bitcoin, this risk is most relevant to “exposed wallets”—situations in which a public key has already been published on the blockchain. While private keys cannot be derived using today’s computers, public keys do not change once exposed, meaning the vulnerability exists in a static form from the moment of disclosure.

2. The 2029–2030 “Deprecation” Window

In a March 2026 white paper, Google Quantum AI demonstrated—under documented theoretical assumptions involving a fully fault-tolerant quantum computer (a machine capable of performing accurate, large-scale calculations by identifying and correcting its own internal errors in real time)—that an exposed elliptic curve private key (a private key that has become vulnerable to extraction because its corresponding public key is visible on a public ledger) could in principle be derived in minutes, often summarized as a “nine-minute” attack. No such machine exists today, but the white paper materially compressed earlier estimates and reframed the discussion as a planning issue rather than a distant abstraction.

The U.S. National Institute of Standards and Technology (NIST), whose cryptographic standards are widely followed by regulators and industry, has also indicated that legacy public-key

cryptography—such as RSA and elliptic-curve signatures— is expected to begin phased deprecation around 2030 in favor of post-quantum algorithms.

Together, these developments did not create an immediate crisis, but they transformed quantum risk from a theoretical concern into a concrete, medium-term issue.

3. The 2035 “Disallowance” Horizon

NIST’s current roadmap further contemplates that by approximately 2035, vulnerable public-key cryptographic algorithms should be fully disallowed for secure communications in regulated environments. Although these timelines formally govern U.S. government systems, they have historically functioned as de facto benchmarks for the private sector as well.

For the Bitcoin ecosystem, this five-to-ten-year window represents the runway required to design, test, and coordinate a transition to post-quantum cryptographic standards. For fiduciaries, it signals that, while there is no immediate emergency, there is a clear need for awareness. Institutions with long-duration exposure to digital assets will likely observe increasing attention to how these transitions develop and how risk is assessed as the cryptographic baseline evolves.

Why Quantum Risk Does Not Mean Bitcoin “Breaks”

A common misconception is that the advent of a sufficiently powerful quantum computer would immediately “switch off” the Bitcoin network. In reality, Bitcoin would continue to operate, and the protocol is capable—through broad consensus—of adopting quantum-resistant cryptographic standards over time.

The challenge is not instantaneous network failure, but the complexity of transitioning existing value to new cryptographic schemes, particularly for funds associated with exposed or unrecoverable keys. In that sense, quantum risk is less about sudden collapse and more about a difficult and uneven migration process.

1. The Upgrade Path: The “Soft Fork”

Bitcoin has a history of implementing significant protocol upgrades through consensus-based changes known as “soft forks,” such as SegWit in 2017 and Taproot in 2021. A soft fork is a backward-compatible update to the protocol where new rules are more restrictive than the old ones.

Because the new blocks are still valid under the old rules, the network does not split into a new blockchain. Discussions of how the network might address future quantum risk often assume using a soft fork yet again. A soft fork can introduce new, quantum-resistant address and

signature formats while permitting legacy formats to remain valid during a potentially extended transition period.

An analogy may be helpful. This is akin to a bank announcing a move to a higher-security vault system with new locks. The institution itself continues operating, but customers are encouraged—over time—to relocate assets from older vaults to the new facility. Unlike a traditional bank, however, Bitcoin cannot compel that migration, and assets left in legacy formats may face different risk profiles as cryptographic conditions evolve.

This approach necessarily implicates what is often described as the “lost coins” dilemma. A non-trivial portion of the Bitcoin supply is widely believed to be held in addresses for which the private keys have been lost or are otherwise unrecoverable, including coins associated with the network’s pseudonymous creator, Satoshi Nakamoto. Because these assets cannot be moved by their owners, they cannot be voluntarily migrated to new, quantum-resistant “vaults.”

That reality introduces a complex question of social consensus. If legacy formats were ever broadly viewed as vulnerable to a quantum-capable attacker, the network would face difficult tradeoffs. One path would be to permit the continued validity of legacy outputs, even if doing so creates the risk that such coins could eventually be claimed through cryptographic attacks. Another—far more controversial—approach would be to adopt protocol rules that restrict or disable the spending of unmigrated legacy outputs in order to preserve broader network security.

This tension underscores that a quantum transition would present not only a technical challenge, but also a governance and philosophical one—forcing the community to balance immutability, property norms, and collective security in a way few prior upgrades have required.

2. Post-Quantum Cryptography (PQC)

The proposed “new locks” are not hypothetical. They already exist in the form of post-quantum cryptographic (PQC) algorithms—cryptographic methods designed to remain secure even against adversaries equipped with large-scale quantum computers. Such algorithms are the subject of active standard-setting efforts and are already being adopted—primarily in hybrid form—in several security-sensitive environments.

In the Bitcoin context, a transition to quantum-resistant signatures would likely involve a multi-step, operational process:

- developers integrating one or more quantum-resistant signature schemes into the protocol;
- users generating new, quantum-resistant address types; and

— asset holders voluntarily transferring Bitcoin from legacy addresses into the new formats over time.

While technically feasible, this process would be more complex than prior cryptographic upgrades, reflecting tradeoffs around efficiency, adoption, and coordination. As with earlier transitions, success would depend not only on code, but on widespread user participation and social consensus.

3. Mining and Quantum Resistance

It is also important to distinguish Bitcoin’s mining process—the mechanism by which transactions are validated and blocks are added to the blockchain—from the digital signature system used to authorize spending. Mining relies on cryptographic hashing, not public-key encryption, and is therefore significantly more resistant to quantum attacks. While quantum computers could in principle provide a modest advantage in hashing, that advantage is limited and does not fundamentally undermine the security model.

Even if quantum-enhanced mining were to emerge, Bitcoin’s protocol automatically adjusts mining difficulty in response to changes in aggregate hash power. This adjustment mechanism has long absorbed major shifts in computing capability—from CPUs to GPUs to specialized ASICs—treating new efficiency gains as part of the normal evolution of mining hardware.

As a result, mining does not present the same category of quantum risk as digital signatures used for transaction authorization. The more acute challenges lie in how ownership is proven and migrated, not in how blocks are produced.

4. The Bottom Line: A Governance and Timing Challenge

The challenge facing Bitcoin is less akin to a sudden system failure and more like a critical piece of infrastructure requiring scheduled structural reinforcement. Such an effort would demand careful coordination and broad global consensus, but it would build on cryptographic techniques and upgrade mechanisms that are already well understood.

Framed this way, the principal risk is not a failure of mathematics, but a coordination gap—whether the network can coordinate migration to new cryptographic standards before cryptographically relevant quantum computers become a practical reality. That question places quantum risk squarely in the realm of governance, incentives, and collective action, rather than abrupt technological breakdown.

Conclusion: An Issue to Watch, Not a Crisis to Solve

Quantum computing does not present an immediate operational threat to Bitcoin or other digital assets. It does, however, introduce a category of future infrastructure risk—one that institutional market participants, regulators, and technologists are increasingly factoring into forward-looking analysis.

For lawyers and fiduciaries, the relevance of the quantum discussion lies less in predicting technological breakthroughs and more in understanding how digital-asset systems evolve over time, how security assumptions change, and how those changes are managed through governance and consensus rather than sudden disruption.

As with many emerging technology issues, quantum risk is best understood not as a problem demanding immediate action, but as a developing backdrop against which future disclosures, custody arrangements, and risk assessments may eventually be evaluated.

This article is intended as a general analysis of technological and legal developments. It does not address any specific investment, custody, or fiduciary decision and should not be considered legal advice.

David Zaslowsky *is a partner at Baker McKenzie.*

Page printed from: <https://www.law.com/newyorklawjournal/2026/04/22/quantum-computing-and-bitcoin-why-q-day-is-not-an-existential-threat/?slreturn=20260423163302>

NOT FOR REPRINT

© 2026 ALM Global, LLC, All Rights Reserved. Request academic re-use from www.copyright.com. All other uses, submit a request to asset-and-logo-licensing@alm.com. For more information visit [Asset & Logo Licensing](#).