Bitcoin Policy Institute

STATE OF PLAY

April 2026

Quantum Computing and Bitcoin's Path Forward

On March 31, 2026, two major research papers landed on the same day and together reshaped the conversation about quantum computing and Bitcoin.

The first, from Google's Quantum AI team, addressed a question that has loomed over the network for years: how powerful does a quantum computer need to be to break Bitcoin's cryptography? Bitcoin's security rests on a math problem that classical computers cannot solve in any reasonable timeframe. But quantum computers, using a technique called Shor's algorithm, could theoretically solve it. For years, the consensus estimate was that an attacker would need roughly 10 million qubits — a unit of quantum computing power — putting the threat somewhere in the mid-2030s at the earliest. **Google's paper showed the same attack could be executed with fewer than 500,000 qubits: a twenty-fold reduction.** The goalposts moved significantly.

The second paper, from researchers at Caltech, Oratomic, and UC Berkeley, went further. Using a different approach to quantum hardware and a novel error-correction technique, they demonstrated the attack could theoretically be performed with as few as 10,000 to 26,000 specialized qubits. The two teams were not contradicting each other. One optimized the software; the other improved the hardware efficiency. Together, they point in the same direction: **the resource requirements for a quantum attack on Bitcoin's cryptography are coming down faster than most experts expected.**

<500K	~10K	105
Qubits needed per Google	Qubits needed per Caltech	Qubits on Google's best chip today

The Threat in Context

These papers do not mean Bitcoin is in danger today. The most advanced quantum computers in existence have a few thousand qubits. Google's own leading chip, Willow, has 105. The gap between where quantum hardware stands and where it would need to be to break Bitcoin's cryptography remains vast. But the Bitcoin community must prepare now for a post-quantum future.

The most important and least understood part of this story is that **workable technical solutions already exist, and Bitcoin developers are actively building them.**

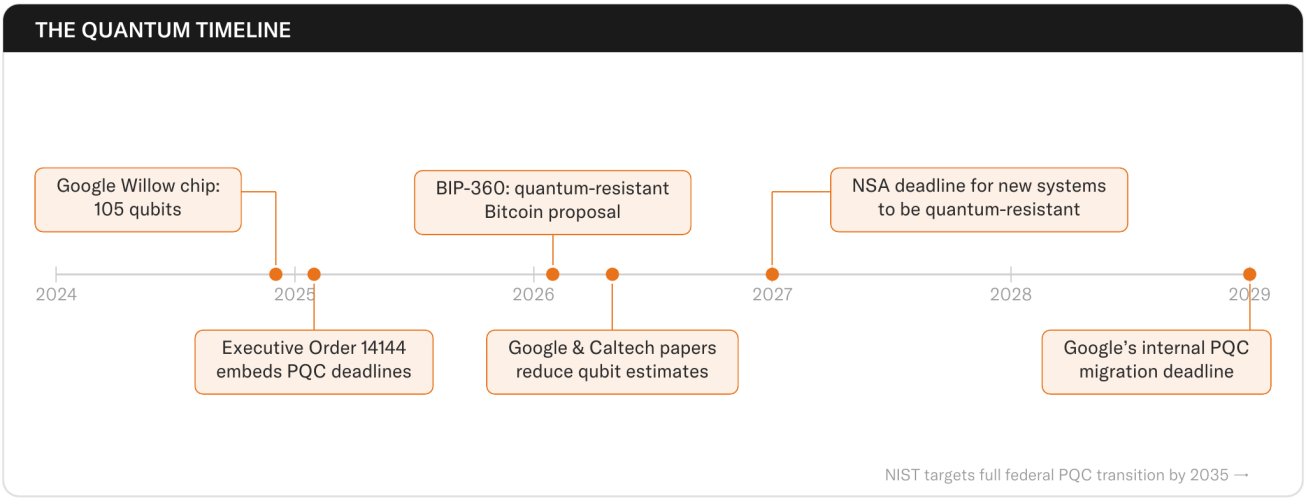
Bitcoin Is Preparing

The narrative that Bitcoin developers are asleep at the wheel is inaccurate. The leading post-quantum proposal — Bitcoin Improvement Proposal 360, or BIP-360 — has generated more developer discussion than any proposal in the protocol's history. The work is substantial, and the people behind it are experienced cryptographers.

BIP-360 proposes a new type of Bitcoin address where the cryptographic key is never visible, even when funds are spent. Under the current design, creating a Bitcoin address is a bit like placing your house key in a locked box on the front porch: the box protects the key, but the moment you open it, anyone watching can see it. BIP-360 eliminates that exposure entirely. It is designed as the foundation onto which a quantum-resistant signature system could eventually be built. This update aims to address the most urgent vulnerability now while preserving flexibility for future cryptographic decisions. A working testnet implementing BIP-360 launched in March 2026, with over 50 miners, more than 100,000 blocks processed, and contributions from over 100 cryptographers.

Beyond BIP-360, Bitcoin's most recent major upgrade — Taproot, activated in 2021 — already contains architectural scaffolding for quantum resistance. Every Taproot transaction includes hidden fallback spending conditions that can be configured to require quantum-safe verification. The upgrade path is already built into the protocol.

The broader cryptographic building blocks are also in place. In August 2024, the National Institute of Standards and Technology finalized three post-quantum cryptographic standards designed to replace the algorithms that quantum computers threaten. These standards are ready for deployment, and Bitcoin developers can draw from them as the network's transition takes shape.



The Policy Landscape

The federal government has already begun its own migration to post-quantum cryptography. Executive Order 14144, issued in January 2025, embedded post-quantum deadlines into federal cybersecurity requirements for the first time. NIST has given federal agencies until 2035 to complete the transition. Google has set an internal deadline of 2029.

This context matters for understanding Bitcoin's position. When quantum computers threaten the same cryptography that secures banking, military communications, and government systems, those institutions can push software updates or issue mandates. Bitcoin cannot. It is a decentralized network with no CEO, no board of directors, and no ability to compel anyone to upgrade. That is one of Bitcoin's greatest strengths, but it is also the dimension that requires the most careful attention.

The good news is that Bitcoin has navigated complex protocol upgrades before. SegWit in 2017 and Taproot in 2021 both demonstrated the network's ability to coordinate major changes through deliberative, decentralized consensus. And unlike previous upgrade debates, which were fundamentally disputes about Bitcoin's identity, quantum security is a challenge where every participant's incentives align: no one benefits from an insecure network.

Looking Ahead

The quantum threat to Bitcoin is neither imminent nor insurmountable. Cryptographic tools to make Bitcoin quantum-resistant already exist, and the development work is underway. The question is less about finding a technical solution and more about the network forging consensus on how and when to deploy one.

The Bitcoin Policy Institute will continue to keep policymakers informed of the work that developers, cryptographers, and other network participants are doing to prepare Bitcoin for a post-quantum future.

The Bitcoin Policy Institute (BPI) is a non-profit, non-partisan think tank advancing sound Bitcoin policy through research, education, and direct engagement with policymakers. Support our mission at btcpolicy.org/donate.