

Source Map

How Quantum Computing Could Challenge Bitcoin—and the Race to Secure the Future of Digital Money

A compact map of the main public technical source families used to frame the manuscript. It is not the book's complete Works Cited. Draft proposals are identified as drafts; forecasts and estimates remain attributed to their sources.

1. Babbush et al. (2026) - Google Quantum AI / collaborators

Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations. Core 2026 resource-estimate reference for Shor-type attacks on elliptic-curve cryptography; treated as a resource estimate, not evidence that such a machine exists. [Source](#)

2. Milton & Shikhelman - Chaincode Labs (2025)

Bitcoin and Quantum Computing: Current Status and Future Directions. Bitcoin-specific threat model, exposed-key issues, mining/signature distinctions, and migration constraints. [Source](#)

3. Neha Narula - MIT Digital Currency Initiative (2026)

Bitcoin and Quantum Computing: A Roadmap. Staged migration framing, deployment questions, open problems, and the distinction between protecting individual users and protecting Bitcoin as a system. [Source](#)

4. Project Eleven - Pruden & Deegan (2026)

The Quantum Threat to Blockchains - 2026 Report. Cross-chain threat modeling, quantum-readiness framework, migration difficulty, and attributed Q-Day scenarios. The book does not adopt its baseline date as a prediction. [Source](#)

5. BIP 360 - Pay-to-Merkle-Root (P2MR)

Draft consensus proposal. A quantum-resistant script-tree output designed to reduce long-exposure ECC risk while explicitly not solving short-exposure attacks that may require post-quantum signatures. [Source](#)

6. BIP 361 - Post Quantum Migration and Legacy Signature Sunset

Draft / Informational proposal. Explores a staged sunset of legacy ECDSA/Schnorr use after a post-quantum output path exists; used as a live example of the migration, incentive, and dormant-coin debate. [Source](#)

7. NIST Post-Quantum Cryptography standards

FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA), plus transition guidance. These provide the broader post-quantum standards context; they are not presented as plug-in Bitcoin solutions. [Source](#)

8. Bitcoin primary specifications and developer literature

The Bitcoin white paper and relevant Bitcoin Improvement Proposals/specifications (including Taproot/Schnorr material) provide the baseline for Bitcoin keys, scripts, signatures, and consensus terminology. [Source](#)

Source-discipline note: The manuscript separates fact, estimate, argument, proposal, and scenario. Conflicting expert positions are preserved rather than collapsed into a single "Bitcoin community" view.