

Technical Brief

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

PURPOSE

This one-page note defines the claim boundaries used throughout the advance review copy. It is intended to make technical review faster and to prevent the book from being read as a sensational prediction. Factual corrections, missing caveats, and disagreement are welcome before publication lock.

WHAT THE BOOK CLAIMS - AND DOES NOT CLAIM

- **No fixed Q-Day.** The book does not assign a confident arrival date to a cryptographically relevant quantum computer (CRQC). Timelines are treated as uncertain ranges, scenarios, or attributed estimates.
- **No present-day Bitcoin break.** The book does not claim that current publicly known quantum hardware can recover Bitcoin private keys or break Bitcoin signatures today.
- **Shor and Grover are kept separate.** Shor-type attacks are treated as the core public-key/signature threat because a sufficiently capable CRQC could solve the elliptic-curve discrete-log problem. Grover-type search provides a quadratic speedup and is not treated as an equivalent break of Bitcoin mining or hash security.
- **Exposure is not uniform.** The book distinguishes long-exposed public keys, keys revealed only when spent, address reuse, Taproot/P2TR exposure, and other categories. “Exposed” does not mean stolen, lost, or inevitably compromised.
- **Migration is the central engineering problem.** The book treats post-quantum readiness as a protocol, wallet, infrastructure, governance, deployment, and user-migration problem - not merely a matter of choosing a new signature algorithm.
- **Proposals are labeled by status.** BIP 360 (P2MR) and BIP 361 are discussed as Draft proposals, not adopted Bitcoin consensus. The manuscript does not imply that Bitcoin has selected a final post-quantum migration path.

REQUESTED TECHNICAL FEEDBACK

Please flag anything that is technically wrong, stale, overstated, under-qualified, or missing an important tradeoff - especially around signature exposure, resource estimates, post-quantum migration design, consensus/deployment, or the handling of uncertainty. No endorsement or positive review is expected.