Getting a Quantum Upgrade Adopted Is a Security Problem

Josh · Secure Sovereign

Bitcoin Security Consortium · Published October 1, 2026

A research proposal to the Bitcoin Security Consortium. October 2026.

The gap

A quantum-resistant upgrade protects Bitcoin only after the network adopts it. No one can mandate that. Thousands of independent node operators have to run the new rules, miners and economic nodes have to enforce them, and holders have to move their coins. An upgrade that stalls protects nothing. One that activates under contested legitimacy adds chain-split risk on top of the quantum exposure it was meant to remove. Adoption failure is a security failure.

The design space is wide and still open. Candidate output types include P2MR (BIP-360), P2TRv2, P2TRH, and P2QR, compared side by side in the PQC output type discussion on Delving Bitcoin. Leading signature candidates are hash-based, including SHRINCS and SHRIMPS from Blockstream researchers. For coins that never move, the options range from leaving legacy spends valid, to rate-limiting them, to commit-then-reveal migration, to a sunset with a recovery path as in BIP-361.

Several of the central disputes are adoption questions in technical form. P2TRv2 keeps today's fee profile and wallet behavior to win broad early adoption, and relies on a later consensus change to disable elliptic-curve spends. P2MR gives up some spend efficiency for protection that does not depend on that later change. Which tradeoff holds up depends on how quickly users adopt an output type under each design, and on whether a contested elliptic-curve disable could activate when it is needed.

Existing migration estimates bound how long migration would take given block space. They do not say how quickly holders will actually choose to move, which is the constraint most likely to bind. Estimates of exposed supply run from about ten thousand coins at near-term risk to roughly a third of all bitcoin, depending on the exposure model, and much of the exposed value sits with a small number of large custodians. This proposal measures the behavioral side with data.

What I propose

A research report that analyzes the network conditions a quantum migration depends on and maps the realistic paths to adoption, with the failure modes of each. The report would serve as input to the consortium's published material on Bitcoin's security. It would cover four areas.

1. **Activation precedent.** The SegWit and Taproot histories from proposal to activation, including the activation-method disputes (BIP 148 and BIP 91 in 2017, the LOT=true versus LOT=false debate and Speedy Trial in 2021). The output is what each episode shows about timelines, about where consensus held and where it nearly broke, and what that history implies for a follow-up change, such as an elliptic-curve disable, that may face organized opposition.

2. **Behavioral migration rates from chain data.** Existing work, including the Chaincode Labs post-quantum report, Presidio Bitcoin's readiness report, and ongoing Delving Bitcoin and bitcoin-dev discussions on migration incentives, bounds migration time by block space. This section measures holder behavior. It tracks how quickly value moved to each new output type after activation (P2SH, SegWit, Taproot), separates custodial and exchange flows from individual holders where chain heuristics allow, and tests how fee profile and wallet support shaped each curve. The result is a set of realistic adoption curves to set against each candidate design, and a bound on how much supply any legacy-coin policy would actually catch.

3. **Process conditions.** A quantitative picture of how consensus changes move through review and merge, drawn from an existing dataset covering Bitcoin Core development from 2010 to 2026 across GitHub, the development mailing list, and IRC. This section establishes what the development pipeline can realistically carry, and on what timeline.

4. **Design and failure-mode map.** For the leading designs, and the combinations of output type, signature scheme, and legacy-coin policy their authors propose, the report sets out what has to be true for adoption, which follow-up consensus changes the design depends on, where the path can split the network, and which observable signals would show it is on or off track. The framework takes new proposals as they appear, so the map stays current as the design space moves.

The report will not recommend a specific proposal or activation method. It describes conditions and risks so that developers, node operators, and holders can make that call with better information. This keeps the work consistent with the consortium's position of not advocating code changes.

Optional workstream

A migration rule is easier to review when it is stated precisely and tested on more than one codebase before activation. I wrote a formal mathematical specification of Bitcoin's consensus rules (the Orange Paper) and maintain an independent Rust node built from it. As an optional extension, I can express a candidate output type or opcode, such as P2MR or a SHRINCS verification opcode, in the specification, implement it in the independent node, and differential-test it against the proposal's reference implementation. Disagreements between two independent implementations of the same rule text surface ambiguities before any activation discussion.

What already exists

- **Governance dataset.** Bitcoin Core development from 2010 to 2026, drawn from GitHub pull requests, reviews, and comments, the development mailing list, and IRC. github.com/secsovereign/bitcoin-governance-research
- **Orange Paper.** A formal specification of Bitcoin consensus, with consensus functions checked against it using Z3. thebitcoincommons.org/spec.html
- **Independent node.** Built from that specification, with extensive differential tooling against Bitcoin Core in its bench tool, blvm-bench. github.com/BTCDecoded

Collaboration

I will coordinate with other prominent researchers in this space, including the authors of the leading proposals, to review the technical sections.

Disclosure

I build an independent Bitcoin implementation, I have written critically about Bitcoin Core's governance model, and I have argued publicly that implementation diversity strengthens the network. A report on adoption conditions touches those questions. I am stating the interest up front so the method can be judged on its own terms. Every finding will rest on public data, and the dataset and analysis code will be published with the report.

Deliverables and timeline

- **Report.** Final report with published data and analysis code, delivered 16 weeks from start. An interim draft goes to the funder at week 8 for factual review. Conclusions remain mine.
- **Optional workstream.** Six additional weeks.

SECURESOVEREIGN
Markdown is the canonical source: https://secsov.com/proposals/quantum-adoption/index.md
Formatted snapshot of https://secsov.com/proposals/quantum-adoption
Josh · Secure Sovereign