BIP-360: Making Bitcoin (Taproot) Quantum-Resistant

Summary

BIP-360 is a Bitcoin soft fork proposal enabling quantum-resistant Tapscript functionality through the introduction of a new output type: Pay to Tapscript Hash (P2TSH).

Proposed P2TSH output types are, essentially, Taproot addresses with the quantum-vulnerable keypath spend disabled - removing risks associated with potential breaks in elliptic curve cryptography by quantum computers or other mathematical or technical advancements.

At present, Taproot addresses - which are critical for Lightning, most Layer 2s, and various other protocol developments - are one of the few Bitcoin address types vulnerable to "long-exposure" quantum attacks. BIP360 aims to address this vulnerability as a first step in a broader series of potential quantum mitigation efforts.

Importantly, the introduction of P2TSH addresses also lays the technical groundwork for integrating post-quantum signature algorithms in future upgrades, without the need for a hard fork.

Why BIP-360

Bitcoin's current signature model is based on Elliptic Curve Cryptography (ECC), which is potentially vulnerable to attacks from sufficiently advanced quantum computers using Shor's algorithm. Once a public key is revealed (e.g. in certain address formats, or after a spending transaction), such addresses are vulnerable to quantum theft.

As of 2025, over 6.7 million bitcoin reside in addresses vulnerable to long-exposure quantum attacks, including P2PK and Taproot addresses (~2M bitcoin) and re-used addresses (~4.7M). BIP-360 proposes a quantum-resistant Tapscript-supportive address type as a proposed first step in Bitcoin's broader quantum mitigation strategy.

How P2TSH Works

- Eliminates key path spend: Commits instead to the script path, omitting the public key currently used in P2TR output types — explanation video.
- Maintains Taproot compatibility: Leverages existing Taproot/tapscript infrastructure.
- Supports future post-quantum signatures: Built to accommodate signatures like ML-DSA (Dilithium) and SLH-DSA (SPHINCS+) via follow-up soft forks.
- Backwards compatible and low-risk: Requires no hard fork or block size increase; minimal disruption for wallets and nodes.

Global Context
Governments and global industry leaders are rapidly accelerating their quantum computing defenses:

- The NSA's CNSA 2.0 mandates quantum safe cryptography by 2030.
- NIST plans to disallow ECC in federal systems after 2035.
- Billions of dollars are being invested in and by companies including IBM, Google, Microsoft, PsiQuantum, and others, in quantum R&D.
- Multiple experts have warned and been vocal about the quantum threat, not only to Bitcoin, but to cryptography in general.

BIP-360 is Bitcoin's response to the quantum threat, aligned with the broader global transition.

BIP 360 Authors
Hunter Beast — Bitcoin developer and Sr. Protocol Engineer at MARA
Ethan Heilman — Cryptographic researcher and co-author of OP_CAT
Isabel Foxen Duke — Bitcoin communications consultant and editor

Contact
For interviews and press inquiries - contact:
isabel.duke@mara.com
diego.vera@mara.com

Resources
Website: https://bip360.org
Hunter Beast official headshot