BIP-360: Enabling Quantum-Resistance for Bitcoin

Summary
BIP-360 is a Bitcoin Improvement Proposal that introduces Pay to Quantum Resistant Hash (P2QRH) — a new output type that mitigates one of the most pressing long-term risks to Bitcoin: the ability of future quantum computers to break public key cryptography.

P2QRH strengthens Bitcoin's resistance to quantum attacks by removing the key-spend path found in Taproot (P2TR) outputs, which can expose public keys and enable private key recovery in a quantum scenario. It also lays the technical groundwork for integrating post-quantum signature algorithms in future upgrades, without the need of 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. after a transaction), it becomes a target. It's also important to note that Taproot and P2PK addresses expose their public key even before spending.

As of 2025, over 6 million bitcoin reside in quantum exposed addresses, including P2PK, reused SegWit, and Taproot outputs. These coins are at risk of long exposure quantum attacks, where public keys remain on chain indefinitely.

BIP-360 also mitigates short exposure attacks, scenarios where a powerful enough quantum computer could recover a private key while a transaction is still waiting to be mined.

How P2QRH Works

- Eliminates key path spend: Commits instead to the merkle root, omitting the ECC that is currently used in P2TR — explanation video.
- Maintains Taproot compatibility: Leverages existing Taproot/tapscript infrastructure.
- Supports future post-quantum signatures: Built to accommodate algorithms 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 technology firms are rapidly advancing toward practical 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.

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

Authors
Hunter Beast — Bitcoin developer and Sr. Protocol Engineer at Anduro
Ethan Heilman — Cryptographic researcher and co-author of OP_CAT

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

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