21ST CAPITAL

BITCOIN VS. QUANTUM

Jan. 2025

Is Bitcoin at Risk from Quantum Computers?

Author: Ziya S.
Date: January 16, 2025
Email: contact@21stcapital.com
www.21stcapital.com

Is Bitcoin at Risk from Quantum Computers?

Bitcoin's security relies heavily on the Elliptic Curve Digital Signature Algorithm (ECDSA) for key generation and signatures. But, as the development of quantum computers accelerates, a question arises: Could quantum computers eventually break Bitcoin's cryptography and compromise the security of funds stored in wallets?

The Short Answer: Not Today

Right now, Bitcoin is not at risk from quantum computers. The technology required for quantum computers to break Bitcoin's cryptographic defenses is still decades away. Even if quantum computers eventually become capable of breaking ECDSA, it's expected that advancements in cryptography will outpace this risk.

Looking Ahead: Post-Quantum Cryptography (PQC)

Despite the current lack of immediate threat, there is ongoing discussion in the Bitcoin developer community about how to make Bitcoin quantum-resistant in the future. Developers are exploring the concept of Post-Quantum Cryptography (PQC) as a safeguard against future quantum threats.

For example, forums like the Bitcoin-dev mailing list and *Delving Bitcoin* have seen some discussions on approaches to quantum-resistant Bitcoin. Developers are discussing algorithms like:

SPHINCS+, a hash-based signature algorithm, is one of the prominent candidates being explored. While it is secure, its downside is the large signature size — about 17KB — which is quite large for the Bitcoin network.

Alternatively, **SQISignHD**, a more compact solution, is also gaining attention. This algorithm is only about 30% larger than the current ECDSA, making it a potentially more feasible choice for Bitcoin's future scalability.

How Could Bitcoin Adapt to Post-Quantum Cryptography?

The key challenge with adopting PQC for Bitcoin is how to implement it without compromising the network's performance. One approach that has been discussed is implementing a **soft fork** when quantum computers become a genuine threat. This would involve encouraging users to adopt quantum-resistant measures by incentivizing users with block space discounts (similar to what we did with the SegWit soft fork)

Another possible solution involves **locking dormant coins**. For instance, a proposal by Bitcoin developer achow101 suggests locking unspent transaction outputs (UTXOs) until an owner can provide zero-knowledge proofs (zk-proof) to confirm ownership. This would help protect coins from quantum threats without disrupting the entire network.

> "For example, users could provide a proof that they have the BIP 32 seed that was used to derive the private key for the given public key. Since it is a Zero-Knowledge Proof, the seed itself is not exposed (note that the seed is not part of a public-private keypair so there is no public component that is shared). Since most wallets use BIP 32, this should be sufficient. There may be other ways to prove ownership without risking coins that have not been thought of yet."

The Challenge of Balancing Security and Scalability

The biggest hurdle to implementing PQC in Bitcoin is the trade-off between security and scalability. While stronger cryptographic systems may offer greater security, they often come with increased computational requirements, potentially slowing down the network.

Why the Conversation Matters

While it's clear that quantum computers are not an immediate threat, it's crucial to engage in technical discussions about the future. These conversations help develop a roadmap for how Bitcoin could adapt if the need for PQC arises. It also helps assess how quickly the network could adopt new tools and strategies to fend off future quantum threats.

A Bigger Picture: Global Impact of Quantum Computers

It's also worth noting that if quantum computers ever become powerful enough to threaten Bitcoin's security, they wouldn't just disrupt Bitcoin. They would pose a risk to global systems that rely on cryptography, including military, banking, and energy sectors. Bitcoin won't face the quantum threat alone — the world's reliance on cryptography means that a quantum breakthrough would be a global issue, not just a Bitcoin problem.

In conclusion, while quantum computing poses theoretical risks to Bitcoin's cryptography, it's still far from a present concern. However, the ongoing discussions and proposals for a quantum-resistant Bitcoin show the foresight of developers working to ensure Bitcoin's security in the future. As technology advances, the Bitcoin community continues to be proactive in preparing for whatever the future might hold.