BTQ

↖ Back to blog

MAY 2, 2024

Quantum Secure Cryptocurrencies of the Future

Explore how quantum-resistant cryptography is shaping the future of cryptocurrencies like Bitcoin and Ethereum. Learn about the latest standards from NIST and delve into innovative solutions to safeguard digital currencies against quantum threats.

Digital currencies like Bitcoin and Ethereum are here to stay. These cryptocurrencies are built on the blockchain, which helps keep transactions safe and secure while being trustless and verified by a consensus mechanism. These cryptocurrencies have even expanded financial access to people who are unbanked.

However, quantum computing could change the landscape of digital currencies. Quantum computers work very differently from the computers we use today. They can solve complex problems much faster. This speed is great for science and medicine, but it's a problem for cryptocurrencies because many rely on encryption vulnerable to quantum computers. Right now, regular computers can't easily solve these problems, which keeps the transactions secure.

But with large enough quantum computers, someone could steal your coins and re-direct your transactions because the transactions are secured with vulnerable cryptographic schemes. Does that mean digital currencies are going to be hacked? Luckily, the National Institute of Standards and Technology (NIST) has been working on researching and standardizing post-quantum cryptography for almost a decade.

Quantum Readiness in Cryptocurrencies

In 2024, NIST expects to publish its post-quantum cryptographic standards, a milestone in the effort to secure digital information against the quantum threat. These standards will specify algorithms designed to be resistant to the capabilities of quantum computers. Among these algorithms are CRYSTALS-Dilithium, CRYSTALS-KYBER, and SPHINCS+, which are moving ahead to the final standardization steps.

So, the challenge is, do we completely wipe the slate clean and create new cryptocurrencies with quantum resistance, or upgrade old ones? Some people say there's little chance of getting consensus to upgrade the larger coins, and Bitcoin will be defunct sooner or later. So, a few cryptocurrencies have begun implementing quantum-resistant algorithms, though the algorithms for post-quantum cryptographic standards haven't been fully approved.

Quantum-resistant cryptocurrencies typically use a variety of cryptographic families that are believed to be secure against quantum computing attacks.

These families include:

- Hash-Based Cryptography: Relies on the security of hash functions and includes algorithms like the Extended Merkle Signature Scheme (XMSS).
- Code-Based Cryptography: Based on the difficulty of decoding generic linear codes.
- Lattice-Based Cryptography: Utilizes the complexity of lattice problems, such as the shortest vector problem, to ensure security.
- Multivariate Cryptography: Involves multivariate polynomials over a finite field.

Quantum-resistance is not new, but some cryptocurrencies have been ahead of the curve by building quantum-first.

Mochimo

Mochimo is a cryptocurrency specifically designed with quantum resistance in mind. It uses the WOTS+, a Winternitz-type one-time signature scheme. While they acknowledge the key sizes of quantum signatures, they have put additional work into reducing key sizes for scalability and efficiency.

Quantum Resistant Ledger (QRL)

The Quantum Resistant Ledger (QRL) was developed to be resistant to classical and quantum computing attacks from the beginning. They bet on a future early, where quantum computers will exist that will break encryption. It uses XMSS, a hash-based digital signature scheme. QRL's approach is unique as it was one of the first cryptocurrencies to implement quantum-resistant technology from the ground up.

QRL's blockchain uses a multi-algorithm mining approach, which includes algorithms like Sha256, Scrypt, Skein, Qubit, and Odocrypt. This diversity in mining algorithms contributes to the decentralization and security of the network.

And QRL's design includes the potential for future upgrades and enhancements. This adaptability is key to maintaining relevance and security in the rapidly evolving field of blockchain technology. This "crypto-agility" will be important not just for blockchains, but for any company that transacts online.

New Research and Roadmaps

Some other cryptocurrencies are exploring the quantum-resistance space. Cardano publishes work on quantum resistance, but is not currently implementing it into the cryptocurrency roadmap. While currently not quantum resistant, Ethereum has released a roadmap with plans to upgrade to zero-knowledge proofs and quantum resistance in the future.

Challenges for Quantum-Resistant Blockchains

As cryptocurrencies evolve to combat the threat of quantum computing attacks, they face several significant challenges.

Balancing Strength and Efficiency

One of the primary challenges is developing cryptographic systems that are both quantum-resistant and efficient. The algorithms designed to resist quantum attacks often need more processing power, leading to potential issues in scalability and speed, which affect the user experience. You can't wait for 10 minutes to confirm a transaction! Finding a balance between the strength of cryptography and its practical implementation in terms of computational resources is critical for practical quantum cryptography.

Industry-Wide Standardization

Another missing piece of the puzzle to quick quantum-resistance adoption is achieving industry-wide standardization for quantum-resistant algorithms. To upgrade blockchains, there's a need for a consensus within the cryptocurrency industry on adopting these standards, even within its own core developers and voters. Some of these cryptocurrencies went ahead and started using certain cryptographic schemes that are not yet approved, but others are waiting for official confirmation from NIST to create a roadmap for upgrading the cryptography.

Importance of Early Preparation

The upcoming NIST standards release is important for organizations to keep an eye on as they prepare for the quantum era. The NSA, CISA, and NIST created a roadmap that underlines the need for organizations to develop a quantum-readiness roadmap and start preparing for the implementation of these new standards in all industries, including cryptocurrency and blockchain. This includes engaging with technology vendors, conducting an inventory of cryptographic systems, and creating migration plans that prioritize sensitive and critical assets. The time for business to start getting quantum-ready is today!

Quantum Computing Won't Kill Cryptocurrencies

These challenges show the complex pieces involved in transitioning to quantum-resistant cryptography, whether building a cryptocurrency from scratch or upgrading blockchains. Balancing efficiency with security and achieving consensus for standardization is key to the successful implementation of quantum-resistant technologies.

Despite these challenges, the proactive steps taken by projects Ethereum and Quantum Resistant Ledger (QRL) demonstrate a strong commitment to securing the future of cryptocurrencies. The blockchain industry is one of the most advanced in the awareness of the quantum computing threat. Though there are different approaches to solving the quantum threat, whether it is building a blockchain from scratch or forking it to upgrade the system, as we move forward, the collaborative effort between cryptography experts, blockchain developers, and standardization bodies like NIST will allow blockchain technology to thrive.

BTQ