Quantum Safe Coin (QSC)

qsc.fdn@gmail.com

2025.02.16 (v1.0)

Abstract

Quantum Safe Coin (QSC) is a next-generation cryptocurrency designed to address the existential threat quantum computing poses to classical blockchain cryptography. Built on an enhanced iteration of the Quantum Resistant Ledger (QRL), QSC introduces groundbreaking advancements:

1. **Automated One-Time Signature (OTS) Management**: Each QSC address is preloaded with over 1 million OTS keys, eliminating user complexity.
2. **Instant Address Generation**: Address creation time reduced to 2 seconds (vs. minutes in traditional QRL implementations).
3. **Energy-Efficient CPU Mining**: A sustainable, decentralized mining mechanism resistant to ASIC/GPU dominance.

With a total supply of 100 million QSC tokens and a focus on quantum-safe cryptography, QSC aims to become the standard for secure, future-proof digital assets.

1. Introduction

The Quantum Threat

Most cryptocurrencies (e.g., Bitcoin, Ethereum) rely on Elliptic Curve Cryptography (ECC) and SHA-256 hashing for security. Quantum computers, using Shor’s Algorithm, can break ECC and RSA encryption exponentially faster than classical computers. This means that private keys could be extracted from public keys, allowing attackers to steal funds or forge transactions. Cryptocurrencies aim to be long-term stores of value. If quantum computers become powerful enough, non-quantum-resistant coins could be completely compromised. Hence, developing a post-quantum secure crypto coin ensures that funds remain safe even in a quantum era.

It is very urgent to prevent attacks against "Harvest Now, Decrypt Later" nowadays, since quantum computers are ready to be used commercially widely. **Adversaries may already be collecting encrypted blockchain data**, planning to decrypt it once quantum computers become powerful enough. Therefore, a quantum-secure blockchain ensures that **even past transactions remain secure**.

Governments and financial institutions are increasingly interested in **quantum-safe cryptography**. A cryptocurrency that is **quantum-resistant** could gain **regulatory approval** and attract institutional investment. Organizations like **NIST (National Institute of Standards and Technology)** are already standardizing **post-quantum cryptographic algorithms**. Implementing **lattice-based cryptography, hash-based signatures (like SMSS^{MT})** can ensure long-term security.

Why QSC?

QSC addresses this by leveraging hash-based post-quantum signatures and innovative optimizations. QSC builds on QRL's foundation but introduces critical improvements:

- **User-Friendly OTS Management**: Users no longer need to manually manage OTS keys. For one hand, it is inconvenient for users to manage OTS keys each time. For the other hand, it is prone to errors. If the OTS keys are manually managed by users, it is possible to see duplicate keys used in real transactions. Consequently, the attackers can use the duplicate public keys to crack the private keys. Hence, it is not safe with this OTS management mechanism. In QSC, the OTS keys are automatically managed to ensure no duplicate public keys will be used.
- **Faster Address Generation**: Optimized algorithms based on XMSS^{MT} reduce address creation time to 2 seconds. The OTS keys are organized with multiple tree structures to significantly improve the generation efficiency.
- **Eco-Friendly Mining**: CPU-first consensus ensures accessibility and energy efficiency. The mining intensity can be adjusted based on CPU computation power, so that even low computation power CPUs can be used for mining.

---

2. Technology Overview

Enhanced Architecture

QSC uses a modified version of QRL's Merkle tree-based XMSS (Extended Merkle Signature Scheme) with the following upgrades:

Automated OTS Management

- Each QSC address is generated with **>1 million OTS keys** stored securely in a decentralized network layer.
- Users interact seamlessly without managing keys manually, reducing risk of key exhaustion.

Lightning-Fast Address Generation

- Traditional QRL address generation slows significantly with large Merkle tree heights (e.g., 20 minutes for height 20).
- QSC's **optimized algorithms** enable address creation in **2 seconds**.

Quantum-Safe Consensus Mechanism

- **Proof-of-Work (PoW)**: CPU-optimized mining algorithm based on RandomX to ensure decentralization and energy efficiency.
- **Resistance to Shor's/Grover's Algorithms**: Hash-based signatures ($XMSS^{MT}$) secure transactions against quantum attacks.

---

3. Tokenomics

Supply Distribution

- **Total Supply**: 100,000,000 QSC
- **Mining Rewards**: 60,000,000 QSC (60%) allocated to CPU miners over 100 years.
- **Development & Ecosystem**: 20,000,000 QSC (20%).
- **Community & Partnerships**: 10,000,000 QSC (10%).
- **Reserve Fund**: 10,000,000 QSC (10%) for future upgrades.

Note that initially the 40,000,000 coins will be under the **QSC Foundation** control. With the project progress, these coins will be allocated to corresponding participants accordingly.

Mining Mechanism

- **CPU-First Design**: Prioritizes energy efficiency and accessibility.
- **Dynamic Difficulty Adjustment**: Ensures fair rewards for small-scale miners.
- **Halving Cycle**: Rewards halve every 4 years to mimic Bitcoin's scarcity model.

---

4. Advantages Over Competitors

Feature	**QSC**	**Traditional QRL**
OTS Management	Fully automated (>1M keys/address)	Manual user management
Address Generation Time for height 20	2 seconds	Minutes to hours
Mining Hardware	CPU-only, compatible with low energy CPUs (eco-friendly)	CPU-only

Quantum Resistance	XMSS^{MT} with automated key rotation	XMSS with manual key rotation

5. Roadmap

- **Q4 2024**: Testnet launch with OTS automation and fast address generation.
- **Q1 2025**: Mainnet release, including QSC node, wallet (Python).
- **Q2~Q3 2025**: Block explorer release; mobile wallet release.
- **Q4 2025**: Partnerships with firms for exchange enlist preparations.
- **Q1 2026**: Exchange enlist.
- **Q2 2026 ~ future**: R &D for advanced secure features.

6. Team & Advisors

Founder: Dr. HE XueJian, Jim, the main project leader with rich experiences in blockchain, cryptography and AI.

7. Conclusion

QSC represents a paradigm shift in blockchain security, combining quantum resistance with user-centric design. By solving key limitations of QRL and prioritizing sustainability, QSC is positioned to lead the post-quantum era of decentralized finance.

Disclaimer

This document is for informational purposes only. It does not constitute financial advice.

Contact: qsc.fdn@gmail.com
Website: https://qsc-fdn.github.io/