

Quantum Safe Token (QSE) Whitepaper

Version 1.0 — August 2026

QSE Team

August 24, 2026

Abstract

Quantum Safe Token (QSE) is a quantum-resistant crypto asset fully deployed at the application layer of Ethereum. By directly integrating SHA-256-based W-OTS+ and Merkle tree signature verification into smart contracts, QSE allows ordinary users to store crypto assets under a quantum-safe identity without waiting for Ethereum’s underlying protocol to upgrade.

This whitepaper details the technical implementation of QSE and its innovative tokenomics, including a dual-layer mechanism where ordinary tokens and quantum-safe tokens coexist. High-value assets are stored and transferred under quantum-safe identities, while only a minimal amount of tokens remain in ordinary form for gas fees and daily small payments. The ecosystem also includes time-lock staking and wallet installation airdrops, aiming to build a sustainable and genuinely quantum-threat-resistant crypto economy.

Contents

1	Background and Motivation	3
2	QSE Token Basic Information	3
3	Technical Architecture	3
3.1	ERC-20 Base Token	3
3.2	Quantum-Safe Vault	4
3.3	User’s Quantum-Safe Identity and Mnemonic	4
3.4	Windows Wallet with 12 Languages, Integrating Quantum-Safe Vault, Airdrop, Time-Lock Staking, and ETH/QSE Transfers	4
4	Decentralized Airdrop of Ordinary QSE (100 QSE × 1 Million Wallets)	5
4.1	Security and Fairness	5
5	Innovative Tokenomics	5
5.1	“Quantum-Safe Behavior Is Value” — Dual-Layer Mechanism	5
5.2	Time-Lock Staking	6
6	Token Allocation	6
7	Team and Security	6

8	Risk Disclaimer	6
9	Conclusion	7

1 Background and Motivation

Quantum computers breaking cryptography is a “Sword of Damocles” hanging over the crypto industry — sometimes called the “Quantum Damocles Sword.”

- **Core threat:** A sufficiently powerful quantum computer can run Shor’s algorithm to derive a private key from a public key. This means attackers could directly seize assets, rendering traditional mathematically based cryptographic systems instantly vulnerable.
- **Not hypothetical:** Research continues to lower the barrier. By 2026, researchers had already broken simplified keys on real quantum hardware. Analysts estimate that the probability of a quantum computer cracking a specific Bitcoin private key could reach 10% by 2032.

The threat is no longer a distant assumption. Traditional digital signature schemes such as ECDSA and EdDSA are vulnerable to Shor’s algorithm, while a full migration of Ethereum’s base layer to post-quantum cryptography may still take years.

QSE believes asset security cannot wait. By using smart contract programmability, we have built a quantum-safe vault at the application layer that is independent of the underlying chain. Through economic incentives, quantum resistance is no longer a privilege of a few experts, but a standard feature available to everyone.

2 QSE Token Basic Information

Item	Description
Token name	Quantum Safe Token
Token symbol	QSE
Total supply	100,000,000,000 (100 billion)
Decimals	18
Network	Ethereum mainnet
Token standard	ERC-20
Contract license	MIT
Quantum-safe primitive	W-OTS+ (W=16, n=32) + Merkle tree height 15
Hash function	SHA-256 (Ethereum precompiled contract)
Signature capability	Each QSE quantum-safe wallet supports 32,768 quantum-safe signatures. Users can create multiple wallets, so total signatures are unlimited.

3 Technical Architecture

3.1 ERC-20 Base Token

QSE is a standard ERC-20 token with a fixed supply. The entire supply is minted to the deployer address at deployment, with no additional issuance capability. All tokens are initially managed by the project team for ecosystem development, airdrops, time-lock staking rewards, and liquidity provision.

3.2 Quantum-Safe Vault

The quantum-safe vault is an independent smart contract called `QuantumSafeVault`. Inside the wallet, users can:

- **A. Deposit:** Transfer ordinary QSE into the vault and bind it to a quantum-safe identity (Merkle Root), making the assets quantum-safe.
- **B. Withdraw:** Extract QSE from the vault to a specified ordinary Ethereum address (EOA). This requires a valid W-OTS+ signature and the corresponding Merkle proof.
- **C. Quantum-to-quantum transfer:** Send quantum-safe QSE directly to another quantum-safe identity (Merkle Root), also requiring a W-OTS+ signature and Merkle proof.
- **D. Receive:** Users can publicly share their quantum-safe address (Merkle Root) to receive quantum-safe QSE.

Key features:

- **SHA-256 only:** All hash operations call Ethereum’s native `sha256` precompile. Gas cost is approximately 150,000–200,000 per withdrawal/transfer (may vary with network conditions).
- **One-time use:** Each W-OTS+ index can only be used once. The contract enforces this to prevent reuse.
- **Decentralized verification:** Anyone can verify all quantum-safe transactions on-chain, with public data visible on Etherscan logs — no third-party trust required.

3.3 User’s Quantum-Safe Identity and Mnemonic

A user’s quantum-safe identity is derived from a standard BIP39 12-word mnemonic. The mnemonic generates a 512-bit seed, which then derives 32,768 W-OTS+ private keys via a deterministic process. Users only need to back up 12 words to recover all quantum-safe assets in any compatible wallet, eliminating traditional private key files.

3.4 Windows Wallet with 12 Languages, Integrating Quantum-Safe Vault, Airdrop, Time-Lock Staking, and ETH/QSE Transfers

The wallet is designed for Windows with automatic adaptation to 12 languages. If a translation is missing, English is displayed by default.

The QSE quantum-safe wallet includes a user-customizable RPC option. Leaving it blank uses public nodes; users can enter a custom RPC (such as Infura/Alchemy) to run the wallet in a decentralized manner.

When the wallet’s remaining quantum-safe signatures drop to 1,000 or fewer, the wallet reminds the user to create a new wallet and migrate assets (each new wallet has 32,768 signatures).

Addresses and QR codes for ETH / QSE and quantum-safe QSE can be copied and saved, making sharing and receiving convenient.

4 Decentralized Airdrop of Ordinary QSE (100 QSE × 1 Million Wallets)

4.1 Security and Fairness

- No email or centralized verification; fully decentralized.
- Gas fees are paid by users, preventing Sybil attacks.
- Each wallet address can claim only once.

5 Innovative Tokenomics

5.1 “Quantum-Safe Behavior Is Value” — Dual-Layer Mechanism

QSE’s economic model revolves around “quantum-safe behavior is value,” using a **dual-layer mechanism of ordinary tokens and quantum-safe tokens**:

- **High-value assets are stored and transferred under quantum-safe identities**, enjoying quantum attack protection.
- **Only a minimal amount of tokens remain in ordinary form for gas fees and daily small payments**, preserving daily convenience.

This design makes quantum computer attacks on crypto assets unprofitable. QSE pioneers quantum-safe behavior, and as more crypto assets adopt similar mechanisms, the “Quantum Damocles Sword” hanging over the industry will be removed, unlocking tremendous value.

(The following points are market analysis perspectives, not project team promises.)

Eliminating the “Quantum Discount” to Release Suppressed Valuation

Markets have already priced a certain “quantum discount” into crypto assets.

- Some analyses suggest quantum risk may have suppressed Bitcoin’s valuation by about 30%.
- Once the threat is formally removed, the risk discount could quickly disappear, pushing prices toward fair value.

Igniting a Catalyst and Opening a Security Narrative

- **Sparking institutional enthusiasm:** Quantum risk is a major consideration for large institutions entering the market. Removing it clears a significant obstacle for larger institutional inflows.
- **Creating new investment themes:** Market funds have begun chasing “quantum-resistant” concepts. Projects that have upgraded early may enjoy a “security premium.”

5.2 Time-Lock Staking

The wallet integrates time-lock staking, with a reward pool of 20 billion QSE. Rewards will be distributed over several years, encouraging long-term holding and improving market capitalization stability.

6 Token Allocation

Category	Ratio	Amount (QSE)	Description
Wallet installation airdrop	0.1%	100 million	1 million wallets airdrop (100 QSE/wallet)
Exchange circulation	24.9%	24.9 billion	Includes centralized and decentralized exchanges
Staking and incentive pool	20%	20 billion	Time-lock staking rewards lasting several years
Team and advisors	10%	10 billion	Locked for 1 year or more
Foundation and development	15%	15 billion	Operations, development, audits, multilingual wallet maintenance
Early swap to more holders	30%	30 billion	Locked for 6 months or more from swap date

7 Team and Security

- The QSE team consists of cryptography researchers, smart contract engineers, and product designers, operating primarily in a decentralized manner.
- All contracts are audited by third parties and use OpenZeppelin standard libraries.
- The quantum-safe primitives (W-OTS+, SHA-256) implementation follows NIST post-quantum cryptography guidelines.
- Wallet code is open source (address will be published on the official website). Mnemonics and quantum-safe signatures are generated locally and never touch the network.

- **Quantum Safe Token (QSE) Founder Profile:**

Wu Wen Jiang received a Bachelor's degree in Water Supply and Drainage Engineering from Chongqing Institute of Architecture and Engineering (now Chongqing University) in 1982.

In the punched paper tape era of computing (when computers had no keyboard, monitor, or printer and relied solely on punched paper tape to input programs and data and output computation results), he was a perfect-score student in Algorithmic Language and Computer Programming.

He once worked at The Architectural Design and Research Institute of Guangdong Province.

He also studied at Boston University and Boston Architectural College.

8 Risk Disclaimer

- Quantum computing technology is still in its early stages; the actual threat may arrive later than expected, but QSE aims to be prepared in advance.
- Crypto asset markets are highly volatile; participants should bear their own risks.
- This whitepaper does not constitute investment advice.

9 Conclusion

Quantum Safe Token (QSE) brings post-quantum cryptography from academic papers into a practical user wallet, pioneering the large-scale application of quantum-resistant assets. The unique tokenomics deeply ties quantum-safe behavior to token value, driving growth in demand, circulation, and narrative simultaneously. The dual-layer mechanism of ordinary tokens and quantum-safe tokens makes quantum computer attacks on crypto assets unprofitable and has the potential to unlock massive value for the entire crypto industry. Quantum Safe Token (QSE) is poised to become the preferred quantum-safe crypto asset for Super Intelligence agents.

Official Website: <https://8qse.com>