

Quantum Safe Token (量子安全代币 QSE) 白皮书

版本 1.0

2026 年 8 月

摘要

Quantum Safe Token (量子安全代币 QSE) 是一种在以太坊应用层实现的量子安全加密资产。它通过智能合约直接集成基于 SHA-256 的 W-OTS+ 与 Merkle 树签名验证，使普通用户无需等待以太坊底层协议升级，即可将加密资产存储在抗量子计算攻击的“量子安全身份”之下。

本白皮书详细阐述 QSE 的技术实现与创新代币经济学，包括普通代币与量子安全状态双层运行机制、时间锁质押、钱包空投等设计，旨在建立一个可持续的、真正抗量子威胁的加密经济生态。

1. 背景与动机

量子计算机破解密码，是悬在加密行业头上的“达摩克利斯之剑”（也称“量子达摩克利斯之剑”）。

- 威胁核心：**足够强大的量子计算机能运行 Shor 算法，从公开的“公钥”反向推导出“私钥”。这意味着黑客可直接掌控资产，传统基于数学难度的加密体系将瞬间失效。
- 并非空谈：**研究不断降低破解门槛。2026 年已有研究者在真实量子硬件上破解了简化版密钥。分析师估计到 2032 年，量子计算机破解特定比特币私钥的概率可能达到 10%。

量子计算对现有区块链的威胁已不再是遥远假设。ECDSA 与 EdDSA 等传统数字签名方案在 Shor 算法面前不堪一击，而以太坊底层全面迁移至后量子密码学仍需数年。

QSE 项目认为，资产安全不能等待。我们利用智能合约的可编程性，在应用层构建了与底层无关的量子安全金库，并通过一套经济学激励，使抗量子保护不再是少数专家的特权，而是任何人均可轻易获取的标准配置。

2. QSE 代币基本信息

项目	说明
代币名称	Quantum Safe Token
代币符号	QSE

项目	说明
总供应量	100,000,000,000 (1000 亿)
小数位数	18
网络	以太坊主网
代币标准	ERC-20
合约许可证	MIT
量子安全原语	W-OTS+ (W=16, n=32) + Merkle 树高度 15
哈希函数	SHA-256 (以太坊预编译合约)
量子安全签名能力	每个 QSE 量子安全钱包可进行 32768 次量子安全签名，用户可创建多个钱包

3. 技术架构

3.1 ERC-20 基础代币

QSE 为标准 ERC-20 代币，供应量固定，部署时一次性铸造至部署者地址，无增发能力。所有代币初始由项目方管理，用于生态建设、空投、时间锁质押奖励及流动性提供。

3.2 量子安全金库

量子安全金库是一个独立智能合约 `QuantumSafeVault`，用户可在钱包内完成以下操作：

- **A. 存入：**将普通 QSE 存入金库，与一个量子安全身份（Merkle Root）绑定，成为“量子安全状态”下的资产。
- **B. 提取：**将量子安全状态下的 QSE 提取至指定的普通以太坊地址（EOA）。该操作需要提供有效的 W-OTS+ 签名及对应的 Merkle 证明。
- **C. 量子对量子转移：**将量子安全状态下的 QSE 直接发送至另一个量子安全身份（Merkle Root），同样需要 W-OTS+ 签名与 Merkle 证明。
- **D. 接收：**用户可公开分享自己的量子安全地址（Merkle Root），用于接收量子安全状态的 QSE。

核心特征：

- 完全基于 **SHA-256**：所有哈希运算调用以太坊原生 `sha256` 预编译，Gas 成本约为每次提取/转移 15~20 万 Gas（可能因网络状况波动）。

- 一次一密：每个 W-OTS+ 索引仅能使用一次，合约强制标记，杜绝重用。
- 去中心化验证：任何人均可在区块链上验证所有量子安全交易，数据公开可查，无需信任第三方。

3.3 用户的量子安全身份与助记词

用户的量子安全身份由一个 BIP39 标准 12 单词助记词确定派生。助记词生成 512 位种子，再通过种子派生 32768 组 W-OTS+ 私钥。用户只需备份 12 个单词，即可在任何兼容钱包中恢复全部量子安全资产，彻底告别传统私钥库文件。

3.4 集成量子安全金库、空投、时间锁质押及 ETH/QSE 收发的 12 种语言 Windows 自适应钱包

钱包设计为 Windows 自适应 12 种语言，若所选语言翻译缺失，默认显示英文。

QSE 量子安全钱包设有用户自定义 RPC 选项，留空采用公共节点；用户填写自定义 RPC（如 Infura/Alchemy 节点）即可去中心化地运行钱包。

当钱包的量子安全签名次数不大于 1000 时，钱包会提醒用户创建新钱包并迁移资产（每个新钱包有 32768 次签名）。

ETH / QSE 及量子安全 QSE 的地址和二维码均可复制和保存，方便分享和接收。

4. 普通 QSE 去中心化空投（100 QSE × 100 万钱包）

4.1 安全与公平

- 无需邮箱或中心化验证，完全去中心化。
- Gas 费由用户自付，防止女巫攻击。
- 每个钱包地址仅可领取一次。

5. 创新代币经济学

5.1 “量子安全行为即价值”双层运行机制

QSE 的经济模型围绕“量子安全行为即价值”设计，采用普通代币与量子安全状态双层运行：

- 大量高价值的代币以量子安全身份存储和相互转移，享受抗量子攻击的保护。
- 只余极少价值的代币以普通身份用于 Gas 支付和日常小额支付，维持日常便利。

这种设计使量子计算机破解加密资产变得不再有利可图。QSE 率先实践量子安全行为，随着更多加密资产采用类似机制，悬在加密行业头上的“量子达摩克利斯之剑”将被移除，从而为整个行业释放巨大价值。

（以下为市场分析观点摘引，不代表项目方承诺。）

 消除“量子折扣”，释放被压抑的估值

目前市场已对加密资产价格计入了一定程度的“量子折扣”。

- 有分析认为，量子风险因素可能压低了比特币估值约 30%。
- 一旦威胁被正式解除，相关风险折扣可能快速消失，推动价格向公允价值回归。

 点燃催化剂，开启安全叙事

- 激发机构热情：量子风险是大型机构入场时的重要考量，消除该风险将为更大规模资金流入扫清障碍。
- 催生新投资主题：市场资金已开始追捧“抗量子”概念，提前布局的项目可能获得“安全溢价”。

5.2 时间锁质押

钱包内集成时间锁质押功能，质押奖励池总量为 200 亿 QSE，奖励将持续多年发放，鼓励长期持有，提升市值稳定性。

6. 代币分配

类别	比例	数量（QSE）	说明
安装钱包空投	0.1%	1 亿	100 万钱包空投（100 QSE/钱包）
交易所流通	24.9%	249 亿	包括中心化与去中心化交易所
质押与激励池	20%	200 亿	时间锁质押奖励延续数年
团队与顾问	10%	100 亿	锁仓 1 年或以上
基金会与开发	15%	150 亿	运营、开发、审计、多语言钱包维护
前期置换给更多持有者	30%	300 亿	从置换日起锁仓 6 个月或以上

7. 团队与安全

- QSE 团队由密码学研究者、智能合约工程师及产品设计师组成，主要以去中心化方式运作。
- 所有合约均经过第三方审计，采用 OpenZeppelin 标准库。
- 量子安全原语（W-OTS+, SHA-256）实现遵循 NIST 后量子密码学指南。

- 钱包代码开源（地址将公布于官网），助记词与量子安全签名均在本地生成，绝不触网。
- Quantum Safe Token（量子安全代币 QSE）创始人简介：

吴文江，1982年重庆建筑工程学院（现重庆大学）给水排水工程学士学位。
计算机穿孔纸带时代（计算机没有键盘，显示器及打印机，仅靠穿孔纸带输入程序和数据及输出计算结果），计算机算法语言及程序设计满分学生。
曾工作于广东省建筑设计研究院。
曾学习于波士顿大学及波士顿建筑学院。

8. 风险提示

- 量子计算技术仍处于早期，实际威胁可能晚于预期；QSE 项目旨在提前做好准备。
- 加密资产市场波动剧烈，参与者需自行承担风险。
- 本白皮书不构成投资建议。

9. 结论

Quantum Safe Token（量子安全代币 QSE）通过将后量子密码学从学术论文带入用户实用钱包，开创了抗量子资产的大规模应用。独特的代币经济学深度绑定量子安全行为，使 QSE 在需求、流通与叙事三个层面同步增长。普通代币与量子安全状态的双层运行机制，使量子计算机破解加密资产的行为失去价值，并有望为整个加密行业释放巨大价值。**Quantum Safe Token（量子安全代币 QSE）有望成为超级智能代理首选的量子安全加密资产。**

官网：<https://8qse.com>