

Quantum Safe Token (量子安全代幣 QSE) 白皮書

版本 1.0
2026 年 8 月

摘要

Quantum Safe Token (量子安全代幣 QSE) 是一種在以太坊應用層實現的量子安全加密資產。它通過智能合約直接集成基於 SHA-256 的 W-OTS+ 與 Merkle 樹簽名驗證，使普通用戶無需等待以太坊底層協議升級，即可將加密資產存儲在抗量子計算攻擊的「量子安全身份」之下。

本白皮書詳細闡述 QSE 的技術實現與創新代幣經濟學，包括普通代幣與量子安全狀態雙層運行機制、時間鎖質押、錢包空投等設計，旨在建立一個可持續的、真正抗量子威脅的加密經濟生態。

1. 背景與動機

量子計算機破解密碼，是懸在加密行業頭上的「達摩克利斯之劍」（也稱「量子達摩克利斯之劍」）。

- 威脅核心：足夠強大的量子計算機能運行 Shor 演算法，從公開的「公鑰」反向推導出「私鑰」。這意味著駭客可直接掌控資產，傳統基於數學難度的加密體系將瞬間失效。
- 並非空談：研究不斷降低破解門檻。2026 年已有研究者在真實量子硬體上破解了簡化版密鑰。分析師估計到 2032 年，量子計算機破解特定比特幣私鑰的概率可能達到 10%。

量子計算對現有區塊鏈的威脅已不再是遙遠假設。ECDSA 與 EdDSA 等傳統數位簽名方案在 Shor 演算法面前不堪一擊，而以太坊底層全面遷移至後量子密碼學仍需數年。

QSE 項目認為，資產安全不能等待。我們利用智能合約的可編程性，在應用層構建了與底層無關的量子安全金庫，並通過一套經濟學激勵，使抗量子保護不再是少數專家的特權，而是任何人均可輕易獲取的標準配置。

2. QSE 代幣基本信息

項目	說明
代幣名稱	Quantum Safe Token
代幣符號	QSE

項目	說明
總供應量	100,000,000,000 (1000 億)
小數位數	18
網路	以太坊主網
代幣標準	ERC-20
合約許可證	MIT
量子安全原語	W-OTS+ (W=16, n=32) + Merkle 樹高度 15
哈希函數	SHA-256 (以太坊預編譯合約)
量子安全簽名能力	每個 QSE 量子安全錢包可進行 32768 次量子安全簽名，用戶可創建多個錢包

3. 技術架構

3.1 ERC-20 基礎代幣

QSE 為標準 ERC-20 代幣，供應量固定，部署時一次性鑄造至部署者地址，無增發能力。所有代幣初始由項目方管理，用於生態建設、空投、時間鎖質押獎勵及流動性提供。

3.2 量子安全金庫

量子安全金庫是一個獨立智能合約 `QuantumSafeVault`，用戶可在錢包內完成以下操作：

- **A. 存入：**將普通 QSE 存入金庫，與一個量子安全身份（Merkle Root）綁定，成為「量子安全狀態」下的資產。
- **B. 提取：**將量子安全狀態下的 QSE 提取至指定的普通以太坊地址（EOA）。該操作需要提供有效的 W-OTS+ 簽名及對應的 Merkle 證明。
- **C. 量子對量子轉移：**將量子安全狀態下的 QSE 直接發送至另一個量子安全身份（Merkle Root），同樣需要 W-OTS+ 簽名與 Merkle 證明。
- **D. 接收：**用戶可公開分享自己的量子安全地址（Merkle Root），用於接收量子安全狀態的 QSE。

核心特徵：

- 完全基於 **SHA-256**：所有哈希運算調用以太坊原生 `sha256` 預編譯，Gas 成本約為每次提取/轉移 15~20 萬 Gas（可能因網路狀況波動）。

- 一次一密：每個 W-OTS+ 索引僅能使用一次，合約強制標記，杜絕重用。
- 去中心化驗證：任何人均可在區塊鏈上驗證所有量子安全交易，數據公開可查，無需信任第三方。

3.3 用戶的量子安全身份與助記詞

用戶的量子安全身份由一個 BIP39 標準 12 單詞助記詞確定派生。助記詞生成 512 位種子，再通過種子派生 32768 組 W-OTS+ 私鑰。用戶只需備份 12 個單詞，即可在任何相容錢包中恢復全部量子安全資產，徹底告別傳統私鑰庫文件。

3.4 集成量子安全金庫、空投、時間鎖質押及 ETH/QSE 收發的 12 種語言 Windows 自適應錢包

錢包設計為 Windows 自適應 12 種語言，若所選語言翻譯缺失，預設顯示英文。

QSE 量子安全錢包設有用戶自定義 RPC 選項，留空採用公共節點；用戶填寫自定義 RPC（如 Infura/Alchemy 節點）即可去中心化地運行錢包。

當錢包的量子安全簽名次數不大於 1000 時，錢包會提醒用戶創建新錢包並遷移資產（每個新錢包有 32768 次簽名）。

ETH / QSE 及量子安全 QSE 的地址和 QR Code 均可複製和保存，方便分享和接收。

4. 普通 QSE 去中心化空投（100 QSE × 100 萬錢包）

4.1 安全與公平

- 無需郵箱或中心化驗證，完全去中心化。
- Gas 費由用戶自付，防止女巫攻擊。
- 每個錢包地址僅可領取一次。

5. 創新代幣經濟學

5.1 「量子安全行為即價值」雙層運行機制

QSE 的經濟模型圍繞「量子安全行為即價值」設計，採用普通代幣與量子安全狀態雙層運行：

- 大量高價值的代幣以量子安全身份存儲和相互轉移，享受抗量子攻擊的保護。
- 只餘極少價值的代幣以普通身份用於 Gas 支付和日常小額支付，維持日常便利。

這種設計使量子計算機破解加密資產變得不再有利可圖。QSE 率先實踐量子安全行為，隨著更多加密資產採用類似機制，懸在加密行業頭上的「量子達摩克利斯之劍」將被移除，從而為整個行業釋放巨大價值。

(以下為市場分析觀點摘引，不代表項目方承諾。)



消除「量子折扣」，釋放被壓抑的估值

目前市場已對加密資產價格計入了一定程度的「量子折扣」。

- 有分析認為，量子風險因素可能壓低了比特幣估值約 30%。
- 一旦威脅被正式解除，相關風險折扣可能快速消失，推動價格向公允價值回歸。



點燃催化劑，開啟安全敘事

- 激發機構熱情：量子風險是大型機構入場時的重要考量，消除該風險將為更大規模資金流入掃清障礙。
- 催生新投資主題：市場資金已開始追捧「抗量子」概念，提前佈局的項目可能獲得「安全溢價」。

5.2 時間鎖質押

錢包內集成時間鎖質押功能，質押獎勵池總量為 200 億 QSE，獎勵將持續多年發放，鼓勵長期持有，提升市值穩定性。

6. 代幣分配

類別	比例	數量 (QSE)	說明
安裝錢包空投	0.1%	1 億	100 萬錢包空投 (100 QSE/錢包)
交易所流通	24.9%	249 億	包括中心化與去中心化交易所
質押與激勵池	20%	200 億	時間鎖質押獎勵延續數年
團隊與顧問	10%	100 億	鎖倉 1 年或以上
基金會與開發	15%	150 億	運營、開發、審計、多語言錢包維護
前期置換給更多持有者	30%	300 億	從置換日起鎖倉 6 個月或以上

7. 團隊與安全

- QSE 團隊由密碼學研究者、智能合約工程師及產品設計師組成，主要以去中心化方式運作。
- 所有合約均經過第三方審計，採用 OpenZeppelin 標準庫。
- 量子安全原語 (W-OTS+, SHA-256) 實現遵循 NIST 後量子密碼學指南。

- 錢包代碼開源（地址將公佈於官網），助記詞與量子安全簽名均在本地生成，絕不觸網。
- Quantum Safe Token（量子安全代幣 QSE）創始人簡介：

吳文江，1982年重慶建築工程學院（現重慶大學）給水排水工程學士學位。
計算機穿孔紙帶時代（計算機沒有鍵盤，顯示器及印表機，僅靠穿孔紙帶輸入程式和數據及輸出計算結果），計算機算法語言及程式設計滿分學生。
曾工作於廣東省建築設計研究院。
曾學習於波士頓大學及波士頓建築學院。

8. 風險提示

- 量子計算技術仍處於早期，實際威脅可能晚於預期；QSE 項目旨在提前做好準備。
- 加密資產市場波動劇烈，參與者需自行承擔風險。
- 本白皮書不構成投資建議。

9. 結論

Quantum Safe Token（量子安全代幣 QSE）通過將後量子密碼學從學術論文帶入用戶實用錢包，開創了抗量子資產的大規模應用。獨特的代幣經濟學深度綁定量子安全行為，使 QSE 在需求、流通與敘事三個層面同步增長。普通代幣與量子安全狀態的雙層運行機制，使量子計算機破解加密資產的行為失去價值，並有望為整個加密行業釋放巨大價值。Quantum Safe Token（量子安全代幣 QSE）有望成為超級智能代理首選的量子安全加密資產。

官網：<https://8qse.com>