

# QuantumCoin Whitepaper

## Introduction

QuantumCoin is the world's first quantum-resistant cryptocurrency engineered for long-term digital sovereignty. Our mission is to offer individuals ever-lasting protection against both classical and quantum-based attacks by utilizing post-quantum cryptography, specifically the Dilithium2 signature scheme.

## Purpose and Vision

QuantumCoin was created to redefine trust, privacy, and financial autonomy. Every user is in full control, protected by our proprietary RevStop system, and shielded from censorship, surveillance, and asset seizure-ever.

## Key Features

- Quantum-Safe Cryptography (Dilithium2)
- RevStop: Sovereign Wallet Security
- No Central Authority - 100% Community Driven
- Fixed Max Supply: 22,000,000 QTC
- Mining Logic: CPU only, with increasing difficulty post-genesis
- Bitcoin-style halving: Every 2 years, for scarcity and fairness

## Mining Logic

Mining does not start until the genesis block (1.25 million QTC) is fully allocated. Mining is CPU-based, non-commercial, and strategically slowed over time. Halvings occur every 2 years until the year 2090.

## Wallet and RevStop

QuantumCoin wallets are quantum-secure and user-owned. Each wallet supports RevStop, a unique toggle security system that enables users to freeze or protect funds using a USB key or passphrase. Keys must be saved securely-ever compromised, funds may be inaccessible.

## **Explorer and API**

QuantumCoin includes a blockchain explorer for transparency and developer APIs to support real-time data retrieval, transaction lookups, and integrations with external platforms.

## **Privacy and Ethics**

We do not sell user data. All user information is stored in quantum-resistant storage. No third party-including government agencies-has access. QuantumCoin is built on privacy, ethics, and financial freedom.

## **Mobile App and Future**

We are building a mobile application for easier access and real-world adoption. Biometric authentication will be supported, alongside traditional wallet sign-in. Long term, QuantumCoin will evolve into a global monetary protocol rooted in integrity-ever.

## **Conclusion**

QuantumCoin is not just a cryptocurrency; it is a decentralized movement against surveillance capitalism, centralized banking, and vulnerability to quantum threats. We invite the world to join the Quantum era. Own your future-forever. Ever.