QbitCoin Whitepaper v1.0 - English Version

Raul - Founder of QbitCoin

November 26, 2025

1 Executive Summary

QbitCoin (QBC) represents a revolution in cryptographic security by introducing RubikPoW, a quantum-resistant proof-of-work algorithm. Unlike current systems based on elliptic curves or hash functions, RubikPoW is founded on the mathematical complexity of the Rubik's Cube group, offering inherent security against quantum algorithms such as Shor and Grover.

2 Introduction

The quantum threat to current cryptocurrencies is real and growing. With the development of scalable quantum computers, algorithms like Shor could break the asymmetric encryption protecting Bitcoin and Ethereum wallets, while Grover's algorithm would halve the security of proof-of-work systems.

QbitCoin addresses this threat with RubikPoW, a proof-of-work algorithm based on the mathematical group of the Rubik's Cube. This technology provides theoretically quantum-resistant security by design, not as an add-on.

3 RubikPoW: The Quantum-Resistant Proof-of-Work Algorithm

RubikPoW is based on the mathematical group of the Rubik's Cube, a deep subject of study in abstract algebra. Security derives from the computational difficulty of solving the Rubik's Cube in its generalized n×n×n form.

The key to the system is the discrete logarithm problem in the Rubik's Cube group, where finding the minimum sequence of moves to solve a scrambled state is extremely difficult even for quantum computers.

4 Technical Implementation

Mining in QbitCoin is based on the RubikPoW protocol. A block is mined when a miner finds a valid sequence of turns that solves a scrambled cube state, subject to a hash target condition.

5 Tokenomics

The total supply of QBC is limited to 21 million coins, following Bitcoin's scarcity model, but with mathematical security designed for the quantum future.

6 Roadmap

- Q4 2025: Whitepaper v1.0 launch and first functional implementation
- Q1 2026: Public testnet with full functionality
- Q2 2026: Mainnet launch (Genesis block)
- Q4 2026: Smart contracts integration
- Q2 2027: Scalability and performance improvements

7 Conclusion

QbitCoin represents an innovative and theoretically sound solution to the quantum threat approaching the cryptographic space. RubikPoW combines advanced mathematical security with practical efficiency, offering a sustainable transition to a quantum-resistant cryptocurrency infrastructure.