QbitCoin

Investor Dossier v2

RubikPoW: The First Quantum-Resistant Blockchain

Raul
Founder and Lead Developer

QbitCoin Core Team

November 25, 2025

www.qbitcoin.io

Contents

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.

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. Distribution will be fair, with 70% allocated to mining rewards, 20% for development/community, and 10% for founders/investors.

2 Context and Quantum Threat

2.1 The Quantum Computing Threat

Quantum computing poses an existential threat to current cryptocurrencies. 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.

Studies indicate that by 2030-2040, a quantum computer could break RSA-2048 encryption and ECDSA in hours or minutes. This would put at risk over 1 trillion USD in current cryptocurrency market capitalization.

2.2 Limitations of Current Solutions

Currently, many blockchains propose additional post-quantum solutions, such as lattice-based cryptography or hash-based signatures (Merkle Signatures). However, these solutions often require significant changes to existing architecture or present disadvantages such as excessively large signature sizes.

3 Solution: RubikPoW

3.1 Mathematical Foundations

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. It has been shown that certain problems in permutation groups do not admit efficient quantum algorithms like those existing for number theory problems.

3.2 Advantages of RubikPoW

- **Theoretical Security**: Quantum resistance is inherent to the mathematical design, not an add-on.

- **Efficiency**: Can be implemented efficiently on standard hardware without requiring quantum-safe chips.
- **Adaptability**: Difficulty can be adjusted according to cube size (2×2×2 to n×n×n).
- **Fast Verification**: Solutions can be quickly verified by multiplying sequences of permutations.

4 Technical Implementation

4.1 Mining Algorithm

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.

Formally, given:

- S_0: The initial cube state generated pseudo-randomly
- H: The target hash function (similar to SHA-256 in Bitcoin)
- D: The current difficulty target

The miner searches for a solved state S_f and the sequence of moves M such that:

$$H(\text{block\_header} \,\|\, \text{solution\_hash}(M)) < D$$

4.2 Solution Verification

Solution verification involves checking that:

1. The sequence of moves solves the initial state: $S_0 + M = S_{solved}$
2. The solution hash meets the difficulty target
3. The initial state is consistent with the block header

This process is efficient and can be performed in polynomial time.

5 Tokenomics and Distribution

5.1 Supply and Distribution

- **Total Supply**: 21,000,000 QBC
- **Mining (PoW)**: 14,700,000 QBC (70%)
- **Development/Community**: 4,200,000 QBC (20%)
- **Founders/Investors**: 2,100,000 QBC (10%)

The block reward starts at 50 QBC and halves every 210,000 blocks (approximately every 4 years), following Bitcoin's model.

5.2 Incentive Model

To incentivize decentralized mining, QbitCoin implements:

- Predictable reward curve similar to Bitcoin
- Adaptive difficulty adjustment based on block times
- No premine advantage for founders
- Full transparency in initial distribution

6 Roadmap and Development

6.1 Technical Milestones

- **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

6.2 Funding and Use of Funds

- **Series A Target**: 5 million USD
- **Development**: 40% (2 million USD)
- **Marketing and Community**: 25% (1.25 million USD)
- **Advisors and Legal**: 20% (1 million USD)
- **Operations**: 15% (750,000 USD)

7 Risk Analysis

7.1 Technical Risks

- **Cryptographic Security**: Although RubikPoW appears quantum-resistant, its long-term security depends on advances in group theory.
- **Adoption**: Adoption of a new consensus algorithm requires community trust.
- **Optimization**: Algorithm efficiency could improve with new mathematical discoveries.

7.2 Market Risks

- **Competition**: Existing projects might adopt their own post-quantum solutions.
- **Regulation**: New regulations could affect mining or trading.
- **Volatility**: Cryptocurrencies experience high price volatility.

8 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.

The combination of robust mathematical foundations, solid technical implementation, and fair distribution strategy will position QBC as the first choice for investors seeking truly secure digital assets for the post-quantum future.

With an experienced team, a clear roadmap, and a committed community, QbitCoin is poised to lead the next era of cryptocurrencies.

This document is confidential and intended solely for potential investor use. It does not constitute an offer of securities in any jurisdiction.