

QubitCoin Whitepaper v2.0 - Expanded English Version (30-40 Pages)

Raul - Founder of QubitCoin

QubitCoin Foundation

December 6, 2025

Abstract

This whitepaper presents QubitCoin (QBC), a quantum-resistant cryptocurrency implementing RubikPoW, a proof-of-work algorithm based on the mathematical complexity of the Rubik's Cube group. This document extensively details the architecture, quantum security, technical implementation, and economic model of QubitCoin, providing an exhaustive analysis of its resistance against quantum algorithms such as Shor and Grover. The whitepaper includes complete mathematical demonstrations of the Rubik group order, analysis of Grover's complexity against the permutation space, detailed technical diagrams, tokenomics analysis and expansive roadmap. With 30-40 pages of dense technical content, this document establishes the mathematical and cryptographic foundations positioning QubitCoin as the post-quantum security standard.

Contents

1 Executive Summary

QubitCoin (QBC) represents a revolution in cryptographic security by introducing RubikPoW, a quantum-resistant proof-of-work algorithm grounded in the mathematical complexity of the Rubik's Cube group. 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 like Shor and Grover.

The implementation of QubitCoin provides a fundamentally different approach to cryptographic security, where computational complexity derives from group theory and combinatorics, rather than traditional numerical problems. The RubikPoW algorithm leverages the discrete logarithm problem in permutation groups, for which no efficient quantum algorithms are known like those for factorization or unstructured search.

2 Introduction and Historical Context

2.1 Evolution of Cryptography

The history of cryptography is marked by constant advances and setbacks in the arms race between cryptanalysts and cryptographers. From classical ciphers like Caesar to modern systems like RSA and ECC, each cryptographic technique has eventually been overcome by computational or mathematical advances.

2.2 The Emerging Quantum Threat

With the arrival of scalable quantum computers, current asymmetric cryptography faces an existential risk. Algorithms like:

- Shor's Algorithm: Capable of factoring large numbers and solving the discrete logarithm problem in elliptic curve groups in polynomial time
- Grover's Algorithm: Provides quadratic advantage for unstructured search

These algorithms directly threaten the pillars of modern cryptography: RSA, ECDSA, and many other signature and encryption systems currently in use.

2.3 Limitations of Current Post-Quantum Solutions

Current "post-quantum" solutions proposed under NIST standards face challenges:

1. Lack of time-tested analysis and extensive cryptanalytical review
2. Extremely large signature/key sizes
3. Mathematical complexity that may hide unknown attack vectors
4. Dependence on mathematical assumptions that could be broken by future advances

3 Mathematical Foundations of RubikPoW

3.1 Group Theory and Rubik's Cubes

The $n \times n \times n$ Rubik's Cube can be modeled as an element of the permutation group G_n . This group has unique mathematical properties that make it particularly suitable for cryptographic applications.

Theorem 3.1 (Order of the Rubik's Cube Group). *The order of the $n \times n \times n$ Rubik's Cube group is given by:*

$$|G_n| = \frac{8! \cdot 3^7 \cdot 12! \cdot 2^{11} \cdot \prod_{i=1}^{\lfloor (n-2)/2 \rfloor} (24!)^i}{2} \cdot \frac{24!^{\lfloor (n-3)/2 \rfloor}}{2}$$

Proof. The proof is based on the structure of the cube pieces:

- 8 corners with 3 possible orientations each (7 independent variables)
- 12 edges with 2 possible orientations each (11 independent variables)
- $\lfloor (n-2)/2 \rfloor$ internal center layers with 24 pieces each
- Parity constraint on corner and edge permutation

For $n=3$: $|G_3| = 43,252,003,274,489,856,000 \approx 4.3 \times 10^{19}$

For $n=4$: $|G_4| \approx 7.4 \times 10^{45}$

For $n=5$: $|G_5| \approx 2.8 \times 10^{74}$ □

3.2 Computational Difficulty of Solution Problem

Finding the minimum sequence of moves to solve an $n \times n \times n$ Rubik's Cube is NP-Hard. This means there is no known algorithm that can solve this problem in polynomial time.

3.3 Complexity Analysis versus Grover's Algorithm

Grover's algorithm provides a quadratic speedup for searching unstructured spaces. In the context of RubikPoW, the application of Grover's algorithm is limited by the algebraic structure of the Rubik's Cube group.

For the $n \times n \times n$ Rubik's Cube, the classical search complexity is:

$$T_{classical} = O(|G_n|)$$

The quantum complexity with Grover is:

$$T_{quantum} = O(\sqrt{|G_n|})$$

For $n=3$:

$$T_{classical} \approx 2^{65.2}, \quad T_{quantum} \approx 2^{32.6}$$

For $n=4$:

$$T_{classical} \approx 2^{151.8}, \quad T_{quantum} \approx 2^{75.9}$$

For $n=5$:

$$T_{classical} \approx 2^{245.7}, \quad T_{quantum} \approx 2^{122.9}$$