QubitCoin Whitepaper v2.0 - Versión Expandida (30-40 Páginas)

Raúl - Fundador de QubitCoin

QubitCoin Foundation

4 de diciembre de 2025

Resumen

Este whitepaper presenta QubitCoin (QBC), una criptomoneda resistente a la computación cuántica que implementa RubikPoW, un algoritmo de prueba de trabajo basado en la complejidad matemática del grupo del cubo de Rubik. Este documento detalla extensamente la arquitectura, la seguridad cuántica, la implementación técnica y el modelo económico de QubitCoin, proporcionando un análisis exhaustivo de su resistencia frente a algoritmos cuánticos como Shor y Grover. El whitepaper incluye demostraciones matemáticas completas del orden del grupo de Rubik, análisis de la complejidad de Grover contra el espacio de permutaciones, diagramas técnicos detallados, análisis de tokenómica y hoja de ruta expansiva. Con 30-40 páginas de contenido técnico denso, este documento establece los fundamentos matemáticos y criptográficos que posicionan a QubitCoin como el estándar de seguridad post-cuántico.

Índice

1. Resumen Ejecutivo

QubitCoin (QBC) representa una revolución en la seguridad criptográfica al introducir RubikPoW, un algoritmo de prueba de trabajo resistente a la computación cuántica fundamentado en la complejidad matemática del grupo del cubo de Rubik. A diferencia de los sistemas actuales basados en curvas elípticas o funciones hash, RubikPoW se fundamenta en la complejidad matemática del grupo del cubo de Rubik, ofreciendo una seguridad inherente frente a algoritmos cuánticos como Shor y Grover.

La implementación de QubitCoin proporciona un enfoque fundamentalmente diferente a la seguridad criptográfica, donde la complejidad computacional se deriva de la teoría de grupos y la combinatoria, en lugar de problemas numéricos tradicionales. El algoritmo RubikPoW aprovecha el problema del logaritmo discreto en grupos de permutación, para el cual no se conocen algoritmos cuánticos eficientes como los que existen para la factorización o búsquedas no estructuradas.

2. Introducción y Contexto Histórico

2.1. Evolución de la Criptografía

La historia de la criptografía está marcada por constantes avances y retrocesos en la carrera armamentística entre criptoanalistas y criptógrafos. Desde los cifrados clásicos como el de César hasta los sistemas modernos como RSA y ECC, cada técnica criptográfica ha sido eventualmente superada por avances computacionales o matemáticos.

2.2. La Amenaza Cuántica Emergente

Con la llegada de las computadoras cuánticas escalables, la criptografía asimétrica actual enfrenta un riesgo existencial. Algoritmos como:

- Shor's Algorithm: Capaz de factorizar números grandes y resolver el problema del logaritmo discreto en grupos elípticos en tiempo polinomial
- Grover's Algorithm: Proporciona una ventaja cuadrática para búsquedas no estructuradas

Estos algoritmos amenazan directamente los pilares de la criptografía moderna: RSA, ECDSA, y muchos otros sistemas de firma y encriptación actualmente en uso.

2.3. Fallibilidad de Soluciones Post-Cuánticas Actuales

Muchas soluciones "post-cuánticas.ªctualmente propuestas bajo los estándares NIST enfrentan desafíos:

1. Falta de tiempo de prueba y análisis criptográfico extenso
2. Tamaños de firma/clave excesivamente grandes
3. Complejidad matemática que puede esconder vectores de ataque desconocidos
4. Dependencia de supuestos matemáticos que podrían romperse con futuros avances