QbitCoin Whitepaper v1.0 - Versión en Español

Raúl - Fundador de QbitCoin

26 de noviembre de 2025

1. Resumen Ejecutivo

QbitCoin (QBC) representa una revolución en la seguridad criptográfica al introducir RubikPoW, un algoritmo de prueba de trabajo resistente a la computación cuántica. 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.

2. Introducción

La amenaza cuántica para las criptomonedas actuales es real y creciente. Con el desarrollo de computadoras cuánticas escalables, algoritmos como Shor podrían romper el cifrado asimétrico que protege las carteras de Bitcoin y Ethereum, mientras que el algoritmo de Grover reduciría la seguridad de los sistemas de prueba de trabajo a la mitad.

QbitCoin aborda esta amenaza con RubikPoW, un algoritmo de prueba de trabajo basado en el grupo matemático del cubo de Rubik. Esta tecnología proporciona una seguridad teóricamente resistente a cuánticos por diseño, no como una adición.

3. RubikPoW: El Algoritmo de Prueba de Trabajo Cuántico-Resistente

RubikPoW se basa en el grupo matemático del cubo de Rubik, un objeto de estudio profundo en álgebra abstracta. La seguridad se deriva de la dificultad computacional de resolver el cubo de Rubik en su forma generalizada n×n×n.

La clave del sistema es el problema del logaritmo discreto en el grupo del cubo de Rubik, donde encontrar la secuencia mínima de movimientos para resolver un estado desordenado es extremadamente difícil incluso para computadoras cuánticas.

4. Implementación Técnica

El proceso de minería en QbitCoin se basa en el protocolo RubikPoW. Un bloque se mina cuando un minero encuentra una secuencia de giros válida que resuelve un estado inicial del cubo, sujeta a una condición de hash objetivo.

5. Tokenómica

El suministro total de QBC está limitado a 21 millones de monedas, siguiendo el modelo de escasez de Bitcoin, pero con una seguridad matemática adaptada al futuro cuántico.

6. Hoja de Ruta

- Q4 2025: Lanzamiento del whitepaper v1.0 y primera implementación funcional
- Q1 2026: Testnet público con funcionalidad completa
- Q2 2026: Lanzamiento de la mainnet (Génesis block)
- Q4 2026: Integración de contratos inteligentes
- Q2 2027: Mejoras de escalabilidad y rendimiento

7. Conclusión

QbitCoin representa una solución innovadora y teóricamente sólida para la amenaza cuántica que se avecina en el espacio criptográfico. RubikPoW combina seguridad matemática avanzada con eficiencia práctica, ofreciendo una transición sostenible hacia una infraestructura de criptomoneda resistente a cuánticos.