QbitCoin (QBC)

La Primera Blockchain con Consenso basado en
Grupos de Permutación No Abelianos (RubikPoW)

WHITEPAPER TÉCNICO v2.0
Edición Institucional

Francisco Raúl Rueda Adán
Fundador y Arquitecto Jefe

Diciembre 2025

Resumen

Resumen Ejecutivo: La inminente llegada de la computación cuántica (Q-Day) dejará obsoletos los algoritmos RSA y de Curva Elíptica (ECDSA) que protegen actualmente el 99 % de la economía digital mundial, incluido Bitcoin. QbitCoin introduce una solución definitiva: **RubikPoW**. Un mecanismo de prueba de trabajo basado en la complejidad combinatoria de resolver espacios de estado en subgrupos G_n, resistente matemáticamente al Algoritmo de Shor y Grover. Este protocolo implementa una arquitectura de seguridad escalonada (del 3K al 6K) para ofrecer utilidad real desde micropagos hasta secretos de estado.

Índice general

Índice de cuadros

Capítulo 1

La Amenaza Cuántica y la Obsolescencia de Bitcoin

1.1. El Algoritmo de Shor

Los ordenadores cuánticos utilizan cúbits y superposición para resolver la factorización de enteros en tiempo polinómico $O((\log N)^3)$. Esto significa que las claves privadas de Bitcoin (secp256k1) podrán ser derivadas de las claves públicas en cuestión de horas.

1.2. La Solución QbitCoin

QbitCoin abandona la aritmética modular en favor de la **Teoría de Grupos**. La seguridad de nuestra red no depende de factorizar números, sino de encontrar el camino más corto ("Número de Dios") en un espacio de permutaciones de alta entropía.

Capítulo 2

Tecnología RubikPoW: El Motor del Consenso

2.1. Fundamentos Matemáticos

El puzzle criptográfico se basa en el Grupo del Cubo G. Para un cubo de dimensiones $N \times N \times N$, el espacio de estados Ω crece super-exponencialmente.

$$Size(N) = \frac{8! \cdot 3^7 \cdot 12! \cdot 2^{11}}{2} \approx 4{,}3 \times 10^{19} \quad (\text{para } N = 3) \tag{2.1}$$

Para nuestro nivel máximo ($N = 6$), el espacio de búsqueda supera $1{,}57 \times 10^{116}$, una cifra mayor que el número de átomos en el universo observable.

Capítulo 3

Arquitectura de Seguridad Escalonada (Tiered Security)

A diferencia de las blockchains monolíticas, QbitCoin ofrece niveles de encriptación adaptativos según la criticidad de la transacción.

Nivel	Estructura	Usuario Objetivo	Aplicación Real
3K	Cubo 3x3x3	Usuario Estándar	Pagos diarios, compras online.
4K	Cubo 4x4x4	Corporativo	Contratos B2B, Nóminas.
5K	Cubo 5x5x5	Institucional	Banca, Reservas Federales.
6K	Cubo 6x6x6	Militar/Científico	Secretos de Estado, Datos Genéticos.

Cuadro 3.1: Matriz de Seguridad y Casos de Uso de QbitCoin

3.1. Escalabilidad Infinita (XK-XK-XK)

El protocolo está diseñado para ser agnóstico a la dimensión. A medida que la computación cuántica avance, la red puede activar mediante soft-fork niveles superiores (7K, 8K...), garantizando la seguridad perpetua.

Capítulo 4

Tokenomics y Economía del Protocolo

Diseñado para ser dinero duro, escaso y deflacionario.

- **Suministro Total:** 21,000,000 QBC (Inmutable).
- **Halving:** Cada 210,000 bloques.
- **Recompensa Minera:** Basada en la dificultad del cubo resuelto. Resolver un bloque 6K otorga mayores recompensas que un bloque 3K, incentivando la inversión en hardware de alta computación.

Capítulo 5

Conclusión

QbitCoin no es solo una criptomoneda, es la infraestructura de seguridad para la era post-cuántica. Mientras otras redes tendrán que migrar o morir, QbitCoin ha nacido preparada.