QbitCoin (QBC) â€” Whitepaper tÃ©cnico completo

VersiÃ³n: 1.0
Autor / Fundador: Francisco RaÃºl Rueda AdÃ¡n
Proyecto: QbitCoin â€” "La Blockchain del Cubo CuÃ¡ntico"
Fecha de conceptualizaciÃ³n registrada: 8 de noviembre de 2025, 17:02 CET

Resumen ejecutivo (ES / EN / DE)

EspaÃ±ol
QbitCoin (QBC) es una blockchain Layer-1 diseÃ±ada para la era cuÃ¡ntica. Combina un puzzle combinatorio inspirado en el cubo de Rubik (RubikPoW), criptografÃa post-cuÃ¡ntica (PQC) para identidades y firmas, y un modelo de consenso hÃbrido (PoW/PoS) para finalizaciÃ³n. La arquitectura es escalable mediante "capas de cubos": 3x3x3 para uso general y configuraciones multi-cubo o cubos de mayor orden para requisitos institucionales.

English
QbitCoin (QBC) is a Layer-1 blockchain engineered for the quantum era. It combines a combinatorial puzzle inspired by the Rubik's Cube (RubikPoW), post-quantum cryptography (PQC) for identities and signatures, and a hybrid PoW/PoS consensus model for finality. The architecture scales via "cube layers": 3x3x3 for general use and multi-cube or larger-cube setups for institutional security.

Deutsch
QbitCoin (QBC) ist eine Layer-1-Blockchain, die fÃ¼r die QuantenÃ¤ra konzipiert ist. Sie kombiniert ein kombinatorisches Puzzle basierend auf dem Rubik-WÃ¼rfel (RubikPoW), Post-Quantum-Kryptographie (PQC) fÃ¼r IdentitÃ¤ten und Signaturen sowie ein hybrides PoW/PoS-Konsensmodell zur Finalisierung.

Ãndice

---

1 DeclaraciÃ³n de autorÃa y registro de idea

Yo, **Francisco RaÃºl Rueda AdÃ¡n**, declaro ser el autor e inventor de la idea denominada "QbitCoin: La Blockchain del Cubo CuÃ¡ntico". Fecha de creaciÃ³n y registro: **8 de noviembre de 2025, 17:02 CET**.

(RecomendaciÃ³n: generar hash SHA-256 del PDF final y registrarlo en un servicio de timestamp o en una transacciÃ³n OP_RETURN).

---

2 MotivaciÃ³n y objetivos

(SecciÃ³n completa en el PDF final. AquÃ se incluye la justificaciÃ³n tÃ©cnica, problem statement y objetivos del proyecto.)

---

3 Fundamentos matemÃ¡ticos y cientÃficos
- CriptografÃa (hashes, firmas, PQC).
- Ãlgebra de grupos (cubo de Rubik como grupo finito).
- TeorÃa de sistemas distribuidos.
- ComputaciÃ³n cuÃ¡ntica: modelos de ataque Grover/Shor y mitigaciones.

(El PDF final incluye fÃ³rmulas y derivaciones matemÃ¡ticas.)

---

4 Arquitectura conceptual â€” Capas de cubos

(Capa 1: 3x3x3 para pÃºblico; Capa 2: multi-cubo / 4x4 para instituciones; Capa 3: alta seguridad)

---

5 EspecificaciÃ³n tÃ©cnica: RubikPoW

(EspecificaciÃ³n del puzzle, S0, M, nonce, verificaciÃ³n H(...), prevenciÃ³n precomputations, etc.)

---

6 Modelo de consenso hÃbrido
(ProposiciÃ³n PoW â€” Finalidad PoS; distribuciÃ³n de recompensa sugerida.)

---

7 CriptografÃa post-cuÃ¡ntica
(RecomendaciÃ³n: Dilithium, Kyber, SPHINCS+; migraciÃ³n hÃbrida.)

---

8 AnÃ¡lisis de seguridad y evaluaciÃ³n cuÃ¡ntica
(Incluye N3 = 4.3252e19, anÃ¡lisis Grover, estrategias de mitigaciÃ³n)

---

9 Simulador: metodologÃa y resultados
(Los resultados se incluyen en /Simulator_Results/ - CSV y grÃ¡ficos)

---

10 TokenÃ³mica y economÃa de incentivos (QBC)
(Resumen de emisiÃ³n, reward schedule y staking)

---

11 ImplementaciÃ³n tÃ©cnica y stack
(Substrate (Rust), liboqs, prototipos Python, wallet WASM)

---

12 Estudio de viabilidad tÃ©cnica y de mercado
(Resumen ejecutivo y recomendaciones)

---

13 Presupuesto detallado (0â€“18 meses)
(Resumen de costes y fases)

---

14 Riesgos y mitigaciones
(HeurÃsticas, PQC, centralizaciÃ³n, regulatorios)

---

15 Roadmap
(Fases: investigaciÃ³n -> prototipo -> testnet -> audits -> mainnet)

---

16 ApÃ©ndices y cÃ³digo
(Se incluyen en /Code_Prototypes/)

Firma
Francisco RaÃºl Rueda AdÃ¡n
Founder & Inventor â€” QbitCoin Project (QBC)

(Nota: este archivo Markdown es la base para el PDF tÃ©cnico. El script intentarÃ¡ convertirlo automÃ¡ticamente.)