ES VERSIÓN EN ESPAÑOL

Título: QUANTAR (QTR): Una Blockchain Layer-1 Nativa en Rust con Seguridad Post-Cuántica (Dilithium-5). **Versión:** 1.0 (Génesis) **Fecha:** Diciembre, 2025

1. Resumen Ejecutivo (Abstract)

La criptografía moderna, base de la economía digital de billones de dólares, se enfrenta a una amenaza existencial inminente: la computación cuántica. El algoritmo de Shor amenaza con romper la Criptografía de Curva Elíptica (ECC) utilizada por Bitcoin y Ethereum, poniendo en riesgo todos los activos digitales actuales. **Quantar Protocol (QTR)** propone una solución definitiva: una blockchain Layer-1 construida desde cero en **Rust**, utilizando criptografía basada en retículos (*Lattice-based Cryptography*) a través del algoritmo **Dilithium-5**, garantizando seguridad de nivel militar contra ataques tanto cuánticos como clásicos, manteniendo un alto rendimiento y escalabilidad.

2. El Problema: El "Día Q" (Q-Day)

Las blockchains actuales (Bitcoin, Ethereum, Solana) dependen matemáticamente de problemas de logaritmo discreto (secp256k1, ed25519).

- **La Vulnerabilidad:** Los ordenadores cuánticos con suficientes qubits podrán resolver estos problemas matemáticos en segundos, derivando Claves Privadas a partir de Claves Públicas.
- **El Impacto:** En el momento en que esto ocurra (el llamado "Día Q"), cualquier billetera estándar podría ser hackeada y vaciada, colapsando la confianza en el sistema financiero descentralizado.
- **La Urgencia:** La transición a una criptografía resistente debe ocurrir *antes* de que los ordenadores cuánticos sean comercialmente viables.

3. La Solución Técnica: Quantar Protocol

Quantar no es un "fork" (copia) de proyectos antiguos. Es una arquitectura nueva centrada en tres pilares:

3.1. Criptografía Post-Cuántica (PQC)

A diferencia de los estándares RSA o ECC, Quantar utiliza **CRYSTALS-Dilithium (Nivel 5)**.

- **Mecanismo:** Basado en la dificultad de encontrar vectores cortos en retículos (Lattices). No existe ningún algoritmo cuántico conocido capaz de resolver este problema de manera eficiente.
- **Nivel de Seguridad:** Dilithium-5 ofrece una seguridad comparable a AES-256 y es recomendado por el NIST (Instituto Nacional de Estándares y Tecnología de EE.UU.) para aplicaciones de alta seguridad.

3.2. Rendimiento con Rust (Seguridad de Memoria)

El núcleo de Quantar (`quantar-core`) está escrito 100% en **Rust**.

- **Sin Garbage Collector:** Elimina las pausas de procesamiento comunes en lenguajes como Go o Java.
- **Seguridad de Memória:** El compilador de Rust previene clases enteras de errores (como *buffer overflows*) que históricamente han causado hacks en otras redes.
- **Benchmarks Reales:** En pruebas de Mainnet, la validación de bloques y la firma ocurren en el orden de **microsegundos (µs)**, permitiendo un alto flujo de transacciones (TPS).

3.3. Arquitectura de Datos y Red

- **Motor de Almacenamiento:** Utiliza **Sled**, una base de datos integrada de alto rendimiento, garantizando una persistencia rápida y confiable de los bloques.
- **Networking:** Red P2P descentralizada basada en `libp2p` con el protocolo GossipSub, asegurando una propagación eficiente de bloques y resistencia a la censura.

4. Tokenomics (Economía del Token)

La política monetaria de Quantar es deflacionaria y está programada matemáticamente en el código fuente, garantizando escasez digital.

- **Ticker:** QTR
- **Recompensa Inicial:** 50 QTR por bloque.
- **Mecanismo de Halving:** La recompensa se reduce a la mitad cada 1.000 bloques (durante la etapa inicial/Génesis para el arranque de la red).
- **Suministro Total (Supply):** Estrictamente limitado por la progresión geométrica de las recompensas. No hay emisión infinita.
- **Utilidad:** QTR se utiliza para las tarifas de transacción (Gas) y para incentivar a los mineros que aseguran la red con poder computacional.

5. Roadmap (Hoja de Ruta)

- **Fase 1: Génesis (Completada)**
  - Desarrollo del Core en Rust.
  - Implementación de Dilithium-5.
  - Lanzamiento de Mainnet v1.0.
  - Minería vía CPU activa.
- **Fase 2: Expansión (Actual)**
  - Lanzamiento de Billetera GUI (Interfaz Gráfica) para usuarios comunes.
  - Optimización del algoritmo de minería.
  - Listado en agregadores de datos.
- **Fase 3: Ecosistema (Futuro)**
  - Implementación de Smart Contracts en Rust (WASM).
  - Listado en Exchanges Centralizados (CEX).
  - Auditoría Externa de Seguridad (Certik/Trail of Bits).

6. Conclusión

Quantar (QTR) representa la próxima evolución necesaria de la tecnología blockchain. Mientras el mercado se centra en la volatilidad a corto plazo, Quantar se centra en la **supervivencia a largo plazo** contra las amenazas cuánticas. Al combinar la robustez

de Rust con la matemática avanzada de Retículos, Quantar se posiciona como el "Refugio Seguro" para el capital digital del siglo XXI.

*"Developed by Chaveiro Batel Engineering | [chaveirobatel@gmail.com] | [*https://github.com/chaveirobatelcuritiba/quantar-core*]"*