US ENGLISH VERSION (Official)

Title: QUANTAR (QTR): A Rust-Native Layer-1 Blockchain with Post-Quantum Security (Dilithium-5). **Version:** 1.0 (Genesis) **Date:** December, 2025

1. Abstract

Modern cryptography, the foundation of the trillion-dollar digital economy, faces an imminent existential threat: quantum computing. Shor's algorithm threatens to break the Elliptic Curve Cryptography (ECC) used by Bitcoin and Ethereum, endangering all current digital assets. **Quantar Protocol (QTR)** proposes a definitive solution: a Layer-1 blockchain built from scratch in **Rust**, utilizing **Lattice-based Cryptography** via the **Dilithium-5** algorithm. This ensures military-grade security against both quantum and classical attacks while maintaining high performance and scalability.

2. The Problem: "Q-Day"

Current blockchains (Bitcoin, Ethereum, Solana) rely mathematically on discrete logarithm problems (secp256k1, ed25519).

- **The Vulnerability:** Quantum computers with sufficient qubits will be able to solve these mathematical problems in seconds, deriving Private Keys from Public Keys.
- **The Impact:** The moment this occurs (the so-called "Q-Day"), any standard blockchain wallet could be hacked and drained, collapsing trust in the decentralized financial system.
- **The Urgency:** The transition to resistant cryptography must happen *before* quantum computers become commercially viable.

3. The Technical Solution: Quantar Protocol

Quantar is not a fork of legacy projects. It is a novel architecture focused on three pillars:

3.1. Post-Quantum Cryptography (PQC)

Unlike the RSA or ECC standards, Quantar utilizes **CRYSTALS-Dilithium (Level 5)**.

- **Mechanism:** Based on the difficulty of finding short vectors in Lattices. No known quantum algorithm can solve this problem efficiently.
- **Security Level:** Dilithium-5 offers security comparable to AES-256 and is recommended by NIST (National Institute of Standards and Technology) for high-security applications.

3.2. Performance via Rust (Memory Safety)

The Quantar core (`quantar-core`) is written 100% in **Rust**.

- **No Garbage Collector:** Eliminates processing pauses common in languages like Go or Java.
- **Memory Safety:** The Rust compiler prevents entire classes of bugs (such as buffer overflows) that have historically caused hacks in other networks.
- **Real Benchmarks:** In Mainnet tests, block validation and signing occur in the order of **microseconds (μs)**, allowing for high transaction throughput (TPS).

3.3. Data & Network Architecture

- **Storage Engine:** Utilizes **Sled**, a high-performance embedded database, ensuring fast and reliable block persistence.
- **Networking:** Decentralized P2P network based on `libp2p` with the GossipSub protocol, ensuring efficient block propagation and censorship resistance.

4. Tokenomics

Quantar's monetary policy is deflationary and mathematically hard-coded into the source code, ensuring digital scarcity.

- **Ticker:** QTR
- **Initial Reward:** 50 QTR per block.
- **Halving Mechanism:** The reward is cut in half every 1,000 blocks (during the initial/Genesis stage for network bootstrapping).
- **Total Supply:** Strictly limited by the geometric progression of rewards. No infinite minting.

- **Utility:** QTR is used for transaction fees (Gas) and to incentivize miners who secure the network with computational power.

5. Roadmap

- **Phase 1: Genesis (Completed)**
  - Core development in Rust.
  - Dilithium-5 implementation.
  - Mainnet v1.0 Launch.
  - CPU Mining active.
- **Phase 2: Expansion (Current)**
  - GUI Wallet Launch for everyday users.
  - Mining algorithm optimization.
  - Listing on data aggregators.
- **Phase 3: Ecosystem (Future)**
  - Smart Contracts implementation in Rust (WASM).
  - Listing on Centralized Exchanges (CEX).
  - External Security Audit (Certik/Trail of Bits).

6. Conclusion

Quantar (QTR) represents the necessary next evolution of blockchain technology. While the market focuses on short-term volatility, Quantar focuses on **long-term survival** against quantum threats. By combining the robustness of Rust with advanced Lattice mathematics, Quantar positions itself as the "Safe Haven" for 21st-century digital capital.

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