📄 PROJETO DE WHITEPAPER: QUANTAR PROTOCOL

Título: QUANTAR (QTR): Uma Blockchain Layer-1 Nativa em Rust com Segurança Pós-Quântica (Dilithium-5). **Versão:** 1.0 (Genesis) **Data:** Dezembro, 2025

1. Resumo Executivo (Abstract)

A criptografia moderna, base da economia digital de trilhões de dólares, enfrenta uma ameaça existencial iminente: a computação quântica. O algoritmo de Shor ameaça quebrar a criptografia de Curvas Elípticas (ECC) utilizada pelo Bitcoin e Ethereum, colocando em risco todos os ativos digitais atuais. O **Quantar Protocol (QTR)** propõe uma solução definitiva: uma blockchain Layer-1 construída do zero em **Rust**, utilizando assinaturas baseadas em reticulados (*Lattice-based Cryptography*) através do algoritmo **Dilithium-5**, garantindo segurança nível militar contra ataques quânticos e clássicos, mantendo alta performance e escalabilidade.

2. O Problema: O "Dia Q" (Q-Day)

As blockchains atuais (Bitcoin, Ethereum, Solana) dependem matematicamente de problemas de logaritmo discreto (secp256k1, ed25519).

- **A Vulnerabilidade:** Computadores quânticos com qubits suficientes poderão resolver esses problemas matemáticos em segundos, derivando Chaves Privadas a partir de Chaves Públicas.
- **O Impacto:** No momento em que isso ocorrer (o chamado "Q-Day"), qualquer carteira de Bitcoin poderá ser invadida e esvaziada, colapsando a confiança no sistema financeiro descentralizado.
- **A Urgência:** A transição para criptografia resistente precisa acontecer *antes* que os computadores quânticos sejam viáveis comercialmente.

3. A Solução Técnica: Quantar Protocol

O Quantar não é um "fork" (cópia) de projetos antigos. É uma arquitetura nova focada em três pilares:

3.1. Criptografia Pós-Quântica (PQC)

Diferente do padrão RSA ou ECC, o Quantar utiliza o **CRYSTALS-Dilithium (Nível 5)**.

- **Mecanismo:** Baseado na dificuldade de encontrar vetores curtos em reticulados (Lattices). Não existe algoritmo quântico conhecido capaz de quebrar esse problema de forma eficiente.
- **Nível de Segurança:** O Dilithium-5 oferece segurança comparável ao AES-256, sendo recomendado pelo NIST (Instituto Nacional de Padrões e Tecnologia dos EUA) para alta segurança.

3.2. Performance com Rust (Memory Safety)

O núcleo do Quantar (`quantar-core`) é escrito 100% em **Rust**.

- **Sem Garbage Collector:** Elimina pausas de processamento comuns em linguagens como Go ou Java.
- **Segurança de Memória:** O compilador do Rust impede classes inteiras de bugs (como *buffer overflows*) que historicamente causaram hacks em outras redes.
- **Benchmarks Reais:** Em testes de Mainnet, a validação de blocos e assinatura ocorre na ordem de **microsegundos (µs)**, permitindo alta vazão de transações (TPS).

3.3. Arquitetura de Dados e Rede

- **Storage Engine:** Utiliza **Sled**, um banco de dados embarcado de alta performance, garantindo persistência rápida e confiável dos blocos.
- **Networking:** Rede P2P descentralizada baseada em `libp2p` com protocolo GossipSub, garantindo propagação eficiente de blocos e resistência à censura.

4. Tokenomics (Economia do Token)

A política monetária do Quantar é deflacionária e programada matematicamente no código-fonte, garantindo escassez digital.

- **Ticker:** QTR
- **Recompensa Inicial:** 50 QTR por bloco.
- **Mecanismo de Halving:** A recompensa é cortada pela metade a cada 1.000 blocos (no estágio inicial/Genesis para bootstrapping da rede).
- **Supply Total (Máximo):** Estritamente limitado pela progressão geométrica das recompensas. Não haverá emissão infinita.
- **Utilidade:** O QTR é utilizado para taxas de transação (Gas) e incentivo aos mineradores que protegem a rede com poder computacional.

5. Roadmap (Roteiro de Desenvolvimento)

- **Fase 1: Genesis (Concluído)**
  - Desenvolvimento do Core em Rust.
  - Implementação do Dilithium-5.
  - Lançamento da Mainnet v1.0.
  - Mineração via CPU ativa.
- **Fase 2: Expansão (Atual)**
  - Lançamento de Carteira GUI (Interface Gráfica) para usuários comuns.
  - Otimização do algoritmo de mineração.
  - Listagem em agregadores de dados.
- **Fase 3: Ecossistema (Futuro)**
  - Implementação de Smart Contracts (Contratos Inteligentes) em Rust (WASM).
  - Listagem em Corretoras Centralizadas (CEX).
  - Auditoria Externa de Segurança (Certik/Trail of Bits).

6. Conclusão

O Quantar (QTR) representa a próxima evolução necessária da tecnologia blockchain. Enquanto o mercado foca na volatilidade de curto prazo, o Quantar foca na **sobrevivência de longo prazo** contra ameaças quânticas. Ao combinar a robustez do Rust com a matemática avançada dos Reticulados, o Quantar se posiciona como o "Porto Seguro" para o capital digital do século 21.

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