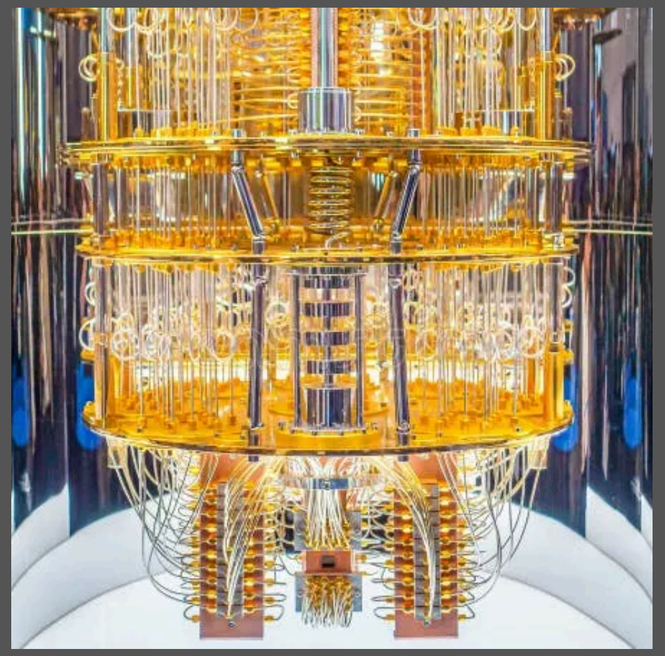
Transição para Criptografia Pós-Quântica em Redes Blockchain de Alta Performance

UMA ANÁLISE DA ARQUITETURA SOLANA

O problema

- **Computadores quânticos podem quebrar ECDSA/EdDSA.**
- **Algoritmo de Shor**
- **Estratégia "Harvest Now, Decrypt Later"**



A Solução : Criptografia Pós-Quântica

- NIST iniciou padronização de Algoritmos em 2016.
- Revisar algoritmos PQC padronizados
  - FIPS 203 (ML-KEM - CRYSTALS-Kyber)
  - FIPS 204 (ML-DSA - CRYSTALS-Dilithium)
  - FIPS 205 (SLH-DSA - SPHINCS+)
- Baseados em problemas matemáticos resistentes a ataques quânticos:
  - Reticulados
  - Funções Hash

Objetivos

Analisar arquitetura criptográfica atual da Solana

Revisar algoritmos PQC padronizados (ML-KEM, ML-DSA, Falcon, SPHINCS+)

Avaliar impacto em throughput, tamanho de transações e custos

Propor estratégias de migração

Primitivas Criptográficas em Blockchain

Três pilares fundamentais:

Funções hash criptográficas

Criptografia de chave pública

Esquemas de assinatura digital

Arquitetura da Solana

- **Proof of History**
- **Tower BFT**
- **Turbine**
- **Gulf Stream**
- **Sealevel**
- **Pipeline**
- **Cloudbreak**
- **Archivers**

Ameaça Quântica

Algoritmo de Shor

- Resolve fatoração e logaritmo discreto em tempo polinomial: $O(n^3)$
- Quebra curvas de 256 bits com ~2.330 qubits lógicos
- Impacto: ECDSA/EdDSA tornam-se inseguros

Algoritmo de Grover

- Aceleração quadrática em busca: $O(2^n) \rightarrow O(2^{(n/2)})$
- Impacto em hash: SHA-256 reduzido de 256 para 128 bits efetivos
- Solução: dobrar tamanhos de saída (ex: SHA-512)

Níveis de Segurança NIST

Níveis	Equivalente Simétrico	Bits de Segurança
1	AES-128 (Busca de Chave)	143
2	SHA-256 (Colisão)	207
3	AES-192 (Busca de Chave)	207
4	SHA-384 (Colisão)	272
5	AES-256 (Busca de Chave)	272

Comparações de Esquemas de Assinatura Digital

Esquema	Chave Pública	Assinatura	Total	Fator
Ed25519	32	64	96	1.0×
Falcon-512	897	666	1563	16.3×
ML-DSA	1312	2420	3732	38.9×
SPHINCS+	32	7856	7888	82.2×

Tamanhos em bytes. Fator calculado como (pk +sig)relativo ao Ed25519.

Pontos Positivos e Negativos

Falcon-512:

- ✓ Alta frequência de assinaturas
- ✓ Restrições severas de largura de banda
- ✓ Necessidade de manter throughput elevado
- ✗ Complexidade de implementação aceitável (Fast Fourier Sampling)

ML-DSA

- ✓ Implementação mais simples
- ✓ Tempos de assinatura consistentes
- ✓ Prioridade em latência previsível
- ✗ Overhead 3.6× maior que Falcon

SPHINCS+

- ✓ Base conservadora (Hash)
- ✓ Elimina riscos de descobertas matemáticas em reticulados
- ✓ Ideal para aplicações de longo prazo
- ✗ Overhead inviável para alta frequência (11.8× maior que Falcon)

Conclusão

Falcon-512:

- Menor overhead viável - 16.3× total vs 38.9× (ML-DSA) e 82.2× (SPHINCS+)
- Permite ~20-25k TPS vs ~6k TPS (ML-DSA)
- Nível 1 NIST = suficiente (equivalente AES-128)
- Complexidade de implementação (FFS) é compensada pelos ganhos de performance