

# Transição para Criptografia Pós-Quântica em Redes Blockchain de Alta Performance: Uma Análise da Arquitetura Solana

Arthur T. Oliveira<sup>1</sup>, Ana Cristina dos Santos<sup>1</sup>

<sup>1</sup>Instituto de Tecnologia e Liderança  
Av. Professor Almeida Prado, 520, Butantã – 05508-901 – São Paulo – SP – Brasil

arthur.oliveira@sou.inteli.edu.br, anacris.santos@prof.inteli.edu.br

**Abstract.** *The emergence of quantum computing poses an existential threat to current blockchain cryptographic primitives, particularly elliptic curve-based digital signatures. This work investigates the technical and economic implications of transitioning high-performance blockchain networks to post-quantum cryptography (PQC). We focus on the Solana network as a case study, analyzing how NIST-standardized algorithms (ML-KEM, ML-DSA, Falcon, and SPHINCS+) can be integrated into its unique architecture. Our analysis examines the mathematical foundations of lattice-based and hash-based cryptography, evaluates performance trade-offs in transaction size and throughput, and proposes implementation pathways that preserve network scalability while ensuring quantum resistance.*

**Resumo.** *O surgimento da computação quântica representa uma ameaça existencial às primitivas criptográficas atuais de blockchain, particularmente às assinaturas digitais baseadas em curvas elípticas. Este trabalho investiga as implicações técnicas e econômicas da transição de redes blockchain de alta performance para criptografia pós-quântica (PQC). Focamos na rede Solana como estudo de caso, analisando como os algoritmos padronizados pelo NIST (ML-KEM, ML-DSA, Falcon e SPHINCS+) podem ser integrados em sua arquitetura única. Nossa análise examina os fundamentos matemáticos da criptografia baseada em reticulados e hashes, avalia trade-offs de desempenho em tamanho de transação e throughput, e propõe caminhos de implementação que preservam a escalabilidade da rede enquanto garantem resistência quântica.*

## 1. Introdução

A tecnologia blockchain evoluiu de uma proposta experimental em 2008 para um componente fundamental da infraestrutura digital global. Desde a publicação do whitepaper do Bitcoin por Satoshi Nakamoto [1], as redes descentralizadas expandiram-se para suportar casos de uso que vão além de transferências financeiras, incluindo contratos inteligentes, finanças descentralizadas (DeFi) e tokenização de ativos. Segundo dados de 2025, o mercado de criptoativos atingiu uma capitalização de aproximadamente USD 3,8 trilhões, com a rede Solana posicionando-se como a sexta maior com USD 116 bilhões [2].

A segurança dessas redes fundamenta-se em primitivas criptográficas de chave pública, particularmente no Elliptic Curve Digital Signature Algorithm (ECDSA) e suas

variantes como o EdDSA. Conforme Narayanan et al. (2016) [3], "a criptografia fornece um mecanismo para codificar de forma segura as regras de um sistema de criptomoeda no próprio sistema". No entanto, o advento de computadores quânticos criptograficamente relevantes (CRQCs) ameaça comprometer essa base de segurança.

O algoritmo de Shor [4], desenvolvido em 1994, demonstrou que computadores quânticos suficientemente poderosos podem resolver o problema do logaritmo discreto em curvas elípticas em tempo polinomial, quebrando efetivamente a segurança do ECDSA. Para contextos de blockchain, onde a imutabilidade do ledger é fundamental, essa vulnerabilidade é particularmente crítica. Atores maliciosos podem empregar estratégias de "Harvest Now, Decrypt Later", capturando dados criptografados hoje para decifrá-los no futuro quando CRQCs estiverem disponíveis [5].

Em resposta a essa ameaça, o National Institute of Standards and Technology (NIST) iniciou em 2016 um processo de padronização para algoritmos de Criptografia Pós-Quântica (PQC). Em agosto de 2024, o NIST publicou os primeiros padrões finalizados: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) e FIPS 205 (SLH-DSA) [6]. Esses algoritmos baseiam-se em problemas matemáticos considerados intratáveis mesmo para computadores quânticos, como o Learning With Errors (LWE) em reticulados estruturados e funções hash criptográficas.

Este trabalho investiga a viabilidade técnica e as implicações econômicas da transição de redes blockchain de alta performance, especificamente a Solana, para primitivas criptográficas pós-quânticas. A Solana foi escolhida como caso de estudo por sua arquitetura única baseada em Proof of History (PoH), capacidade de processamento superior a 65.000 transações por segundo (TPS) e uso intensivo de Ed25519 para assinaturas digitais [7].

## 1.1. Objetivos

Os objetivos específicos deste trabalho são:

- Analisar a arquitetura criptográfica atual da rede Solana, identificando componentes vulneráveis a ataques quânticos;
- Revisar os fundamentos matemáticos dos algoritmos PQC padronizados pelo NIST, com foco em ML-KEM, ML-DSA, Falcon e SPHINCS+;
- Avaliar o impacto da substituição de Ed25519 por algoritmos PQC no throughput, tamanho de transações e custos operacionais da rede;
- Propor estratégias de migração que preservem a compatibilidade retroativa e minimizem riscos durante a transição.

## 2. Fundamentação Teórica

Esta seção estabelece os conceitos fundamentais necessários para compreender a transição para criptografia pós-quântica em blockchain. Iniciamos com os princípios de segurança criptográfica em redes descentralizadas, seguimos para a arquitetura específica da Solana e finalizamos com uma introdução aos desafios impostos pela computação quântica.

### 2.1. Primitivas Criptográficas em Blockchain

A tecnologia blockchain depende de três primitivas criptográficas fundamentais: funções hash, criptografia de chave pública e esquemas de assinatura digital. Segundo Narayanan

et al. (2016) [3], essas primitivas trabalham em conjunto para garantir três propriedades essenciais: imutabilidade do ledger, autenticação de transações e consenso distribuído.

### 2.1.1. Funções Hash Criptográficas

Uma função hash criptográfica  $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$  mapeia uma entrada de tamanho arbitrário para uma saída de tamanho fixo  $n$ . Para ser considerada criptograficamente segura,  $H$  deve satisfazer três propriedades [8]:

1. **Resistência à pré-imagem:** Dado  $y$ , é computacionalmente inviável encontrar  $x$  tal que  $H(x) = y$ .
2. **Resistência à segunda pré-imagem:** Dado  $x_1$ , é inviável encontrar  $x_2 \neq x_1$  com  $H(x_1) = H(x_2)$ .
3. **Resistência à colisão:** É inviável encontrar qualquer par  $(x_1, x_2)$  com  $x_1 \neq x_2$  e  $H(x_1) = H(x_2)$ .

No Bitcoin e Solana, funções hash como SHA-256 são utilizadas para construir Merkle Trees, estruturas de dados que permitem verificação eficiente de inclusão de transações em blocos [9].

### 2.1.2. Criptografia de Chave Pública

Sistemas de chave pública utilizam pares de chaves matematicamente relacionadas: uma chave privada  $sk$  mantida em sigilo e uma chave pública  $pk$  distribuída livremente. A segurança baseia-se na dificuldade computacional de derivar  $sk$  a partir de  $pk$ . No contexto de blockchain, a maioria dos sistemas utiliza criptografia de curva elíptica (ECC), especificamente as curvas secp256k1 (Bitcoin) e Curve25519 (Solana) [10].

A segurança do ECC fundamenta-se no Problema do Logaritmo Discreto em Curvas Elípticas (ECDLP): dado um ponto  $P$  na curva e  $Q = kP$ , encontrar o escalar  $k$  é computacionalmente inviável para computadores clássicos quando o tamanho do campo é suficientemente grande [11, 12].

### 2.1.3. Esquemas de Assinatura Digital

Um esquema de assinatura digital consiste em três algoritmos [13]:

- $\text{KeyGen}(1^\lambda) \rightarrow (sk, pk)$ : Gera um par de chaves com parâmetro de segurança  $\lambda$ .
- $\text{Sign}(sk, m) \rightarrow \sigma$ : Produz uma assinatura  $\sigma$  para a mensagem  $m$  usando  $sk$ .
- $\text{Verify}(pk, m, \sigma) \rightarrow \{0, 1\}$ : Verifica se  $\sigma$  é uma assinatura válida de  $m$  sob  $pk$ .

A Solana utiliza o esquema Ed25519, uma variante do EdDSA baseada na Curve25519. Bernstein et al. (2012) [14] demonstraram que Ed25519 oferece segurança de aproximadamente 128 bits contra ataques clássicos, com velocidades de verificação excepcionais devido ao uso de aritmética de Edwards.

## 2.2. Arquitetura da Rede Solana

A Solana representa uma evolução significativa no design de blockchain, projetada para superar o trilema da escalabilidade identificado por Buterin [15]: a dificuldade de alcançar simultaneamente descentralização, segurança e escalabilidade. Yakovenko (2018) [7] introduziu o conceito de Proof of History (PoH) como solução para esse problema.

### 2.2.1. Proof of History

O PoH funciona como um relógio criptográfico verificável que estabelece uma ordem temporal dos eventos antes do consenso. Formalmente, o PoH é implementado como uma Verifiable Delay Function (VDF) sequencial [16]:

$$\text{PoH}(x, i) = H^i(x) = \underbrace{H(H(\dots H(x)\dots))}_{i \text{ vezes}} \quad (1)$$

onde  $H$  é uma função hash criptográfica (SHA-256 no caso da Solana) e  $i$  representa o número de iterações. A propriedade fundamental é que cada hash só pode ser computado após o anterior, criando uma prova verificável de passagem de tempo.

O PoH permite que a rede alcance throughput teórico de até 710.000 TPS, embora o valor prático esteja limitado a aproximadamente 65.000 TPS devido a restrições de hardware e propagação de rede [17].

### 2.2.2. Tower BFT

O mecanismo de consenso da Solana, Tower BFT, é uma variante otimizada do Practical Byzantine Fault Tolerance (PBFT) [18] que aproveita o PoH como fonte de tempo. Os validadores votam em forks específicos com um esquema de lockout exponencial: após votar em um fork, um validador está bloqueado por  $2^k$  slots, onde  $k$  é o número de votos consecutivos naquele fork [19].

### 2.2.3. Primitivas Criptográficas na Solana

A Solana emprega Ed25519 extensivamente para:

- Assinatura de transações pelos usuários
- Autenticação de validadores
- Derivação determinística de endereços (Program Derived Addresses)

Cada transação Solana contém uma ou mais assinaturas Ed25519 de 64 bytes, que são verificadas em paralelo por validadores usando otimizações de GPU [20]. A eficiência dessa verificação é crítica para o alto throughput da rede.

## 2.3. A Ameaça Quântica

A computação quântica fundamenta-se nos princípios de superposição e entrelaçamento quântico para realizar computações que seriam inviáveis classicamente. Segundo Nielsen e Chuang (2010) [21], um computador quântico com  $n$  qubits pode representar  $2^n$  estados simultaneamente, oferecendo paralelismo massivo para certos tipos de problemas.

### 2.3.1. Algoritmo de Shor

O algoritmo de Shor [4] é um algoritmo quântico que resolve os problemas de fatoração de inteiros e logaritmo discreto em tempo polinomial. Para um número de  $n$  bits, o algoritmo de Shor tem complexidade  $O(n^3)$ , comparado à complexidade sub-exponencial dos melhores algoritmos clássicos conhecidos.

Para curvas elípticas, o algoritmo de Shor adaptado pode quebrar uma curva de 256 bits usando aproximadamente 2.330 qubits lógicos com uma taxa de erro de  $10^{-3}$  [22]. Projeções conservadoras sugerem que CRQCs com essas capacidades podem estar disponíveis entre 2030 e 2035 [5].

### 2.3.2. Algoritmo de Grover

O algoritmo de Grover [23] oferece uma aceleração quadrática para problemas de busca não estruturada. Para funções hash com saída de  $n$  bits, o algoritmo de Grover reduz a complexidade de busca de pré-imagem de  $O(2^n)$  para  $O(2^{n/2})$ .

Essa aceleração implica que funções hash que oferecem 256 bits de segurança clássica fornecem efetivamente 128 bits de segurança quântica. Consequentemente, para manter níveis de segurança equivalentes na era pós-quântica, é necessário dobrar os tamanhos de saída das funções hash [24].

## 2.4. Princípios de Criptografia Pós-Quântica

A criptografia pós-quântica busca desenvolver algoritmos que executam em computadores clássicos mas permanecem seguros contra adversários quânticos. O NIST identificou cinco famílias principais de problemas matemáticos considerados resistentes a ataques quânticos [25]:

1. **Reticulados (Lattices)**: Problemas baseados na dificuldade de encontrar vetores curtos em reticulados de alta dimensão.
2. **Multivariados**: Resolução de sistemas de equações polinomiais multivariadas.
3. **Hash**: Esquemas baseados exclusivamente em propriedades de funções hash.
4. **Isogenias**: Problemas relacionados a caminhos em grafos de isogenias de curvas elípticas supersingulares.

Os algoritmos padronizados pelo NIST concentram-se principalmente nas duas primeiras categorias. A Tabela 1 apresenta os níveis de segurança definidos pelo NIST para comparação de algoritmos PQC.

A distinção entre níveis baseados em busca de chave (ímpares) e colisão (pares) reflete os diferentes modelos de ameaça para KEMs e esquemas de assinatura, respectivamente. Esta seção estabeleceu os fundamentos necessários para compreender tanto a arquitetura atual de blockchain quanto os desafios da transição pós-quântica.

## 3. Revisão da Literatura de Algoritmos PQC

Esta seção apresenta uma análise técnica dos algoritmos de criptografia pós-quântica padronizados pelo NIST. Focamos nos esquemas mais relevantes para aplicações em blockchain: ML-KEM para encapsulamento de chaves, e ML-DSA, Falcon e SPHINCS+ para assinaturas digitais.

**Table 1. Níveis de Segurança NIST para Algoritmos PQC**

Nível	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

**Fonte:** NIST (2016) [25]

### 3.1. ML-KEM (FIPS 203)

O Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), derivado do CRYSTALS-Kyber, foi padronizado como FIPS 203 em agosto de 2024 [26]. Bos et al. (2018) [27] descrevem o Kyber como uma evolução do Learning With Errors (LWE) que balanceia segurança e eficiência através de reticulados estruturados.

#### 3.1.1. Fundamentos Matemáticos

A segurança do ML-KEM baseia-se no problema Module-LWE (MLWE), uma generalização do Ring-LWE. Formalmente, o problema MLWE é definido sobre o anel de polinômios quociente  $R_q = \mathbb{Z}_q[x]/(x^n + 1)$ , onde  $n = 256$  e  $q = 3329$  são parâmetros fixos do ML-KEM [28].

Dado um módulo de dimensão  $k$  sobre  $R_q$ , o problema MLWE consiste em distinguir pares  $(\mathbf{A}, \mathbf{b})$  onde  $\mathbf{A} \in R_q^{k \times k}$  é uniforme e:

$$\mathbf{b} = \mathbf{A} \cdot \mathbf{s} + \mathbf{e} \pmod{q} \quad (2)$$

de pares completamente aleatórios, onde  $\mathbf{s}, \mathbf{e} \in R_q^k$  são vetores com coeficientes pequenos amostrados de uma distribuição gaussiana discreta [29].

#### 3.1.2. Conjuntos de Parâmetros

O FIPS 203 especifica três conjuntos de parâmetros, apresentados na Tabela 2, que correspondem a diferentes níveis de segurança NIST.

**Table 2. Parâmetros e Tamanhos para ML-KEM**

Variante	$k$	Nível NIST	pk (bytes)	ct (bytes)
ML-KEM-512	2	1	800	768
ML-KEM-768	3	3	1184	1088
ML-KEM-1024	4	5	1568	1568

**Fonte:** NIST FIPS 203 (2024) [26]

A escolha do parâmetro  $k$  determina a dimensão do problema MLWE subjacente. Langlois e Stehlé (2015) [28] provaram que a segurança do MLWE no caso médio pode ser reduzida à dureza no pior caso do problema do vetor mais curto (SVP) em reticulados ideais com fator de aproximação  $\tilde{O}(\sqrt{nk})$ .

### 3.1.3. Transformação Fujisaki-Okamoto

Para alcançar segurança IND-CCA2, o ML-KEM aplica uma variante da transformação Fujisaki-Okamoto (FO) [30] ao esquema PKE subjacente. A transformação FO converte um esquema IND-CPA em um KEM IND-CCA2 através de três mecanismos [31]:

1. Encapsulamento aleatório: em vez de criptografar uma mensagem externa, gera-se uma mensagem aleatória  $m$  internamente.
2. Derivação de chave: o segredo compartilhado  $K$  é derivado via hash de  $m$  e parâmetros públicos.
3. Re-criptação: durante decapsulamento, o receptor re-cripta  $m$  e compara com o texto cifrado recebido para detectar modificações.

## 3.2. ML-DSA (FIPS 204)

O Module-Lattice-Based Digital Signature Algorithm (ML-DSA), derivado do CRYSTALS-Dilithium, foi padronizado como FIPS 204 [32]. Ducas et al. (2018) [33] propuseram o Dilithium como uma instanciação eficiente do framework Fiat-Shamir com abortos.

### 3.2.1. Framework Fiat-Shamir

O Dilithium baseia-se no paradigma Fiat-Shamir [34], transformando um protocolo de identificação em um esquema de assinatura através de um hash criptográfico como oráculo aleatório. O protocolo subjacente é uma variante do esquema de Lyubashevsky [35] para assinaturas baseadas em reticulados.

A segurança fundamenta-se no problema Short Integer Solution (SIS) sobre módulos. Dado  $\mathbf{A} \in R_q^{k \times l}$  uniforme, o problema SIS consiste em encontrar um vetor curto  $\mathbf{z} \in R_q^l$  tal que:

$$\mathbf{A} \cdot \mathbf{z} = \mathbf{0} \pmod{q} \quad (3)$$

com  $\|\mathbf{z}\| \leq \beta$  para algum limite  $\beta$  [36].

### 3.2.2. Conjuntos de Parâmetros

A Tabela 3 apresenta os três conjuntos de parâmetros do ML-DSA, com tamanhos significativamente maiores que Ed25519 (64 bytes de assinatura).

**Table 3. Parâmetros e Tamanhos para ML-DSA**

Variante	$(k, l)$	Nível	pk (bytes)	sig (bytes)
ML-DSA-44	(4,4)	2	1312	2420
ML-DSA-65	(6,5)	3	1952	3293
ML-DSA-87	(8,7)	5	2592	4595

**Fonte:** NIST FIPS 204 (2024) [32]

### 3.3. Falcon (NIST Round 3)

Falcon (Fast Fourier Lattice-based Compact Signatures over NTRU) foi selecionado pelo NIST por oferecer assinaturas significativamente menores que o Dilithium. Fouque et al. (2020) [37] descrevem Falcon como uma implementação do framework GPV [38] sobre reticulados NTRU.

#### 3.3.1. Reticulados NTRU

Os reticulados NTRU foram introduzidos por Hoffstein, Pipher e Silverman (1998) [39] como uma classe especial de reticulados sobre anéis. No contexto do Falcon, trabalha-se com o anel quociente  $\mathbb{Z}[x]/(\phi)$ , onde  $\phi = x^n + 1$  com  $n = 2^\kappa$  sendo uma potência de dois.

A equação fundamental NTRU é dada por:

$$f \cdot G - g \cdot F = q \pmod{\phi} \quad (4)$$

onde  $f, g, F, G \in \mathbb{Z}[x]/(\phi)$  são polinômios com coeficientes inteiros curtos, e  $q$  é um primo (no Falcon,  $q = 12289$ ) [37].

#### 3.3.2. Fast Fourier Sampling

A inovação central do Falcon é o algoritmo Fast Fourier Sampling (FFS), proposto por Ducas e Prest (2016) [40]. O FFS reduz a complexidade da amostragem gaussiana de  $O(n^2)$  para  $O(n \log n)$  explorando a estrutura recursiva dos reticulados NTRU através da Transformada Rápida de Fourier.

A Tabela 4 mostra que Falcon oferece as menores assinaturas entre todos os candidatos finais do NIST.

**Table 4. Parâmetros e Tamanhos para Falcon**

Variante	$n$	Nível	pk (bytes)	sig (bytes)
Falcon-512	512	1	897	666
Falcon-1024	1024	5	1793	1280

**Fonte:** Falcon Specification v1.2 (2020) [37]

### 3.4. SPHINCS+ (FIPS 205)

O Stateless Hash-Based Digital Signature Algorithm (SLH-DSA), derivado do SPHINCS+, foi padronizado como FIPS 205 [41]. Bernstein et al. (2019) [42] apresentam o SPHINCS+ como uma evolução dos esquemas baseados em hash de Lamport [43] e Merkle [44].

#### 3.4.1. Arquitetura Hierárquica

O SPHINCS+ utiliza uma hipertree de altura  $h$  dividida em  $d$  camadas, cada uma com Árvores de Merkle de altura  $h/d$ . A inovação fundamental é o uso de Few-Time Signatures (FTS) através do esquema FORS (Forest of Random Subsets) em vez de esquemas one-time [45].

A segurança do SPHINCS+ baseia-se exclusivamente nas propriedades de resistência à colisão e segunda pré-imagem de funções hash. Isso confere ao esquema uma base de segurança mais conservadora que algoritmos baseados em reticulados, ao custo de assinaturas substancialmente maiores [46].

#### 3.4.2. Trade-offs de Performance

A Tabela 5 ilustra o trade-off característico do SPHINCS+: assinaturas grandes mas chaves públicas compactas e verificação rápida.

**Table 5. Parâmetros para SPHINCS+ (Variante “s” – Small Signature)**

Variante	Nível	pk (bytes)	sig (bytes)
SPHINCS+-128s	1	32	7856
SPHINCS+-192s	3	48	16224
SPHINCS+-256s	5	64	29792

**Fonte:** NIST FIPS 205 (2024) [41]

### 3.5. Análise Comparativa para Blockchain

A Tabela 6 apresenta uma comparação consolidada dos algoritmos PQC com Ed25519, evidenciando os trade-offs fundamentais para aplicações em blockchain.

**Table 6. Comparaçāo de Esquemas de Assinatura Digital**

Esquema	pk	sig	Total	Fator
Ed25519	32	64	96	1.0×
Falcon-512	897	666	1563	16.3×
ML-DSA-44	1312	2420	3732	38.9×
SPHINCS+-128s	32	7856	7888	82.2×

**Fonte:** Tamanhos em bytes. Fator calculado como  $(\text{pk} + \text{sig})$  relativo ao Ed25519.

Observa-se que Falcon oferece o melhor compromisso entre segurança pós-quântica e overhead de tamanho. Com assinaturas  $10.4\times$  maiores que Ed25519 (666 vs 64 bytes), Falcon é significativamente mais compacto que ML-DSA ( $37.8\times$ ) e SPHINCS+ ( $122.8\times$ ). Para blockchains de alta performance como Solana, onde cada byte impacta diretamente o throughput e custos de armazenamento, essa diferença é crítica [47].

A escolha entre algoritmos depende das prioridades da aplicação. Bindel et al. (2019) [47] argumentam que para sistemas com alta frequência de assinaturas e restrições de largura de banda, Falcon é preferível apesar de sua complexidade de implementação. Por outro lado, ML-DSA oferece implementações mais simples e menor variabilidade nos tempos de assinatura, sendo adequado para contextos onde a previsibilidade de latência é prioritária.

SPHINCS+ ocupa um nicho específico: aplicações que requerem a base de segurança mais conservadora possível e podem tolerar grandes assinaturas. Hülsing et al. (2013) [46] destacam que a segurança baseada apenas em propriedades de hash elimina riscos associados a eventuais descobertas matemáticas que possam comprometer problemas de reticulados.

Esta revisão estabelece que, para o contexto específico de blockchain de alta performance, Falcon emerge como o candidato mais promissor para substituir Ed25519 na Solana. As próximas seções analisarão em profundidade as implicações arquiteturais e os fundamentos matemáticos dessa transição.

## References

- [1] Nakamoto, S. (2008). “Bitcoin: A Peer-to-Peer Electronic Cash System”. <https://bitcoin.org/bitcoin.pdf>
- [2] CoinMarketCap. (2025). “Cryptocurrency Prices”. Acesso em: 08 out. 2025. <https://coinmarketcap.com/>
- [3] Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies*. Princeton University Press.
- [4] Shor, P. W. (1994). “Algorithms for quantum computation: discrete logarithms and factoring”. In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*, p. 124-134.
- [5] Mosca, M. (2018). “Cybersecurity in an Era with Quantum Computers: Will We Be Ready?” *IEEE Security & Privacy*, 16(5), 38-41.
- [6] National Institute of Standards and Technology. (2024). “Post-Quantum Cryptography: FIPS Approved”. Acesso em: 08 out. 2025. <https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved>
- [7] Yakovenko, A. (2018). “Solana: A new architecture for a high performance blockchain v0.8.13”. <https://solana.com/solana-whitepaper.pdf>
- [8] Katz, J., Lindell, Y. (2020). *Introduction to Modern Cryptography*. 3rd ed. CRC Press.
- [9] Merkle, R. C. (1980). “Protocols for Public Key Cryptosystems”. In: *IEEE Symposium on Security and Privacy*, p. 122-134.

- [10] Bernstein, D. J. (2006). “Curve25519: new Diffie-Hellman speed records”. In: *Public Key Cryptography - PKC 2006*, Springer LNCS 3958, p. 207-228.
- [11] Koblitz, N. (1987). “Elliptic curve cryptosystems”. *Mathematics of Computation*, 48(177), 203-209.
- [12] Miller, V. S. (1985). “Use of elliptic curves in cryptography”. In: *CRYPTO 1985*, Springer LNCS 218, p. 417-426.
- [13] Goldwasser, S., Micali, S., Rivest, R. L. (1988). “A digital signature scheme secure against adaptive chosen-message attacks”. *SIAM Journal on Computing*, 17(2), 281-308.
- [14] Bernstein, D. J., Duif, N., Lange, T., Schwabe, P., Yang, B.-Y. (2012). “High-speed high-security signatures”. *Journal of Cryptographic Engineering*, 2(2), 77-89.
- [15] Buterin, V. (2017). “On Sharding Blockchains”. Acesso em: 08 out. 2025. <https://github.com/ethereum/wiki/wiki/Sharding-FAQ>
- [16] Boneh, D., Bonneau, J., Bünz, B., Fisch, B. (2018). “Verifiable Delay Functions”. In: *CRYPTO 2018*, Springer LNCS 10991, p. 757-788.
- [17] Solana Labs. (2024). “Solana Network Performance Metrics”. Acesso em: 08 out. 2025. <https://explorer.solana.com/>
- [18] Castro, M., Liskov, B. (1999). “Practical Byzantine fault tolerance”. In: *OSDI 1999*, p. 173-186.
- [19] Solana Labs. (2021). “Tower BFT - Solana’s High-Performance Implementation of PBFT”. <https://solana.com/news/tower-bft>
- [20] Solana Labs. (2021). “Pipelining in Solana - The Transaction Processing Unit”. <https://solana.com/news/pipelining-in-solana>
- [21] Nielsen, M. A., Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press.
- [22] Roetteler, M., Naehrig, M., Svore, K. M., Lauter, K. (2017). “Quantum resource estimates for computing elliptic curve discrete logarithms”. In: *ASIACRYPT 2017*, Springer LNCS 10625, p. 241-270.
- [23] Grover, L. K. (1996). “A fast quantum mechanical algorithm for database search”. In: *STOC 1996*, p. 212-219.
- [24] Bernstein, D. J., Buchmann, J., Dahmen, E. (Eds.). (2009). *Post-Quantum Cryptography*. Springer.
- [25] National Institute of Standards and Technology. (2016). “Report on Post-Quantum Cryptography”. NISTIR 8105.
- [26] National Institute of Standards and Technology. (2024). “FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard”.
- [27] Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G., Stehlé, D. (2018). “CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM”. In: *IEEE EuroS&P 2018*, p. 353-367.

- [28] Langlois, A., Stehlé, D. (2015). “Worst-case to average-case reductions for module lattices”. *Designs, Codes and Cryptography*, 75(3), 565-599.
- [29] Lyubashevsky, V., Peikert, C., Regev, O. (2010). “On ideal lattices and learning with errors over rings”. In: *EUROCRYPT 2010*, Springer LNCS 6110, p. 1-23.
- [30] Fujisaki, E., Okamoto, T. (1999). “Secure integration of asymmetric and symmetric encryption schemes”. In: *CRYPTO 1999*, Springer LNCS 1666, p. 537-554.
- [31] Hofheinz, D., Hövelmanns, K., Kiltz, E. (2017). “A modular analysis of the Fujisaki-Okamoto transformation”. In: *TCC 2017*, Springer LNCS 10677, p. 341-371.
- [32] National Institute of Standards and Technology. (2024). “FIPS 204: Module-Lattice-Based Digital Signature Standard”.
- [33] Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D. (2018). “CRYSTALS-Dilithium: A lattice-based digital signature scheme”. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2018(1), 238-268.
- [34] Fiat, A., Shamir, A. (1986). “How to prove yourself: Practical solutions to identification and signature problems”. In: *CRYPTO 1986*, Springer LNCS 263, p. 186-194.
- [35] Lyubashevsky, V. (2012). “Lattice signatures without trapdoors”. In: *EUROCRYPT 2012*, Springer LNCS 7237, p. 738-755.
- [36] Micciancio, D., Regev, O. (2009). “Lattice-based cryptography”. In: Bernstein, D. J., Buchmann, J., Dahmen, E. (Eds.), *Post-Quantum Cryptography*, Springer, p. 147-191.
- [37] Fouque, P.-A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., Zhang, Z. (2020). “Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU - Specification v1.2”.
- [38] Gentry, C., Peikert, C., Vaikuntanathan, V. (2008). “Trapdoors for hard lattices and new cryptographic constructions”. In: *STOC 2008*, p. 197-206.
- [39] Hoffstein, J., Pipher, J., Silverman, J. H. (1998). “NTRU: A ring-based public key cryptosystem”. In: *ANTS-III*, Springer LNCS 1423, p. 267-288.
- [40] Ducas, L., Prest, T. (2016). “Fast Fourier orthogonalization”. In: *ISSAC 2016*, p. 191-198.
- [41] National Institute of Standards and Technology. (2024). “FIPS 205: Stateless Hash-Based Digital Signature Standard”.
- [42] Bernstein, D. J., Hülsing, A., Kölbl, S., Niederhagen, R., Rijneveld, J., Schwabe, P. (2019). “The SPHINCS+ signature framework”. In: *CCS 2019*, p. 2129-2146.
- [43] Lamport, L. (1979). “Constructing digital signatures from a one-way function”. Technical Report CSL-98, SRI International.
- [44] Merkle, R. C. (1989). “A certified digital signature”. In: *CRYPTO 1989*, Springer LNCS 435, p. 218-238.
- [45] Aumasson, J.-P., Bernstein, D. J., Beullens, W., Dobraunig, C., Eichlseder, M., Fluhrer, S., Gazdag, S.-L., Hülsing, A., Kampanakis, P., Kölbl, S., Lange, T., Lauridsen, M. M., Mendel, F., Niederhagen, R., Rechberger, C., Rijneveld, J., Schwabe, P., Westerbaan, B. (2022). “SPHINCS+: Submission to NIST Post-Quantum Project, v.3.1”.

- [46] Hülsing, A. (2013). “W-OTS+ - shorter signatures for hash-based signature schemes”. In: *AFRICACRYPT 2013*, Springer LNCS 7918, p. 173-188.
- [47] Bindel, N., Herath, U., McKague, M., Stebila, D. (2019). “Transitioning to a quantum-resistant public key infrastructure”. In: *PQCrypto 2017*, Springer LNCS 10346, p. 384-405.