Segurança em Criptomoedas Frente à Computação Quântica: Uma Revisão Analítica de Abordagens e Propostas

Valmir Bagio de Oliveira Junior[1], Lucy Mari Tabuti[2], Maximiliano de Carvalho Jacomo[3]

[1]Faculdade XP Educação (XPE) – Belo Horizonte – MG – Brazil

[2]Interlab POLI – Universidade de São Paulo (POLI-USP) – São Paulo – SP – Brazil

bagio.valmir@gmail.com, lucymari@gmail.com.br,
maximiliano.jacomo@xpe.edu.br

Abstract. *This study examines the security challenges faced by cryptocurrencies in light of the rapid advancement of quantum computing, which poses a serious threat to the traditional cryptographic foundations of blockchain networks. Widely used algorithms such as RSA and ECDSA are vulnerable to quantum attacks, endangering the confidentiality and integrity of digital transactions. Based on a literature review of academic articles and technical reports, the research identifies key risks and evaluates current post-quantum cryptographic proposals. Although these solutions represent significant progress, their adoption remains limited due to technical, operational, and economic barriers. The study proposes strategies for a secure transition, emphasizing the need for early preparation, continuous development, and active engagement from the crypto community in response to this paradigm shift.*

Keywords: *Cryptocurrencies, Quantum Computing, Post-Quantum Cryptography, Blockchain, Shor's Algorithm, CRYSTALS-Kyber*

Resumo. *Este estudo analisa os desafios de segurança enfrentados pelas criptomoedas diante do avanço da computação quântica, que ameaça comprometer os fundamentos criptográficos tradicionais utilizados em redes blockchain. Algoritmos amplamente adotados, como RSA e ECDSA, mostram-se vulneráveis a ataques baseados em computação quântica, colocando em risco a confidencialidade e a integridade das transações digitais. A pesquisa, fundamentada em revisão bibliográfica de artigos acadêmicos e relatórios técnicos, identifica os principais riscos e avalia as propostas de criptografia pós-quântica atualmente em desenvolvimento. Embora tais soluções representem avanços significativos, sua adoção ainda é limitada por barreiras técnicas, operacionais e econômicas. O estudo propõe estratégias para uma transição segura, reforçando a necessidade de preparação antecipada, desenvolvimento contínuo e engajamento ativo da comunidade cripto frente a essa mudança de paradigma.*

Palavras-chave: *Criptomoedas, Computação Quântica, Criptografia Pós-Quântica, Blockchain, Algoritmo de Shor, CRYSTALS-Kyber*

1. Introdução

A rápida evolução da computação quântica representa uma ameaça para a segurança das criptomoedas, cuja proteção atual depende de mecanismos clássicos como RSA e ECDSA, ambos vulneráveis ao algoritmo de Shor. O algoritmo de Grover também compromete a segurança de funções hash e criptografia simétrica. Estratégias como "Harvest Now, Decrypt Later", que consistem em interceptar dados hoje para decriptá-los futuramente com computadores quânticos, agravam esse cenário [OAKES, 2025].

Esta pesquisa qualitativa e exploratória, baseada em revisão da literatura técnica e científica, analisou os riscos associados e as soluções emergentes. Constatou-se que, em 2021, mais de 99,8% da capitalização de mercado das criptomoedas estava exposta [ALGHAMDI; ALMUHAMMADI, 2021], com provas de conceito recentes (RSA de 50 e 90 bits) reforçando a iminência da ameaça. Como resposta, a criptografia pós-quântica (PQC), com destaque para os padrões do NIST, ML-KEM, ML-DSA e SLH-DSA, surge como principal alternativa [NIST, 2024]. Contudo, sua adoção implica desafios técnicos, como o aumento substancial do tamanho de chaves e assinaturas, impactos no desempenho e escalabilidade das redes, além de barreiras na transição de protocolos. Dado que as projeções indicam a viabilidade de computadores quânticos capazes de quebrar RSA-2048 até 2033 [ALGHAMDI; ALMUHAMMADI, 2021], a adoção proativa de soluções PQC torna-se essencial para assegurar a resiliência e confiabilidade do ecossistema cripto na era quântica.

2. Fundamentação Teórica

A segurança das criptomoedas fundamenta-se em primitivas criptográficas clássicas, como SHA-256 e ECDSA, adotadas no protocolo do Bitcoin desde 2008 para assegurar a autenticidade das transações e a integridade dos dados em sistemas distribuídos baseados em blockchain. A confiabilidade desses sistemas tange na complexidade computacional de problemas matemáticos considerados intratáveis para arquiteturas clássicas, como a fatoração de inteiros e o logaritmo discreto.

A computação quântica representa uma ruptura no paradigma de processamento ao empregar qubits, que exploram os princípios da superposição e do entrelaçamento para realizar operações em múltiplos estados simultaneamente. O algoritmo de Shor (1994) demonstrou a viabilidade de resolver, em tempo polinomial, os problemas de fatoração e logaritmo discreto, bases dos esquemas RSA e ECDSA, por meio da Transformada de Fourier Quântica, essencial para a identificação eficiente de periodicidade em funções aritméticas [VERMA, 2021; NWAGA e IDIMA, 2022]. Adicionalmente, o algoritmo de Grover proporciona uma aceleração quadrática em buscas não estruturadas, impactando a segurança efetiva de funções hash (como SHA-256) e cifradores simétricos (como AES-128), reduzindo a complexidade de ataques de força bruta de $O(2^n)$ para $O(2^{\frac{n}{2}})$.

Embora computadores quânticos tolerantes a falhas ainda estejam em fase experimental, o risco associado a ataques retroativos (“Harvest Now, Decrypt Later”) é significativo, sobretudo para dados cuja exposição de chaves públicas já ocorreu. Avanços recentes incluem a fatoração de inteiros RSA-50 (out. 2024) e RSA-90 (abr. 2025) via técnicas de recozimento quântico com o D-Wave Advantage de 5.760 qubits [HONG et al., 2025]. Apesar de insuficientes frente às chaves modernas (1024 a 2048 bits), esses resultados evidenciam o progresso constante da computação quântica aplicada à criptoanálise.

Nesse cenário, a criptografia pós-quântica (PQC) surge como contramedida, estruturando algoritmos resistentes a adversários providos de capacidades quânticas. As principais linhas de pesquisa incluem esquemas baseados em reticulados (CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon), assinaturas hash-based (SPHINCS+, XMSS), códigos corretores de erros, polinômios multivariados e isogenias sobre curvas elípticas. O processo de padronização liderado pelo NIST desde 2017 culminou em 2024

com a seleção dos primeiros padrões: ML-KEM (criptografia de chave pública baseada em Kyber), ML-DSA (assinaturas digitais com base em Dilithium) e SLH-DSA (assinaturas hash-based com SPHINCS+) [NIST, 2024].

A incorporação de algoritmos PQC em blockchains impõe desafios técnicos substanciais. A substituição de mecanismos como o ECDSA implica reengenharia de carteiras, protocolos de validação de transações, mecanismos de consenso e contratos inteligentes. Aplicações de finanças descentralizadas (DeFi) também herdam vulnerabilidades da camada base [OAKES, 2025]. Embora redes consolidadas, como Bitcoin e Ethereum, adotem uma postura conservadora, iniciativas como Quantum Resistant Ledger (XMSS, WOTS+), IOTA (WOTS, CURL-P), Cellframe, Nexus, HyperCash e Mochimo já integram primitivas resistentes à computação quântica [KIM et al., 2021]. Contudo, mais de 99,8% da capitalização de mercado em 2021 permanecia baseada em ECDSA e EdDSA, mantendo-se suscetível [ALGHAMDI; ALMUHAMMADI, 2021].

A adoção de PQC impacta diretamente requisitos de desempenho e escalabilidade. Assinaturas e chaves públicas tendem a ser ordens de magnitude maiores (até 49 KB no caso de SPHINCS+), elevando a demanda por largura de banda, armazenamento e capacidade de verificação [MARCHSREITER, 2025]. Esquemas baseados em LWE enfrentam adicionalmente o problema do acúmulo de ruído, comprometendo a consistência em ambientes com atualização de chaves [HSU et al., 2024]. A usabilidade também é afetada, devido à complexidade algorítmica e ao impacto na experiência do usuário, exigindo automação e interfaces otimizadas.

Abordagens híbridas, que combinam algoritmos clássicos e pós-quânticos, e blockchains nativamente quânticas estão sendo propostas para mitigar o impacto da transição. Contudo, esquemas híbridos podem herdar vulnerabilidades do algoritmo mais fraco. A migração segura requer protocolos eficazes, variando entre *soft forks* com atraso (como o “commit-delay-reveal”) e *hard forks* estruturais. Um modelo recente, proposto por Almuhammadi e Alghamdi (2025), sugere um *soft fork* sem latência, com período de coexistência (4 anos) entre moedas clássicas (QNR) e pós-quânticas (QR), promovendo transição progressiva com eliminação programada dos ativos não migrados.

A evolução da segurança em criptoativos demanda resiliência diante de ameaças computacionais emergentes. A adoção proativa da PQC configura-se não apenas como necessidade técnica, mas como estratégia de soberania digital. Enquanto os EUA, por meio do NIST, lideram esforços abertos de padronização, a China investe em algoritmos proprietários, apontando para um futuro de possível fragmentação criptográfica global. Estimativas baseadas na Lei de Moore aplicada a qubits projetam a viabilidade de quebra do RSA-2048 por volta de 2033. Assim, o preparo antecipado torna-se imprescindível para assegurar continuidade operacional, integridade dos ativos digitais e mitigação de riscos associados à ausência de *key hygiene*, como exposição de chaves reutilizadas ou transações não rotativas frente a adversários quânticos.

3. Metodologia

3.1 Materiais e Métodos

3.1.1 Delimitação da Pesquisa

Este trabalho adotou uma abordagem qualitativa, exploratória e descritiva, com ênfase em

revisão bibliográfica e análise documental, tendo como foco o estudo da evolução da segurança criptográfica das criptomoedas frente aos avanços da computação quântica. A pesquisa buscou compreender como os sistemas baseados em blockchain, que atualmente se apoiam em algoritmos criptográficos clássicos, podem ser impactados pela emergência da computação quântica e identificar propostas emergentes que visam garantir a resiliência dessas tecnologias. As referências foram organizadas em quatro eixo: criptografia clássica (SHA-256, ECDSA), fundamentos da computação quântica (Shor, Grover), algoritmos pós-quânticos (Kyber, Dilithium, SPHINCS+) e desafios de transição (soft/hard forks, desempenho, usabilidade).

3.1.2 Ferramentas e Procedimentos

A coleta de dados foi realizada por meio de busca sistemática em repositórios como IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, Scopus, Google Scholar e documentos oficiais do NIST. Foram consideradas também white papers de projetos de criptomoedas com foco em segurança pós-quântica (como QRL, IOTA, Cellframe). Utilizou-se Zotero para gestão das referências, Google Planilhas para construção da matriz analítica e Google Docs para a redação final. A leitura crítica priorizou artigos revisados e documentos normativos, com identificação de lacunas, convergências e divergências.

3.2 Etapas da Pesquisa

3.2.1 Delimitação e Análise da Criptografia Clássica

Inicialmente, definiu-se o problema de pesquisa centrado na vulnerabilidade das criptomoedas diante da computação quântica. Foram estudadas as bases da criptografia clássica em blockchain, como SHA-256 e ECDSA, compreendendo seus mecanismos de segurança e papel na arquitetura distribuída das redes.

3.2.2 Fundamentos da Computação Quântica e Algoritmos Pós-Quânticos

A segunda etapa focou nos fundamentos da computação quântica, abordando conceitos como qubits, superposição, entrelaçamento e paralelismo quântico. Estudaram-se os algoritmos de Shor e Grover e seus impactos sobre RSA, ECDSA e SHA-256. Em seguida, foram analisados os principais algoritmos pós-quânticos em processo de padronização pelo NIST (ML-KEM, ML-DSA, SLH-DSA), com ênfase em suas características técnicas e aplicabilidades.

3.2.3 Seleção e Organização das Fontes

Com base na leitura seletiva, os dados foram sistematizados em uma matriz analítica, permitindo a classificação das informações por tipo de abordagem e contribuição. Essa organização serviu como suporte à fundamentação teórica e análise de resultados.

3.2.4 Análise Comparativa e Desafios de Transição

Foi realizada uma análise comparativa entre criptomoedas tradicionais e aquelas com implementação de algoritmos pós-quânticos, como QRL, Cellframe, Nexus e HyperCash. Avaliaram-se os impactos em tamanho de transação, desempenho e escalabilidade. Ademais, investigaram-se os desafios de migração de algoritmos, riscos como o uso de chaves antigas, exposição de carteiras, e protocolos como soft e hard forks.

3.2.5 Artigo e Proposições Finais

A redação dos capítulos foi desenvolvida para apresentar os conceitos e processos técnicos com clareza, visando à máxima acessibilidade e compreensão do tema. Ao final do estudo, as principais conclusões da pesquisa foram consolidadas, enfatizando os desafios e os notáveis avanços da criptografia pós-quântica aplicada à tecnologia blockchain. Adicionalmente, foram delineadas perspectivas para investigações futuras, a fim de garantir a segurança contínua das criptomoedas no cenário da computação quântica emergente.

4.Resultados e Discussão dos Resultados

Esta seção apresenta e analisa criticamente os principais resultados da revisão bibliográfica, relacionando-os ao futuro das criptomoedas frente à computação quântica. O principal resultado foi a criação da Matriz Analítica de Referências sobre Segurança Cripto Pós-Quântica, que sistematiza as contribuições das fontes em temas como tipos de criptografia, vulnerabilidades, migração, padronização, usabilidade e ataques quânticos. A matriz serviu como base empírica para a análise comparativa dos dados.

Fonte (Autor, Ano) \ Aspectos Analisados	Tipo de Criptografia / Algoritmos Base	Vulnerabilidade Quântica Identificada	Proposta de Migração para PQC	Impactos Operacionais da PQC	Desafios de Usabilidade e Privacidade	Adoção Real / Projetos com PQC
[NIST, 2024]	PQC (ML-KEM/Kyber, ML-DSA/Dilithium, SLH-DSA/Sphincs+)	Implícita: necessidade de PQC	Padronização para transição imediata	Critérios de desempenho, tamanho de chaves/assinaturas/recurso	-	Publicação dos primeiros padrões finalizados pelo NIST
[ALGHAMDI; ALMUHAMMADI, 2021]	Clássica (ECDSA, EdDSA, SHA-256)	Shor (exponencial), Grover (quadrático).	Urgência da migração para PQC	Impacto de PQC no desempenho, tamanho de transações, escalabilidade e descentralização	-	Lista criptos vulneráveis (BTC, ETH) e quantum-safe (<0.2% market cap)
[KIM et al., 2021]	Clássica (ECC/ECDSA); PQC (Lamport, WOTS, XMSS, Ring-LWE, Dilithium, Picnic, NTRU, Frodo, SIDH, SPHINCS+)	Shor para ECC/ECDSA.Grover para hashes	Criptomoedas já "quantum-safe" ou com planos de implementação PQC	Chaves hash-based podem ser impraticáveis devido ao desempenho	-	Detalha QRL, IOTA, Nexus, HyperCash, Cellframe, Mochimo e seus algoritmos
[ALMUHAMMADI; ALGHAMDI, 2025]	Clássica vs. PQC	Criptografia de chave pública (assinaturas digitais) vulnerável a ataques quânticos	Propõe novo protocolo soft fork com período de carência (4 anos p/ Bitcoin))	Reduz risco de splitting; garante continuidade de transações durante a migração	-	Proposta de protocolo de transição (soft fork com grace period)
[OAKES, 2025]	Clássica (ECDSA) vs. PQC (Dilithium, SPHINCS+)	Shor (RSA/ECDSA), Grover (hashes) ."Harvest Now, Decrypt Later"	Transição complexa: híbrida, via soft forks/sidechains.	Algoritmos PQC mais volumosos (chaves/assinaturas 10x maiores), afeta armazenamento, processamento	Complexidade para usuário (chaves maiores), privacidade (Harvest Now). Necessidade de "key hygiene"	Ênfase no design centrado no usuário para migração PQC
[VERMA, 2021]	Clássica (RSA, ECC) vs. PQC (Lattice, Hash, Multivariate, Code)	RSA/ECC Shor; hashes Grover	PQC e QKD para segurança futura	PQC computacionalmente intensiva, aumento de tempo, redução de "throughput"	Desafios de usabilidade pela complexidade de PQC, gerenciamento de chaves	QRL (XMSS), QSB (Dilithium)
[GILBERT; GILBERT, 2025]	Clássica (geral) vs. Quantum-Resistant	Criptografia de chave pública e funções hash em blockchain são vulneráveis	QRA como solução emergente.	-	Menciona privacidade e controle de dados pelo usuário em sistemas descentralizados	PQC como promessa para defesas futuras em cybercrimes de criptos.
[HSU et al., 2024]	Clássica (DLP) vs. PQC (LWE-based)	Sistemas baseados em DLP/Shor	Adaptação do protocolo Quisquis para UPKs LWE-based.	Desafios de acumulação de ruído em UPKs LWE-based. Protocolo Quisquis (foco em privacidade e chaves atualizáveis)	Acúmulo de ruído em UPKs LWE-based; necessidade de redesenho	Protocolo Quisquis (foco em privacidade e chaves atualizáveis)
[NWAGA; IDIMA, 2022]	Clássica (RSA, ECC, DH) vs. PQC (Lattice, Hash, Code, Multivariate, Isogeny)	Shor (RSA/ECC/DH), Grover (AES-128). "Harvest Now, Decrypt Later"	Hard/Soft forks. Modelos criptográficos híbridos.	Eficiência computacional, tamanho da chave, sobrecarga de comunicação, escalabilidade	Desafios de eficiência computacional e tamanho de chaves impactam armazenamento e latência em nuvem	Ethereum, Hyperledger, Algorand testando PQC. Google Cloud, Azure, AWS integrando PQC.

Figura 1: Matriz Analítica de Referências sobre Segurança Cripto Pós-Quântica

4.1 A Ameaça Quântica: Da Teoria à Evidência Preliminar

A análise da literatura, sintetizada na Matriz Analítica, confirmou categoricamente a vulnerabilidade intrínseca da segurança criptográfica das criptomoedas modernas frente à emergência de computadores quânticos de grande escala. Algoritmos amplamente utilizados como o RSA e o ECDSA (Elliptic Curve Digital Signature Algorithm), fundamentais para a integridade das transações digitais, são diretamente ameaçados pelo Algoritmo de Shor, que pode resolver os problemas de fatoração de grandes inteiros e de logaritmo discreto em tempo polinomial. Adicionalmente, o Algoritmo de Grover representa um risco significativo ao reduzir quadraticamente a segurança efetiva de funções hash (como SHA-256) e de criptografia simétrica (como AES-128) através de ataques de força bruta, exigindo um dobro no tamanho da chave para manter o mesmo nível de segurança clássico [GILBERT; GILBERT, 2025].

A Matriz Analítica destaca também a crescente[preocupação com a estratégia "Harvest Now, Decrypt Later", onde dados criptografados hoje podem ser interceptados e armazenados para posterior decifração quando a tecnologia quântica atingir a maturidade necessária. Esta ameaça é reforçada por avanços experimentais recentes: em outubro de 2024, pesquisadores chineses demonstraram a fatoração bem-sucedida de um número RSA de 50 bits e, em abril de 2025, um RSA de 90 bits, ambos utilizando um computador quântico D-Wave Advantage de 5.760 qubits via recozimento quântico. Embora esses experimentos sejam provas de conceito impressionantes e os números fatorados ainda sejam ordens de magnitude menores que as chaves RSA de 1024 a 2048 bits em uso atualmente, eles sinalizam que a ameaça quântica está se aproximando da realidade prática. Projeções baseadas na Lei de Moore para qubits estimam que computadores quânticos capazes de quebrar RSA-2048 poderão surgir já em 2033.

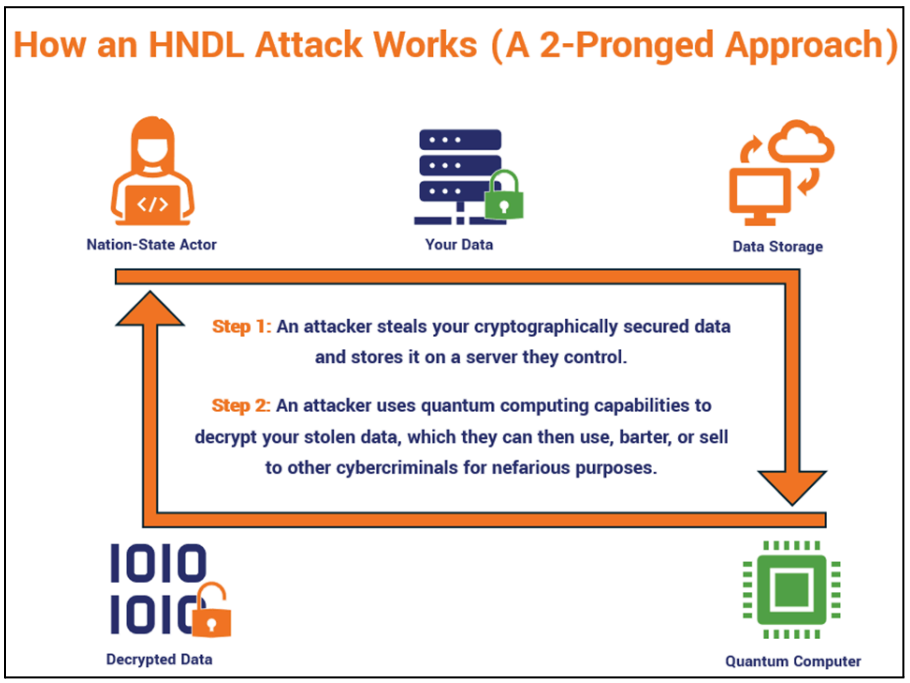

Figura 2: Demonstração da estratégia "Harvest Now, Decrypt Later" [CRANE, 2024]

4.2 Panorama Atual das Criptomoedas sob a Ótica Quântica

A análise dos dados compilados na Matriz corrobora uma vulnerabilidade alarmante no ecossistema atual de criptomoedas. Em 2021, mais de 99,8% da capitalização de mercado total das criptomoedas foi identificada como vulnerável a ataques quânticos. Criptomoedas proeminentes como Bitcoin, Ethereum, Litecoin, Tether, Binance, Zcash, Monero, Grin e Beam, que representavam a vasta maioria da capitalização, dependem principalmente de algoritmos de assinatura digital baseados em Problemas do Logaritmo Discreto em Curvas Elípticas (ECDSA ou EdDSA) ou variações como RingCT, todas suscetíveis ao Algoritmo de Shor.

Em contraste, a Matriz também mapeou uma pequena fração do ecossistema que já implementa soluções resistentes a ataques quânticos. Essas "quantum-safe cryptocurrencies" incluem projetos como Quantum Resistant Ledger (QRL), que utiliza XMSS e WOTS+; IOTA (MIOTA), com WOTS e planos para CURL-P; Cellframe

(CELL), com multi-assinaturas, Dilithium e Picnic; Nexus (NXS), com Signature Chains; HyperCash (HC), adotando Ring LWE; e Mochimo (MCM), com XMSS+ e WOTS+. Contudo, o valor de mercado combinado dessas moedas "quantum-safe" representava menos de 0,2% do total em agosto de 2021, sublinhando a vasta e persistente exposição ao risco.

4.3 Algoritmos Pós-Quânticos (PQC) e Seus Trade-offs

A criptografia pós-quântica (PQC) surge como a principal resposta à ameaça quântica, buscando substituir os algoritmos vulneráveis por novos esquemas baseados em problemas matemáticos considerados difíceis para computadores clássicos e quânticos. A Matriz Analítica detalha as principais famílias de algoritmos PQC, como reticulados (Lattice-based), hash-based, code-based, polinômios multivariados e isogenias. O processo de padronização liderado pelo NIST, iniciado em 2017 e com duração estimada de oito anos, culminou em agosto de 2024 com a finalização dos três primeiros padrões: ML-KEM (baseado em CRYSTALS-Kyber) para criptografia geral; ML-DSA (baseado em CRYSTALS-Dilithium) como padrão primário para assinaturas digitais; e SLH-DSA (baseado em SPHINCS+) como padrão alternativo para assinaturas. Esses algoritmos são extensivamente avaliados quanto à resistência quântica, desempenho, tamanho de chaves e assinaturas, e consumo de recursos.

A análise comparativa presente na Matriz revela trade-offs significativos da PQC em relação aos algoritmos clássicos, impactando diretamente sua viabilidade em ambientes blockchain. Algoritmos PQC geram chaves públicas e assinaturas substancialmente maiores, podendo ser dez vezes maiores ou mais que as clássicas. Por exemplo, o algoritmo SPHINCS+ pode gerar assinaturas de até 49 KB, enquanto Dilithium e Falcon também produzem assinaturas e chaves na ordem dos kilobytes, contrastando com as poucas dezenas de bytes do ECDSA. Esse aumento impacta diretamente o tamanho das transações e blocos, demandando maior largura de banda e poder computacional para validação. Em termos de desempenho, o custo computacional da PQC é geralmente maior. Embora a performance varie, Dilithium demonstra ser mais rápido que Falcon em dispositivos embarcados (ARM CPUs) para TPS, enquanto Falcon-512 é mais adequado para blockchains baseadas em computador. O SPHINCS+ pode ser muito lento para operações em sistemas com recursos limitados.

4.4 Desafios de Transição e Implicações Operacionais

A transição para algoritmos pós-quânticos nas criptomoedas implica uma série de desafios técnicos e operacionais complexos, que vão muito além da simples substituição de códigos, afetando profundamente a infraestrutura existente e a experiência do usuário. A substituição de mecanismos como ECDSA por esquemas PQC requer mudanças profundas na geração e validação de transações, no funcionamento de carteiras digitais, nos protocolos de consenso e na estrutura da blockchain. Além disso, contratos inteligentes e aplicações DeFi também herdariam as vulnerabilidades quânticas da camada base, ampliando o escopo do risco e exigindo atualizações complexas.

O impacto na usabilidade e privacidade emerge como um obstáculo crítico. Chaves e assinaturas maiores podem dificultar a interação do usuário, demandando interfaces mais amigáveis e automatização do gerenciamento de chaves. A privacidade também é afetada, pois transações com chaves públicas expostas hoje poderiam ser decifradas

retroativamente. O conceito de "higiene de chaves" (*key hygiene*) torna-se essencial para que usuários compreendam a necessidade de proteger e atualizar suas chaves. Em esquemas baseados em reticulados (como LWE), o acúmulo de ruído durante atualizações de chave é um desafio que pode levar a falhas de verificação.

As propostas de protocolos de transição variam entre *soft forks* e *hard forks*. *Soft forks*, como o modelo "commit-delay-reveal", apresentam atrasos na confirmação e exigem moedas PQC para transação, sofrendo com lentidão. *Hard forks*, como o proposto por Anhao (2018) para Bitcoin PostQuantum, alteram radicalmente a rede e enfrentam resistência comunitária pelo risco de divisão da blockchain e dificuldade de consenso. A governança das comunidades blockchain é um fator crítico, podendo dificultar ou acelerar a adoção de mudanças complexas como PQC. O protocolo recente de Almuhammadi e Alghamdi (2025) propõe um *soft fork* sem atrasos, com um período de carência (*grace period*) de aproximadamente quatro anos (para Bitcoin, de bloco 945.000 a 1.155.000), durante o qual moedas clássicas (QNR) e pós-quânticas (QR) coexistiriam, e QNRs não convertidas seriam queimadas ao final, promovendo uma migração controlada. A maior complexidade e tamanho dos algoritmos PQC podem reduzir o *throughput* (TPS) e aumentar os requisitos de armazenamento. Soluções como agregação de assinaturas, verificação em lote (*batch verification*), criptografia de limiar (*threshold cryptography*) e escalonamento de camada 2 (*Layer-2*, como *zk-rollups*) são exploradas para mitigar esses gargalos. O custo computacional e energético da PQC é geralmente mais elevado.

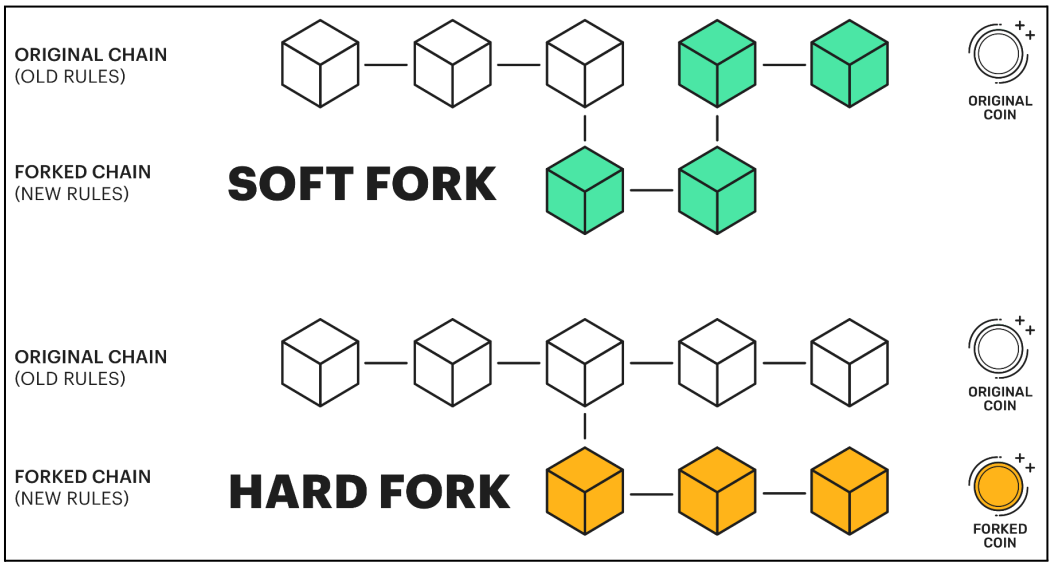

Figura 3: Demonstração da Diferença entre *Soft Fork* e *Hard Fork* [TANGEM, 2023].

4.5 Perspectivas e Necessidade de Ação Proativa

A ameaça da computação quântica à segurança das criptomoedas não é mais especulativa, demandando ação imediata e estratégica. Os artigos analisados indicam uma urgência crescente na adoção de soluções PQC. O NIST, por exemplo, recomenda que administradores de sistema iniciem imediatamente a integração dos novos padrões.

A adoção da criptografia resistente a ataques quânticos assume dimensão de soberania nacional, com governos buscando proteger seus ativos digitais e comunicações estratégicas. Enquanto os EUA, via NIST, lideram o processo de padronização, a China desenvolve sistemas próprios, o que pode levar a fragmentação criptográfica global.

Apesar da maioria das criptomoedas ainda ser vulnerável, iniciativas de PQC estão em andamento em projetos como QRL, IOTA, Cellframe, HyperCash e Mochimo. Grandes empresas como IBM, Google Cloud, Microsoft Azure e Accenture investem em pesquisa, desenvolvimento e testes de soluções PQC para seus serviços de nuvem e blockchain.

5.Conclusão

A iminência da computação quântica impõe uma mudança de paradigma na segurança das criptomoedas. Com algoritmos como RSA e ECDSA comprovadamente vulneráveis ao Algoritmo de Shor, é imprescindível abandonar a postura reativa e iniciar, desde já, a transição para mecanismos criptográficos resistentes a ataques quânticos.

Nesse cenário, os algoritmos padronizados pelo NIST em 2024 despontam como alternativas viáveis para resistir à computação quântica. O CRYSTALS-Kyber (ML-KEM) foi escolhido para criptografia de chave pública, enquanto o CRYSTALS-Dilithium (ML-DSA) tornou-se o principal esquema de assinatura digital. Já o SPHINCS+ (SLH-DSA) foi adotado como uma alternativa segura baseada em funções hash. Contudo, a simples substituição dos algoritmos não é suficiente.

A migração para a criptografia pós-quântica exigirá reestruturações profundas em diversas camadas do ecossistema, incluindo os protocolos de validação de transações e o funcionamento das carteiras digitais, os contratos inteligentes e as plataformas de finanças descentralizadas (DeFi), os mecanismos de consenso e os modelos de governança das redes, além do desenvolvimento de interfaces mais intuitivas, capazes de mitigar a complexidade algorítmica e lidar com o aumento significativo no tamanho das chaves e assinaturas.

Além disso, será necessário implementar práticas de higiene criptográfica, como rotação periódica de chaves, proteção contra reuso de endereços e estratégias contra ataques retroativos ("Harvest Now, Decrypt Later").

Sendo assim, recomenda-se que os desenvolvedores de blockchains adotem modelos de soft fork progressivos, com fases de coexistência entre esquemas clássicos e pós-quânticos, como proposto por Almuhammadi e Alghamdi (2025). O uso de técnicas como agregação de assinaturas, verificação em lote, e soluções Layer-2 (ex.: *zk-rollups*) será fundamental para mitigar os impactos na escalabilidade e desempenho.

Conclui-se, portanto, que garantir a resiliência do ecossistema cripto na era quântica exige mais do que a adoção de novos algoritmos: demanda planejamento estratégico, inovação em protocolos e cooperação ativa entre pesquisadores, desenvolvedores, instituições e governos.

Referências

NIST (National Institute of Standards and Technology). *NIST Releases First 3 Finalized Post-Quantum Encryption Standards*. 13 de agosto de 2024. Disponível em: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards. Acesso em: 22 jun. 2025.

ALGHAMDI, S.; ALMUHAMMADI, S. The Future of Cryptocurrency Blockchains in the Quantum Era. In: *2021 IEEE International Conference on Blockchain (Blockchain)*, Sydney, NSW, Australia, 2021. p. 544-551.

KIM, H. J. et al. 순환 신경망을 활용한 양자 내성 암호화폐 가격 예측 (Prediction of the price of quantum-resistant cryptocurrency using recurrent neural network). In: *ACK 2021 학술발표대회 논문집 (Anais da Conferência da Sociedade Coreana de Criptografia e Segurança da Informação)*, 2021.

ALMUHAMMADI, S.; ALGHAMDI, S. A novel transition protocol to post-quantum cryptocurrency blockchains. *Frontiers in Computer Science*, v. 7, p. 1457000, 21 mai. 2025. DOI: 10.3389/fcomp.2025.1457000.

OAKES, S. T. Enhancing Usable Security and Privacy of Cryptocurrencies in the Quantum Age. *Academic Festival, Event 200*, Sacred Heart University, 2025. Disponível em: https://digitalcommons.sacredheart.edu/acadfest/2025/all/200. Acesso em: 15 mai.2025.

VERMA, R. The Future of Cryptocurrency: Quantum-Secure Blockchain Protocols. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, v. 2, n. 4, p. 11-17, 2021. DOI: 10.63282/30509262/IJAIDSML-V214P102.

GILBERT, C.; GILBERT, M. A. Patterns and vulnerabilities of cryptocurrency-related cybercrimes. *Global Scientific Journals*, v. 13, n. 3, mar. 2025.

HSU, H. Y. et al. Quantum-Resistant Updatable Public Keys: Enhancing the Quisquis Protocol with LWE-Based Security. In: *2024 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, 2024.

NWAGA, P.; IDIMA, S. Post-Quantum Cryptographic Algorithms for Secure Communication in Decentralized Blockchain and Cloud Infrastructure. *International Journal of Computer Applications Technology and Research*, v. 11, n. 4, p. 155-170, 2022. DOI: 10.7753/IJCATR1104.1008.

HONG, C. L. et al. Quantum attack on RSA by D-Wave Advantage: a first break of 80-bit RSA. *Science China Information Sciences*, v. 68, n. 2, p. 129501:1-129501:2, fev. 2025. DOI: 10.1007/s11432-024-4163-6.

CASEY CRANE (The SSL Store™). *Harvest Now, Decrypt Later (HNDL): A Look at This Current & Future Threat.* The SSL Store™. 6 ago. 2024. Disponível em: https://www.thesslstore.com/blog/harvest-now-decrypt-later-hndl/. Acesso em: 5 mar. 2025.

TANGEM Team. Soft Fork vs Hard Fork: Definition and Differences. 13 out. 2023. Disponível em: https://tangem.com/en/blog/post/what-are-hard-forks-and-soft-forks/. Acesso em: 1 jun. 2025.