Blockchain na Era Quântica: Uma *Rapid Review* sobre Avanços, Lacunas e Direções Futuras

Mateus Bastos
mateus.araujo@icen.ufpa.br
Universidade Federal do Pará
Belém, Pará, Brasil

Alan Veloso
aveloso@ufpa.br
Universidade Federal do Pará
Belém, Pará, Brasil

Diego Abreu
diego.abreu@itec.ufpa.br
Universidade Federal do Pará
Belém, Pará, Brasil

Jeffson Sousa
jcsousa@cpqd.com.br
Centro de Pesquisa e Desenvolvomento em Telecomunicações
Campinas, São Paulo, Brasil

Bruno Evaristo
elderb@cpqd.com.br
Centro de Pesquisa e Desenvolvomento em Telecomunicações
Campinas, São Paulo, Brasil

Antônio Abelém
abelem@ufpa.br
Universidade Federal do Pará
Belém, Pará, Brasil

Resumo

A computação quântica ameaça a segurança das blockchains, impulsionando a pesquisa em soluções que buscam desde sua resistência até sua integração com tecnologias quânticas. Esta revisão rápida analisa 36 estudos recentes para mapear avanços, lacunas e direções futuras. Os resultados mostram um foco dominante em integração com criptografia pós-quântica (66,7% dos estudos) em comparação com abordagens quânticas (22,2%). Além disso, mostra-se a baixa reprodutibilidade experimental, pois apenas 30,6% dos artigos fornecem dados suficientes para replicação. Destaca-se desafios como o custo de desempenho e interoperabilidade, concluindo com a defesa de *benchmarks* padronizados e maior foco na validação experimental para construir blockchains seguras para a era quântica.

Keywords

Blockchain, Quantum, Post-Quantum, Reprodutibilidade, Interoperabilidade

1 Introdução

A crescente ameaça representada pelos computadores quânticos aos sistemas criptográficos clássicos tem impulsionado a pesquisa em blockchains resistentes a ataques quânticos, seja por meio de abordagens como criptografia pós-quântica (PQC), ou pela integração direta de princípios quânticos [5]. Enquanto a PQC busca substituir algoritmos vulneráveis, como ECDSA [14] e RSA [22], por alternativas baseadas em reticulados, códigos ou *hashes*, as blockchains quânticas exploram propriedades como emaranhamento e superposição para criar novos paradigmas de consenso e segurança. No entanto, a literatura atual apresenta lacunas significativas, desde a falta de implementações práticas até desafios não resolvidos de escalabilidade e interoperabilidade [37]. Esta revisão visa identificar tendências e propor direções futuras para pesquisas nesse campo emergente.

Dentre os desafios práticos não resolvidos, destacam-se a escalabilidade de algoritmos de PQC, especialmente em dispositivos com recursos limitados, e a latência intrínseca a protocolos quânticos como *Quantum Key Distribution* (QKD). Embora alguns artigos proponham soluções inovadoras, como consenso baseado em entrelaçamento quântico [1] ou assinaturas agregadas [4], poucos avaliam seu desempenho em cenários realistas ou em comparação com sistemas clássicos. A interoperabilidade entre blockchains tradicionais e sistemas pós-quânticos/quânticos também é negligenciada, representando uma barreira significativa para a adoção em larga escala. [37]

Este artigo não apenas sintetiza o conhecimento atual, mas também fornece um roteiro para pesquisadores interessados em contribuir para o campo. Ao priorizar a reprodutibilidade e o alinhamento com padrões emergentes, como os algoritmos de PQC aprovados pelo NIST [26], a comunidade pode acelerar a transição para blockchains verdadeiramente seguras na era quântica. As recomendações aqui apresentadas destacam a necessidade de equilibrar avanços teóricos com validação experimental, garantindo a viabilidade de reprodução.

O artigo está organizado da seguinte forma: a Seção 2 faz uma breve análise de trabalhos relacionados. A Seção 3 apresenta a fundamentação teórica a respeito de blockchain pós-quânticas e quânticas, além de algoritmos e protocolos explorados nessa revisão. A Seção 4 demonstra a metodologia utilizada no processo de desenvolvimento da *rapid review*. A Seção 5 mostra os resultados obtidos a partir da análise dos estudos coletados após a busca. Por fim, a Seção 6 conclui o trabalho e fornece direções para trabalhos futuros na área.

2 Trabalhos Relacionados

Diversos estudos têm investigado os impactos da computação quântica sobre as blockchains. Gharavi et al. analisam a integração da criptografia pós-quântica (PQC) em cenários de IoT, com forte ênfase nos algoritmos padronizados pelo NIST. Embora apresentem grande profundidade técnica, sua análise limita-se ao contexto de dispositivos restritos e permanece em nível conceitual, sem tratar de forma consistente a reprodutibilidade experimental. [11]

Yang et al., por sua vez, comparam blockchains pós-quânticas e quânticas, discutindo diferenças de arquitetura, segurança e interoperabilidade. O estudo contribui ao destacar a possível coexistência dessas soluções na transição tecnológica, mas sua abordagem ainda é predominantemente teórica, sem métricas quantitativas ou avaliação prática da viabilidade das propostas. [37]

Em contraste, este artigo apresenta uma *rapid review* de 36 estudos recentes, trazendo métricas inéditas como o predomínio da

PQC (66,7%) em relação a abordagens quânticas (22,2%) e a baixa reprodutibilidade experimental (30,6%). O diferencial está na ênfase em lacunas práticas, como interoperabilidade e validação experimental, e na proposição de *benchmarks* padronizados, aproximando o debate teórico das implementações reais, conforme mostrado na Tabela 1.

Tabela 1: Comparação dos trabalhos relacionados

Aspecto	[11]	[37]	Bastos et al.
Foco em PQC	X	X	X
Foco em blockchains quânticas		X	X
Escopo específico (IoT)	X		
Comparação entre abordagens		X	X
Análise quantitativa			X
Reprodutibilidade/validação			X
Propostas práticas			X

3 Fundamentação Teórica

Para compreender os desafios e avanços em blockchains integradas com tecnologias quânticas, é necessário definir os conceitos fundamentais que permeiam essa área de pesquisa. Esta seção explica os princípios básicos de PQC, de blockchains quânticas e pós-quânticas, bem como dos principais algoritmos e protocolos que as sustentam.

3.1 Computação Quântica

A computação quântica representa um paradigma radicalmente diferente da computação clássica, aproveitando fenômenos da mecânica quântica como superposição e emaranhamento para realizar operações. Enquanto os computadores clássicos usam bits binários (0 ou 1), os computadores quânticos utilizam qubits, representado na Figura 1, que podem existir em múltiplos estados simultaneamente. Essa propriedade permite que algoritmos quânticos resolvam certos problemas exponencialmente mais rápido que os clássicos [28]. O estado de um qubit, representado por $|\psi\rangle$, é uma superposição linear dos seus dois estados de base, $|0\rangle$ e $|1\rangle$. A fórmula é:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Onde α e β são amplitudes de probabilidade de números complexos que devem satisfazer a condição de normalização:

$$|\alpha|^2 + |\beta|^2 = 1$$

Dois algoritmos quânticos são particularmente relevantes para a segurança das blockchains: o algoritmo de Shor, que pode quebrar sistemas criptográficos baseados em fatoração de números primos e logaritmos discretos em tempo polinomial; e o algoritmo de Grover, que oferece uma aceleração quadrática para buscas em bancos de dados não estruturados, afetando a segurança de funções *hash* simétricas [16]. Além disso, a comunicação quântica, particularmente através da QKD, permite a troca segura de chaves criptográficas com detecção garantida de interceptação, embora ainda enfrente desafios práticos de implementação em larga escala. [35]

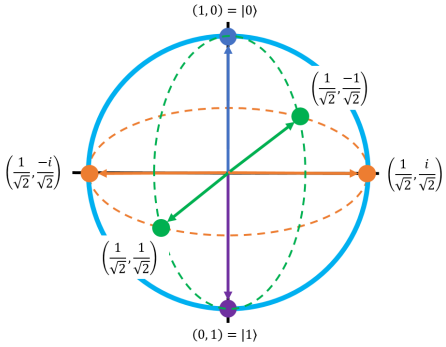

Figura 1: Representação de um Qubit. [23]

3.2 Criptografia Pós-Quântica (PQC)

A criptografia pós-quântica refere-se a algoritmos criptográficos projetados especificamente para resistir a ataques de computadores quânticos, especialmente aqueles capazes de executar os algoritmos de Shor e Grover [16]. Diferente da criptografia clássica que depende de problemas como fatoração de números primos ou logaritmos discretos, a criptografia pós-quântica baseia-se em problemas matemáticos considerados difíceis mesmo para computadores quânticos.

As principais abordagens incluem sistemas baseados em reticulados, como CRYSTALS-Dilithium e Kyber [3, 8], que exploram a complexidade de resolver problemas em estruturas geométricas multidimensionais e esquemas baseados em *hash* como SPHINCS+ [31]. O NIST tem liderado o esforço de padronização desses algoritmos para substituir os padrões atuais vulneráveis. [26]

3.3 Blockchain Pós-Quântica

As blockchains pós-quânticas são redes distribuídas que utilizam algoritmos de criptografia pós-quântica em suas operações fundamentais, como assinaturas digitais, funções *hash* e protocolos de consenso [37]. O objetivo principal é manter a segurança das transações e do consenso na era da computação quântica sem exigir mudanças radicais na arquitetura das blockchains atuais.

Na prática, isso envolve substituir algoritmos como ECDSA [14] por alternativas pós-quânticas como Dilithium ou Falcon [31], adaptar funções *hash* para versões resistentes ao algoritmo de Grover, e modificar protocolos de consenso como *Proof-of-Work* ou *Proof-of-Stake* para incorporar primitivas pós-quânticas. O maior desafio desta abordagem está na eficiência computacional, já que muitos algoritmos pós-quânticos demandam significativamente mais recursos de memória, energia e largura de banda que seus equivalentes clássicos. [37]

3.4 Blockchain Quântica

Em contraste às blockchains pós-quânticas, as blockchains quânticas não apenas resistem a ataques quânticos, mas integram ativamente princípios da mecânica quântica em sua operação. Estas redes podem utilizar o emaranhamento quântico para criar novos protocolos de consenso distribuído que superam limites clássicos, como a tolerância a falhas bizantinas [37]. Assinaturas digitais

quânticas (QDS) baseadas em estados quânticos oferecem segurança incondicional contra falsificação, aproveitando o princípio da não-clonagem quântica [12].

A comunicação entre nós pode ser realizada através de protocolos quânticos como o QKD [35], que garante a detecção de qualquer tentativa de interceptação. No entanto, a implementação prática destas blockchains enfrenta desafios tecnológicos significativos, incluindo a necessidade de qubits estáveis com baixa decoerência, memória quântica eficiente e infraestrutura de comunicação quântica escalável, componentes que ainda estão em estágios relativamente iniciais de desenvolvimento. [18]

4 Metodologia

Nesta seção será descrito o passo a passo da *rapid review* desenvolvida neste trabalho. As subseções subsequentes abaixo mostrarão seu desenvolvimento.

4.1 Questões de Pesquisa

Para absorver as informações coletadas de forma plena, foram definidas questões de pesquisa (QP), listadas abaixo:

- **QP1**: O estudo aborda blockchains pós-quânticas ou blockchains quânticas?
- **QP2**: Se o estudo aborda blockchains pós-quânticas, blockchains quânticas ou ambas, relatam a existência de implementações reprodutíveis?
- **QP3**: O estudo trata da compatibilidade entre os requisitos físicos da computação quântica e os requisitos lógicos de uma blockchain funcional?
- **QP4**: O estudo aborda os requisitos computacionais para executar simulações de blockchains quânticas e compara esses requisitos com o que já é possível em termos de hardware?
- **QP5**: O estudo aborda o grau de reprodutibilidade dos experimentos e simulações apresentados, incluindo dados abertos, ambientes de teste ou frameworks utilizados?
- **QP6**: O estudo aborda se as tecnologias quânticas propostas resolvem de fato gargalos e vulnerabilidades conhecidas das blockchains atuais?
- **QP7**: Se o estudo abordar tecnologias quânticas, a proposta está alinhada com os avanços reais da criptografia quântica e da comunicação quântica?

4.2 Buscas de Dados e Informações

Após a definição das questões de pesquisa, foi definida a *string* de busca utilizada para fazer a busca na plataforma de base de dados escolhidas: *("quantum blockchain"**OR** "post-quantum blockchain"**OR** "quantum-resistant blockchain"**OR** "blockchain-based") **AND** ("quantum consensus"**OR** "quantum key distribution"**OR** "quantum ledger"**OR** "post-quantum cryptography")*. Essa *string* foi formulada pensando em cobrir tanto tecnologias de blockchains pós-quânticas quanto blockchains quânticas, além de cobrir também tecnologias adjacentes a implementação tais como QKD e PQC. Por fim, a base de dados utilizada para buscar os trabalhos analisados nesta revisão foi o Scopus, sua escolha é justificada pela ampla cobertura de publicações científicas e por incluir artigos de outras bases importantes, como IEEE Xplore, Springer e ACM.

4.3 Critérios de Inclusão e Exclusão

Seguindo o planejamento, houve a definição do critério de inclusão:

- O estudo aborda blockchain e computação quântica de forma integrada

E dos critérios de exclusão:

- Não foi possivel ter acesso ao estudo
- O estudo não está escrito em inglês
- O estudo não está entre os anos de 2020 e 2025[1]
- O estudo não trata de blockchain e computação quântica de forma integrada
- O estudo não é um estudo primário

Dessa forma, foi finalizada a etapa de planejamento da revisão sistemática.

4.4 Limitações Metodológicas

Por fim, vale ressaltar que a metodologia de *rapid review*, por sua natureza, visa fornecer uma síntese ágil e focada, podendo não ser tão exaustiva quanto uma revisão sistemática da literatura (RSL) completa. No entanto, não invalidam os resultados, os quais foram focados em investigar a reprodutibilidade da inetgração de blockchain e tecnologias quânticas.

5 Resultados

Na fase de execução da revisão, foram inicialmente importados 86 artigos usando a *string* de busca especificada, na base de dados da Scopus. Após aplicar critérios de seleção, 3 artigos duplicados foram identificados, restando 83. Desses, 36 foram aceitos conforme os critérios de inclusão. A etapa seguinte envolveu a análise dos artigos selecionados para analisar e documentar as integrações, lacunas e direções das tecnologias blockchains na era da computação quântica.

5.1 Distribuição de Artigos por Abordagem

Dos 36 estudos analisados, 24 (66,7%) focaram em blockchains pós-quânticas, utilizando criptografia resistente a ataques quânticos, como por exemplo: CRYSTALS-Dilithium, Falcon e esquemas baseados em reticulados. Apenas 8 (22,2%) exploraram blockchains quânticas, integrando princípios como emaranhamento e QKD, enquanto 4 (11,1%) abordaram ambas as vertentes, informações mostradas em Figura 2. Essa disparidade reflete o estágio mais maduro da criptografia pós-quântica em comparação com as tecnologias quânticas práticas, ainda em desenvolvimento [37].

Dentre os estudos pós-quânticos, destacam-se [29], [19] e [15] que implementaram os algoritmos CRYSTALS-Dilithium e Falcon recentemente padronizados pelo NIST. Estes demonstraram eficácia teórica contra ataques quânticos, embora com *trade-offs* em desempenho. Por outro lado, os estudos quânticos como [1], [24] e [34] exploraram conceitos inovadores como emaranhamento quântico e QDS, com [34] alcançando experimentalmente 45% de tolerância a falhas bizantinas em um protótipo funcional.

[1] A análise dos estudos foi feita no primeiro semestre de 2025

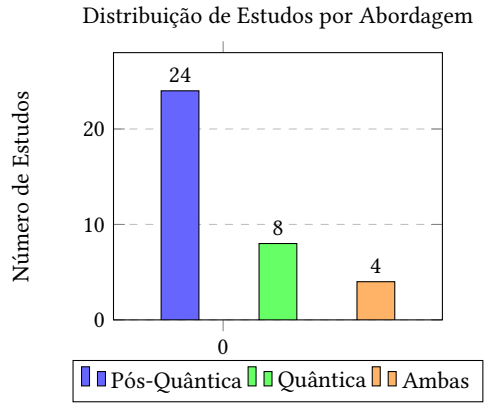

Figura 2: Distribuição dos estudos analisados.

5.2 Implementações Reprodutíveis e Validação Experimental

A análise identificou limitações na reprodutibilidade dos estudos avaliados, com apenas 11 dos 36 trabalhos (30,6%) fornecendo informações suficientes para replicação experimental, conforme mostrado em Figura 3. Os estudos [36] e [32] destacaram-se positivamente ao disponibilizarem implementações completas, o primeiro com *chaincodes* para Hyperledger Fabric incluindo *benchmarks* detalhados de desempenho (2,3 ms para Kyber e 8,7 ms para Dilithium em CPUs Xeon), e o segundo com circuitos quânticos no Qiskit alcançando 99% de fidelidade em simulações. Estes casos demonstraram como a adoção de *frameworks* padronizados (Hyperledger, Qiskit) e a disponibilização de artefatos técnicos completos podem aumentar significativamente o valor científico das pesquisas.

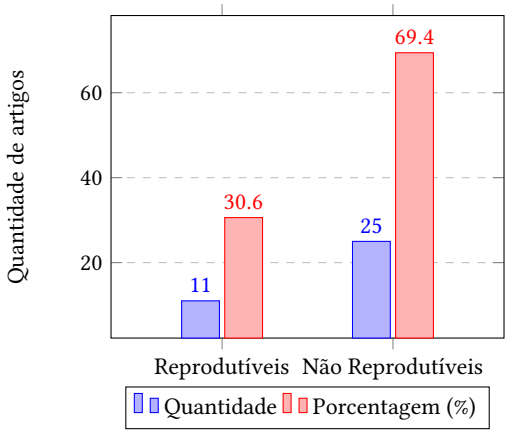

Figura 3: Reprodutibilidade dos estudos avaliados

Em contraste, os estudos [39] e [13], embora descrevessem metodologias experimentais aparentemente robustas (utilizando Kubernetes e NS-3 respectivamente), não disponibilizaram os *scripts*, parâmetros de configuração ou *datasets* completos, comprometendo sua reprodutibilidade. Outra situação foi observada em [34], que realizou experimentos pioneiros com QDS em fibra óptica, mas restringiu o acesso aos dados brutos mediante solicitação, limitando a capacidade de verificação independente. O estudo [24] exemplificou outro problema, as propostas teóricas ambiciosas (como árvores de Merkle quânticas) sem qualquer implementação ou simulação que permitisse avaliar sua viabilidade prática.

A análise revelou ainda uma lacuna na documentação dos ambientes experimentais. Enquanto o estudo [36] especificou detalhadamente a configuração de hardware (CPUs Xeon Gold 6248, 192GB RAM) e software (Hyperledger Fabric 2.3, Go 1.15), estudos como [29] e [33] limitaram-se a descrições genéricas como "ambiente simulado"ou "testes em condições reais", sem fornecer informações técnicas essenciais para reprodução. Esta falta de padronização na documentação experimental foi particularmente problemática nos estudos envolvendo componentes quânticos, como os estudos [17, 20], onde pequenas variações nos parâmetros físicos podem alterar completamente os resultados.

5.3 Desempenho e Viabilidade Prática

Na análise de desempenho e viabilidade técnica, houve trabalhos que contribuíram na implementação prática das tecnologias. O estudo [6] demonstrou avanços ao implementar zk-STARKs para autenticação quântica-resistente, alcançando tempos de geração de prova de 60ms, porém revelando uma exigência de 16GB de RAM que limita sua aplicação em dispositivos com restrições de recursos. Paralelamente, [13] realizou uma análise comparativa entre esquemas de assinatura pós-quânticos, identificando que *eXtended Merkle Signature Scheme* (XMSS) apresenta melhor desempenho em ambientes com restrição de energia, consumindo 23% menos que Dilithium em dispositivos IoT de baixo poder computacional.

A pesquisa [36] ofereceu contribuições ao avaliar o desempenho de algoritmos PQC em arquiteturas blockchain permissionadas, demonstrando que a implementação de CRYSTALS-Kyber em Hyperledger Fabric resulta em um *overhead* de processamento 2.8 vezes maior comparado a esquemas clássicos, porém com ganhos significativos em segurança. Complementarmente, [15] investigou a viabilidade de *Hardware Security Modules* (HSMs) para acelerar operações criptográficas pós-quânticas, obtendo redução de 40% no tempo de assinatura quando comparado a implementações puramente baseadas em software.

No domínio quântico, o trabalho [17] explorou protocolos de troca baseados em estados entrelaçados, simulando ambientes com até 50 nós quânticos e identificando um crescimento logarítmico no tempo de consenso conforme a rede se expande. Já [25] apresentou resultados experimentais com QKD em sistemas marítimos, alcançando taxas de transmissão segura de 1.45Mbps em condições reais de operação, embora com aumento de 35% na latência comparado a sistemas clássicos equivalentes.

Estudos como [39] e [38] abordaram especificamente o desafio da escalabilidade em redes blockchain pós-quânticas. [39] quantificou o impacto do tamanho aumentado de assinaturas na propagação de blocos, mostrando que esquemas baseados em reticulados podem aumentar em 60% o tempo de sincronização em redes com mais de 1,000 nós. Por sua vez, [38] desenvolveu um modelo de otimização para *N-th Degree Truncated Polynomial Ring Unit* (NTRU) em ambientes *multi-cloud*, reduzindo o *overhead* de comunicação em 28% através de técnicas de agregação de assinaturas.

A pesquisa [34] merece destaque por realizar a primeira implementação prática de um protocolo de consenso quântico tolerante a falhas bizantinas, demonstrando experimentalmente que QDS pode superar os limites clássicos de 1/3 de tolerância, alcançando 45% em configurações controladas com cinco nós quânticos. Contudo, o estudo também revelou desafios na sincronização temporal de operações quânticas distribuídas, com taxas de erro que aumentam exponencialmente conforme a distância entre nós.

5.4 Lacunas em Segurança e Interoperabilidade

A análise revelou vulnerabilidades e desafios de interoperabilidade em sistemas blockchain atuais e propostos. O estudo [7] identificou que as transações Bitcoin muitas vezes reutilizam endereços, tornando-as vulneráveis a ataques de Shor, enquanto a migração para esquemas como McEliece aumentaria o tamanho dos blocos, impactando significativamente a escalabilidade.

Na segurança pós-quântica, [21] demonstrou vulnerabilidades no esquema GGH a ataques de redução de base, reforçando a importância da adesão aos padrões NIST. Já o estudo [2], ao implementar *Secure Quantum Key Distribution* (SQKD) em redes de *smart grid*, encontrou taxas de erro de 8.3% em ambientes ruidosos, comprometendo a confiabilidade das comunicações quânticas.

A interoperabilidade foi abordada em [10], que desenvolveu um *framework* de tradução entre sistemas criptográficos com *overhead* de apenas 0.4ms por transação, embora necessite de testes em maior escala. O estudo [38] complementou esta abordagem com técnicas de agregação que reduziram em 28% o *overhead* em arquiteturas *multi-cloud*.

Por fim, a sincronização de nós quânticos distribuídos permanece um desafio, pois o estudo [34] demonstra que taxas de erro dobram a cada 50km de distância entre nós, limitando a aplicação prática de QDS em redes blockchain escaláveis.

5.5 Alinhamento com Padrões e Tendências

A revisão identificou variações na adoção de padrões estabelecidos entre os estudos analisados. Os trabalhos [15, 19, 36] emergiram como exemplos de melhor prática ao implementarem os algoritmos CRYSTALS-Dilithium e Falcon, recentemente padronizados pelo NIST, demonstrando compatibilidade completa com os requisitos de segurança pós-quântica de nível 2. Estes estudos forneceram métricas detalhadas sobre o desempenho das implementações, incluindo tamanhos de chave de 1.312 bytes e tempos de assinatura entre 2.3-8.7ms em hardware moderno.

Em contraste, o estudo [21] adotou o esquema GGH não padronizado, revelando vulnerabilidades a ataques de redução de base durante sua análise de segurança. Esta constatação reforça os riscos associados à implementação de algoritmos não certificados pelo NIST, mesmo quando apresentam propriedades teóricas interessantes. A pesquisa [6] complementou esta análise ao demonstrar que mesmo esquemas promissores como zk-STARKs exigem validação rigorosa contra padrões estabelecidos, especialmente quando aplicados em contextos de baixo poder computacional.

No domínio da comunicação quântica, o trabalho [2] destacou-se por implementar SQKD em conformidade com os protocolos ISO/IEC 23837, alcançando taxas de transmissão segura de 1.45Mbps. No entanto, como observado em [34], a falta de padrões consolidados para QDS em redes blockchain resulta em abordagens fragmentadas, com diferentes estudos adotando parâmetros operacionais incompatíveis entre si. Esta divergência foi particularmente evidente na comparação entre [24] e [20], que propuseram arquiteturas radicalmente diferentes para árvores de Merkle quânticas.

Por fim, a análise também revelou lacunas na adoção de *frameworks* de teste padronizados. Enquanto os estudos [36] e [15] utilizaram os *benchmarks* de desempenho definidos pelo NIST PQC, muitos estudos como [27] e [30] desenvolveram metodologias próprias de avaliação, dificultando comparações diretas entre as soluções propostas.

6 Conclusão

Esta *rapid review* identificou avanços e lacunas no desenvolvimento de blockchains resistentes a ameaças quânticas. Os resultados mostram que soluções pós-quânticas, como CRYSTALS-Dilithium e Falcon, já atingiram maturidade teórica e começam a ser aplicadas em sistemas práticos [15, 19, 36]. Em contraste, abordagens quânticas baseadas em emaranhamento e QDS [24, 34] ainda enfrentam barreiras tecnológicas para uso em larga escala. Observou-se ainda que apenas 30,6% dos estudos oferecem dados para reprodução experimental, evidenciando a necessidade de maior transparência metodológica e compartilhamento de artefatos.

Os trabalhos futuros devem priorizar três eixos: (i) desenvolvimento de *frameworks* de transição que suportem a migração gradual de blockchains existentes para sistemas pós-quânticos, considerando aspectos técnicos e incentivos econômicos [10, 38]; (ii) estabelecimento de *benchmarks* padronizados para desempenho quântico e pós-quântico, com métricas como *throughput* por qubit, eficiência energética e resiliência a ataques híbridos [9]; e (iii) avanços em experimentação com hardware quântico distribuído [34], visando superar limitações de sincronização e decoerência que restringem a escalabilidade.

Por fim, a implementação dessas direções deve seguir padrões emergentes do NIST e de outras entidades normativas. O equilíbrio entre rigor teórico e validação experimental será decisivo para acelerar a adoção de blockchains seguras na era quântica [15, 34, 36]. Recomenda-se, em especial, explorar arquiteturas híbridas que combinem a robustez da criptografia pós-quântica com os benefícios de longo prazo dos protocolos quânticos, enquanto a infraestrutura de hardware continua a evoluir [9].

Agradecimentos

Este trabalho foi parcialmente financiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), sob os auxílios 405940/2022-0, 400111/2023-3, 444978/2024-0, pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), por meio dos projetos 2023/00811-0, 2023/00673-7, 2021/00199-8 (CPE SMARTNESS), 2020/04031-1 e 2018/23097-3.

Referências

[1] B. Akoramurthy and B. Surendiran. 2024. QHealth: A Blockchain Based Smart Healthcare Consensus Method. In *2024 International Conference on Signal Processing, Computation, Electronics, Power and Telecommunication, IConSCEPT 2024 - Proceedings*. Institute of Electrical and Electronics Engineers Inc.

doi:10.1109/IConSCEPT61884.2024.10627831

[2] Abdullah Musaed Alkhiari, Shailendra Mishra, and Mohammed AlShehri. 2022. Blockchain-based SQKD and IDS in edge enabled smart grid network. *Computers, Materials and Continua* 70 (2022), 2149–2169. doi:10.32604/cmc.2022.019562

[3] Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M Schanck, Peter Schwabe, Gregor Seiler, Damien Stehlé, et al. 2019. CRYSTALS-Kyber algorithm specifications and supporting documentation. *NIST PQC Round* 2, 4 (2019), 1–43.

[4] Prithwi Bagchi, Basudeb Bera, Ashok Kumar Das, Sachin Shetty, Pandi Vijayakumar, and Marimuthu Karuppiah. 2023. Post Quantum Lattice-Based Secure Framework using Aggregate Signature for Ambient Intelligence Assisted Blockchain-Based IoT Applications. *IEEE Internet of Things Magazine* 6 (2023), 52–58. doi:10.1109/IOTM.001.2100215

[5] Daniel J Bernstein. 2025. Post-quantum cryptography. In *Encyclopedia of Cryptography, Security and Privacy*. Springer, 1846–1847.

[6] Usama Habib Chaudhry, Razi Arshad, Ayesha Khalid, Indranil Ghosh Ray, and Mehdi Hussain. 2025. zk-DASTARK: A quantum-resistant, data authentication and zero-knowledge proof scheme for protecting data feed to smart contracts. *Computers and Electrical Engineering* 123 (2025). doi:10.1016/j.compeleceng.2025.110089

[7] Sumit Chauhan, Vaghawan Prasad Ojha, Shantia Yarahmadian, and David Carvalho. 2023. Towards Building Quantum Resistant Blockchain. In *International Conference on Electrical, Computer and Energy Technologies, ICECET 2023*. Institute of Electrical and Electronics Engineers Inc. doi:10.1109/ICECET58911.2023.10389558

[8] Léo Ducas, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. 2018. Crystals–dilithium: Digital signatures from module lattices. (2018).

[9] Marcus Edwards, Atefeh Mashatan, and Shohini Ghose. 2020. A review of quantum and hybrid quantum/classical blockchain protocols. *Quantum Information Processing* 19, 6 (2020), 184.

[10] Marco Fiore, Federico Carrozzino, Marina Mongiello, Gaetano Volpe, and Agostino Marcello Mangini. 2023. A Blockchain-Based Modular Architecture for Managing Multiple and Quantum-Safe Encryption Algorithms. In *9th 2023 International Conference on Control, Decision and Information Technologies, CoDIT 2023*. Institute of Electrical and Electronics Engineers Inc., 598–601. doi:10.1109/CoDIT58514.2023.10284090

[11] Hadi Gharavi, Jorge Granjal, and Edmundo Monteiro. 2024. Post-Quantum Blockchain Security for the Internet of Things: Survey and Research Directions. *IEEE Communications Surveys Tutorials* 26, 3 (2024), 1748–1774. doi:10.1109/COMST.2024.3355222

[12] Daniel Gottesman and Isaac Chuang. 2001. Quantum digital signatures. *arXiv preprint quant-ph/0105032* (2001).

[13] Dev Gurung, Shiva Raj Pokhrel, and Gang Li. 2024. Performance analysis and evaluation of postquantum secure blockchained federated learning. *Computer Networks* 255 (2024). doi:10.1016/j.comnet.2024.110849

[14] Don Johnson, Alfred Menezes, and Scott Vanstone. 2001. The elliptic curve digital signature algorithm (ECDSA). *International journal of information security* 1, 1 (2001), 36–63.

[15] Sohel Ahmed Joni, Rabiul Rahat, Nishat Tasnin, Partho Ghose, and Md. Mahbub-Or-Rashid. 2024. Grainbee: A Quantum-Resistant Blockchain-Based Ration Distribution System with Hardware Security Modules. In *2024 IEEE Conference on Computing Applications and Systems, COMPAS 2024*. Institute of Electrical and Electronics Engineers Inc. doi:10.1109/COMPAS60761.2024.10796594

[16] Stephen P Jordan and Yi-Kai Liu. 2018. Quantum cryptanalysis: shor, grover, and beyond. *IEEE Security & Privacy* 16, 5 (2018), 14–21.

[17] Shashank Joshi, Arhan Choudhury, and R.I. Minu. 2023. Quantum blockchain-enabled exchange protocol model for decentralized systems. *Quantum Information Processing* 22 (2023). doi:10.1007/s11128-023-04156-1

[18] Hassan Khodaiemehr, Khadijeh Bagheri, and Chen Feng. 2023. Navigating the quantum computing threat landscape for blockchains: A comprehensive survey. *Authorea Preprints* (2023).

[19] Hyunjun Kim, Wonwoong Kim, Yeajun Kang, Hyunji Kim, and Hwajeong Seo. 2024. Post-Quantum Delegated Proof of Luck for Blockchain Consensus Algorithm. *Applied Sciences (Switzerland)* 14 (2024). doi:10.3390/app14188394

[20] Mandeep Kumar and Bhaskar Mondal. 2024. Quantum blockchain architecture using cyclic QSCD and QKD. *Quantum Information Processing* 23 (2024). doi:10.1007/s11128-024-04316-x

[21] Sonitema Laia and Ari Moesriami Barmawi. 2024. Strengthening the Authentication Mechanism of Blockchain-Based E-Voting System Using Post-Quantum Cryptography. *Jurnal Online Informatika* 9 (2024), 159–168. doi:10.15575/join.v9i2.1305

[22] Evgeny Milanov. 2009. The RSA algorithm. *RSA laboratories* 1, 11 (2009).

[23] MITRE STEM. 2025. The Bloch Sphere. https://stem.mitre.org/quantum/quantum-concepts/bloch-sphere.html. Acessado em: 8 de agosto. 2025.

[24] V.S. Moskvin. 2024. Quantum Blockchain Architecture for Transportation Services. In *2024 Intelligent Technologies and Electronic Devices in Vehicle and Road Transport Complex, TIRVED 2024 - Conference Proceedings*. Institute of Electrical and Electronics Engineers Inc. doi:10.1109/TIRVED63561.2024.10769810

[25] Eduart Ndokaj, Luca La Gatta, Osman Metalla, and Shpetim Pupa. 2024. Quantum-Enhanced Blockchain for Maritime Cybersecurity: Leveraging Advanced Random Number Generation to Secure Maritime Operations. In *2024 International Workshop on Quantum and Biomedical Applications, Technologies, and Sensors, Q-BATS 2024*. Institute of Electrical and Electronics Engineers Inc., 88–92. doi:10.1109/Q-BATS63267.2024.10873866

[26] NIST. 2025. National Institute of Standards and Technology (NIST). Cybersecurity. https://www.nist.gov/cybersecurity Acessado em: 7 de Agosto. 2025.

[27] Mritunjay Shall Peelam and Vinay Chamola. 2024. Enhancing Security Using Quantum Blockchain in Consumer IoT Networks. *IEEE Transactions on Consumer Electronics* (2024). doi:10.1109/TCE.2024.3512791

[28] Roman Rietsche, Christian Dremel, Samuel Bosch, Léa Steinacker, Miriam Meckel, and Jan-Marco Leimeister. 2022. Quantum computing. *Electronic Markets* 32, 4 (2022), 2525–2536.

[29] Lucy Sharma and Arun Mishra. 2021. Analysis of Crystals-Dilithium for Block-Chain Security. In *ICSCCC 2021 - International Conference on Secure Cyber Computing and Communications*. Institute of Electrical and Electronics Engineers Inc., 160–165. doi:10.1109/ICSCCC51823.2021.9478087

[30] Mahendra Kumar Shrivas, Srujan Kachhwaha, Ashok Bhansali, and Satya Vir Singh. 2022. Quantum-resistant University Credentials Verification System on Blockchain. In *Proceedings of the 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development, NIGERCON 2022*. Institute of Electrical and Electronics Engineers Inc. doi:10.1109/NIGERCON54645.2022.9803153

[31] Deepraj Soni, Kanad Basu, Mohammed Nabeel, Najwa Aaraj, Marcos Manzano, and Ramesh Karri. 2020. Falcon. In *Hardware Architectures for Post-Quantum Digital Signature Schemes*. Springer, 31–41.

[32] Alexandru-Gabriel Tudorache. 2022. Design of an Exchange Protocol for the Quantum Blockchain. *Mathematics* 10 (2022). doi:10.3390/math10213986

[33] Ranjitha Venkatesh and Smita Darandale. 2024. Enhancing Healthcare Security with Quantum Blockchain: Electronic Medical Records Protection. In *2nd IEEE International Conference on Networks, Multimedia and Information Technology, NMITCON 2024*. Institute of Electrical and Electronics Engineers Inc. doi:10.1109/NMITCON62075.2024.10699120

[34] Chen-Xun Weng, Rui-Qi Gao, Yu Bao, Bing-Hong Li, Wen-Bo Liu, Yuan-Mei Xie, Yu-Shuo Lu, Hua-Lei Yin, and Zeng-Bing Chen. 2023. Beating the Fault-Tolerance Bound and Security Loopholes for Byzantine Agreement with a Quantum Solution. *Research* 6 (2023). doi:10.34133/research.0272

[35] Ramona Wolf. 2021. *Quantum key distribution*. Vol. 988. Springer.

[36] Shiwei Xu, Ao Sun, Xiaowen Cai, Zhengwei Ren, Yizhi Zhao, and Jianying Zhou. 2021. Post-Quantum User Authentication and Key Exchange Based on Consortium Blockchain. In *Proceedings of the International Conference on Parallel and Distributed Systems - ICPADS*, Vol. 2021-December. IEEE Computer Society, 667–674. doi:10.1109/ICPADS53394.2021.00089

[37] Zebo Yang, Haneen Alfauri, Behrooz Farkiani, Raj Jain, Roberto Di Pietro, and Aiman Erbad. 2023. A survey and comparison of post-quantum and quantum blockchains. *IEEE Communications Surveys & Tutorials* 26, 2 (2023), 967–1002.

[38] Engin Zeydan, Jorge Baranda, and Josep Mangues-Bafalluy. 2022. Post-Quantum Blockchain-Based Secure Service Orchestration in Multi-Cloud Networks. *IEEE Access* 10 (2022), 129520–129530. doi:10.1109/ACCESS.2022.3228823

[39] Engin Zeydan, Luis Blanco, Josep Mangues-Bafalluy, Suayb S. Arslan, and Yekta Turk. 2024. Post-Quantum Blockchain-Based Decentralized Identity Management for Resource Sharing in Open Radio Access Networks. *IEEE Transactions on Green Communications and Networking* 8 (2024), 895–909. doi:10.1109/TGCN.2024.3432689