Impactos da Criptografia Pós-Quântica em Redes Blockchain: Implementação e Avaliação na Hyperledger Besu

Rodrigo Duarte de Meneses *r197962@dac.unicamp.br*
Felipe José Aguiar Rampazzo *f233261@dac.unicamp.br*
Marco Amaral Henriques *maah@dac.unicamp.br*

Departamento de Engenharia de Computação e Automação (DCA)
Faculdade de Engenharia Elétrica e de Computação (FEEC)
Universidade Estadual de Campinas (UNICAMP)

Resumo

Com a iminente ameaça dos computadores quânticos à segurança dos sistemas criptográficos atuais, torna-se essencial avaliar soluções pós-quânticas para sistemas em operação. Este trabalho apresenta a integração de algoritmos de criptografia pós-quântica (PQC) na plataforma Hyperledger Besu, com o objetivo de avaliar o impacto de assinaturas digitais resistentes a ataques quânticos em blockchains permissionadas baseadas no protocolo Ethereum. A proposta consiste na criação de uma arquitetura híbrida que mantém a compatibilidade com o ECDSA (secp256k1) enquanto incorpora esquemas PQC, como ML-DSA, SLH-DSA e MAYO. Os resultados indicam que a adição de criptografia pós-quântica aumenta o tamanho dos blocos e o custo computacional, mas oferece maior robustez criptográfica e permite o futuro uso de algoritmos PQC em redes blockchain permissionadas. Essa integração contribui para a transição gradual rumo à segurança pós-quântica em sistemas distribuídos.

Palavras-Chave — criptografia pós-quântica, assinaturas digitais, blockchain, hyperledger besu.

1. Introdução

Com a ameaça do surgimento de um computador quântico criptograficamente relevante, é esperado que em breve os criptossistemas utilizados atualmente, baseados em fatoração de inteiros e logaritmos discretos (como RSA e ECC), se tornem obsoletos [1]. A criptografia pós-quântica (PQC) é o ramo da criptografia que busca desenvolver algoritmos seguros frente à capacidade de computação dos computadores quânticos. Em 2024, o NIST padronizou os primeiros algoritmos pós-quânticos, incluindo os esquemas de assinatura baseados em reticulados (ML-DSA, FIPS 204 [2]) e em funções de hash (SLH-DSA, FIPS 205 [3]), além de selecionar o Falcon para futura padronização [4].

Neste contexto, nota-se que redes blockchain dependem fortemente de assinaturas digitais (como as de Bitcoin e Ethereum); portanto, são especialmente suscetíveis a ataques do tipo "harvest now, decrypt later" – em que um adversário armazena comunicações criptografadas hoje, com a intenção de decriptá-las futuramente quando computadores quânticos forem capazes de quebrar os algoritmos atuais [5]. Assim, torna-se essencial preparar sua infraestrutura para uma transição segura e gradual rumo a algoritmos pós-quânticos, garantindo a longevidade da segurança do sistema.

Neste trabalho apresentamos os impactos da integração de múltiplos algoritmos pós-quânticos de assinatura digital na Hyperledger Besu, um cliente Ethereum amplamente utilizado para ambientes corporativos e experimentais (e.g., piloto do DREX, o Real Digital [6]). O objetivo principal é permitir que transações e blocos sejam assinados de forma híbrida, utilizando tanto algoritmos tradicionais (ECDSA) quanto pós-quânticos, preservando a compatibilidade com a infraestrutura atual e oferecendo proteção adicional em caso de falha ou ataque bem-sucedido a um dos algoritmos. Nessa abordagem, as assinaturas ECDSA continuam válidas segundo o protocolo original, enquanto as assinaturas PQC adicionam uma camada complementar de segurança frente à ameaça quântica.

2. Métodos

Durante o desenvolvimento, foram incorporados quatro algoritmos pós-quânticos de assinatura digital: ML-DSA-44 (variante do esquema CRYSTALS-Dilithium), SLH-DSA-128s (baseado em funções de hash criptográfico) e MAYO-1 (esquema do tipo "Oil and Vinegar" ainda em estudos pelo NIST para eventual padronização futura). Cada esquema apresenta características específicas quanto a tamanho de chaves e assinaturas, bem como tempos de geração, assinatura e verificação, permitindo uma análise comparativa de desempenho e segurança. A Tabela 1 apre-

senta uma comparação entre os diferentes algoritmos pós-quânticos escolhidos e o ECDSA utilizado nativamente na Besu.

Tabela 1: Tamanhos de chave pública (pk), chave privada (sk) e assinatura (σ) dos algoritmos pós-quânticos ML-DSA, SLH-DSA e MAYO; além do algoritmo tradicional ECDSA (secp256k1).

Algoritmo	Nível	pk (B)	sk (B)	σ (B)
ECDSA (secp256k1)	1	32	32	64
ML-DSA-44	1	1 312	2 560	2 420
ML-DSA-65	3	1 952	4 032	3 309
ML-DSA-87	5	2 592	4 896	4 627
SLH-DSA-128s	1	32	64	7 856
SLH-DSA-192s	3	48	96	16 224
SLH-DSA-256s	5	64	128	29 792
MAYO-1	1	1 420	24	454
MAYO-3	3	2 986	32	681
MAYO-5	5	5 554	40	964

A arquitetura proposta introduz assinaturas pós-quânticas na estrutura de dados da Besu sem alterar os campos fundamentais exigidos pelo protocolo. Em vez de substituir diretamente o mecanismo de assinatura, adotou-se uma abordagem de assinaturas híbridas: cada bloco ou transação é assinado tanto pelo esquema clássico (ECDSA/secp256k1) quanto por um algoritmo PQC adicional. Assim, a rede continua reconhecendo e validando as assinaturas ECDSA como de costume, garantindo compatibilidade, enquanto os dados da assinatura pós-quântica trafegam em campos estendidos, servindo como camada extra de segurança e evidência criptográfica.

Para avaliar o impacto de PQC na validação dos blocos, utilizamos o mecanismo de consenso Clique PoA, explorando o campo `ExtraData` do cabeçalho de bloco para acomodar as novas informações. Este campo normalmente contém 32 bytes de "vanity", uma lista de endereços dos validadores, e 65 bytes da assinatura ECDSA do propositor do bloco [7]. Estendemos esse campo para incluir também a chave pública e a assinatura PQC do validador. Cada bloco, portanto, passou a carregar duas assinaturas: a padrão ECDSA (usada pelo protocolo para verificar o autor do bloco) e uma assinatura pós-quântica gerada com a chave PQC do mesmo validador. A Figura 1 ilustra o novo formato do campo.

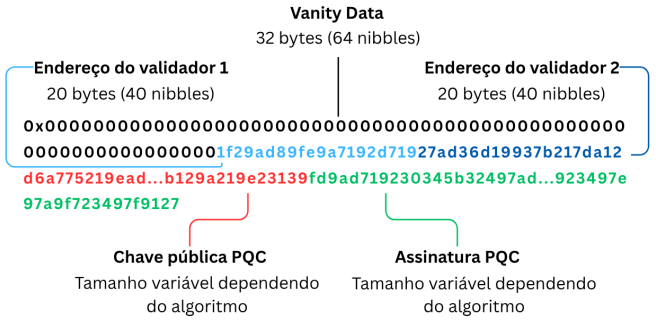

Figura 1: Estrutura do campo ExtraData modificado no consenso Clique PoA após a integração da criptografia pós-quântica (PQC).

No caso das transações, foi adotada uma estratégia semelhante. A Besu não possui um campo nativo para múltiplas assinaturas no formato de transação padrão; portanto, utilizamos o campo `data` da transação para embutir as informações necessárias para as assinaturas pós-quânticas. Em nosso design, transações podem carregar um "payload PQC" no campo `data` (que normalmente é usado para dados de chamada de contrato ou mensagens arbitrárias). Esse pacote inclui a chave pública pós-quântica do remetente e sua assinatura PQC referente àquela transação. Diferentemente do ECDSA, os algoritmos PQC de assinatura não possuem um mecanismo nativo para derivação da chave pública a partir da assinatura [8]. Por esse motivo, além da assinatura também é necessário enviar a chave pública como parte do payload PQC.

3. Impactos da Pesquisa

Dentro do melhor do nosso conhecimento, esta é a primeira implementação que integra assinaturas PQC diretamente na base de código da Hyperledger Besu. Enquanto pesquisas anteriores apenas estimam e discutem teoricamente o impacto de PQC nesta plataforma [9], nossa solução materializa esses conceitos com uma rede Besu funcional. Essa prova de conceito demonstra na prática os impactos da introdução de algoritmos criptográficos pós-quânticos diretamente na plataforma.

Além disso, ao suportar e testar quatro diferentes algoritmos PQC em um cliente blockchain real, o projeto obteve uma comparação para esses algoritmos com restrições práticas de recursos computacionais (incluindo custos de gas, etc.). Outros benchmarks de PQC são feitos isoladamente, sem permitir insights mais concretos sobre os impactos da sua ado-

ção. Por exemplo, confirmamos empiricamente o impacto de assinaturas grandes no uso de gas, atestando a praticidade de algoritmos como o ML-DSA e MAYO, enquanto que o SLH-DSA pode ser oneroso, de acordo com as previsões teóricas. O ambiente de testes desenvolvido pode ser reutilizado para testar futuros candidatos e acelerar a pesquisa aplicada.

Por fim, este trabalho também contribui com a criptoaglidade ao mostrar que a infraestrutura da Besu pode ser adaptada para diferentes algoritmos sem a necessidade mudanças estruturais significativas. Tradicionalmente, blockchains não foram desenvolvidas considerando a troca de algoritmos criptográficos (um hard fork é necessário [10]). Apresentamos um caminho para preparar clientes Ethereum com múltiplos algoritmos pós-quânticos, o que pode no futuro permitir a negociação de algoritmos de assinatura a cada transação ou bloco.

4. Resultados e Discussão

Os resultados evidenciam uma relação linear entre o consumo de gás por bloco e o número de transações incluídas, já que cada transação adiciona um custo fixo proporcional às dimensões das assinaturas e chaves do algoritmo empregado (Figura 2). O ECDSA (Baseline) apresenta o menor consumo por transação, de aproximadamente 21.000 unidades de gás, permitindo atingir 1.510 transações por bloco dentro do limite máximo de 32 milhões de gás.

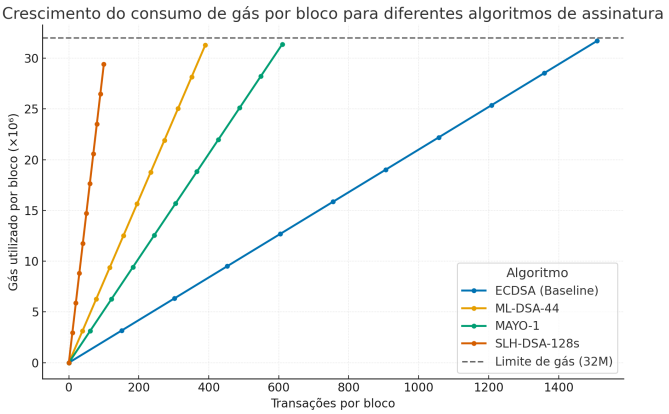

Figura 2: Crescimento do consumo de gás por bloco em função do número de transações para diferentes algoritmos de assinatura.

Em contrapartida, os algoritmos pós-quânticos exibem custos significativamente superiores, o que reduz a capacidade do bloco (Tabela 2). O ML-DSA-44, por exemplo, consome cerca de 80.248 gás por transação, limitando-se a 396 transações por bloco; o MAYO-1 apresenta um consumo intermediário de 51.440 gás, alcançando 617 transações; e o SLH-DSA-128s, com 294.048 gás por transação, consegue apenas 108 transações por bloco. Observa-se que a substituição do ECDSA por esquemas de assinatura pós-quânticos reduz a escalabilidade da rede, pois o tamanho das chaves públicas e assinaturas aumenta o custo computacional e o tamanho das transações. Essa diferença é especialmente marcante para algoritmos baseados em funções hash, como o SLH-DSA, cujo overhead é o mais elevado.

Tabela 2: Comparação de consumo de gás e capacidade de transações por bloco entre algoritmos pós-quânticos e ECDSA.

Algoritmo	**gás/tx**	**tx/bloco**	**Redução (%)**
ECDSA (secp256k1)	21 000	1 510	—
ML-DSA-44	80 248	396	74%
MAYO-1	51 440	617	59%
SLH-DSA-128s	294 048	108	93%

Em termos práticos, o ML-DSA-44 e o MAYO-1 se mostram alternativas viáveis, com reduções de aproximadamente 74% e 59% na taxa de transações por bloco em relação ao ECDSA, mas ainda dentro de margens aceitáveis para redes permissionadas ou privadas. Já o SLH-DSA-128s é inviável para aplicações de alto throughput devido ao consumo extremo de gás.

Portanto, é possível concluir que o uso de algoritmos pós-quânticos em blockchains Hyperledger Besu requer ajustes na política de gasLimit, no tamanho de bloco e na frequência de transações, de modo a equilibrar segurança quântica e desempenho. Nesse contexto, o MAYO-1 e o ML-DSA-44 apresentam o melhor compromisso entre eficiência e segurança dentre os algoritmos analisados.

5. Conclusão

Foi apresentado um estudo sobre a integração de algoritmos pós-quânticos de assinatura digital em blockchains permissionadas usando o cliente Hyperledger Besu. Como contribuição prática, implementou-se um protótipo que suporta assinaturas híbridas em transações e blocos, utilizando os algoritmos ML-DSA, SLH-DSA e MAYO.

Os resultados demonstram a viabilidade técnica dessa integração: é possível oferecer segurança pós-

quântica sem sacrificar o funcionamento da rede, ainda que com alguns custos adicionais de desempenho. Verificou-se que os algoritmos pós-quânticos mais eficientes (ML-DSA, MAYO) introduzem overheads moderados, enquanto algoritmos menos eficientes (SLH-DSA) apresentam obstáculos significativos de performance.

De modo geral, as assinaturas híbridas se mostram uma solução transitória robusta: aumentam a segurança da rede contra ataques quânticos, ao mesmo tempo em que permitem uma adoção incremental, mantendo compatibilidade com as operações fundamentais dos sistemas legados.

Agradecimentos

Os autores agradecem às instituições de pesquisa e agências de fomento que apoiaram este trabalho. Em particular, expressamos nossa gratidão à Rede Nacional de Ensino e Pesquisa (RNP) pelo suporte institucional, e ao Ministério da Ciência, Tecnologia e Inovação (MCTI) pelo financiamento concedido (Projeto "Ilíada"). Agradecemos também aos colegas do grupo ReGrAS (Research Group on Applied Security) pelas discussões técnicas e colaboração no desenvolvimento deste trabalho.

Referências

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997, originally appeared as a preliminary version in the Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, Nov. 20–22, 1994. [Online]. Available: https://arxiv.org/pdf/quant-ph/9508027.pdf

[2] N. I. of Standards and Technology, "Fips 204: Module-lattice-based digital signature standard," NIST, Tech. Rep. FIPS 204, Aug. 2024. [Online]. Available: https://csrc.nist.gov/pubs/fips/204/final

[3] ——, "Fips 205: Stateless hash-based digital signature standard," NIST, Tech. Rep. FIPS 205, Aug. 2024. [Online]. Available: https://csrc.nist.gov/pubs/fips/205/final

[4] ——, "Pqc standardization process: Announcing four candidates to be standardized, plus fourth round candidates," https://csrc.nist.gov/news/2022/pqc-candidates-to-be-standardized-and-round-4, Jul. 2022, news item, *Computer Security Resource Center*.

[5] M. Mosca, "Cybersecurity in an era with quantum computers: The "harvest now, decrypt later" threat," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 68–71, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8438604

[6] B. C. do Brasil, "Piloto drex – fase de testes para operações com a moeda digital brasileira," Banco Central do Brasil, Tech. Rep., Mar. 2023. [Online]. Available: https://www.bcb.gov.br/estabilidadefinanceira/piloto-drex

[7] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, no. 2014, pp. 1–32, 2014. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf

[8] D. Marchsreiter, "Towards quantum-safe blockchain: Exploration of pqc and public-key recovery on embedded systems," IACR Cryptology ePrint Archive, Tech. Rep. 2024/1178, 2024, preprint. [Online]. Available: https://eprint.iacr.org/2024/1178

[9] D. de Haro Moraes, J. P. A. Pereira, B. E. Grossi, G. Mirapalheta, G. M. M. A. Smetana, W. Rodrigues, C. N. G. Jr., B. Domingues, F. Saito, and M. Simplício, "Applying post-quantum cryptography algorithms to a dlt-based cbdc infrastructure: Comparative and feasibility analysis," IACR Cryptology ePrint Archive, Tech. Rep. 2024/1206, 2024, preprint. [Online]. Available: https://eprint.iacr.org/2024/1206

[10] B. T. Corp., "Ethereum's roadmap for post-quantum cryptography," https://www.btq.com/blog/ethereums-roadmap-post-quantum-cryptography, Oct. 2024, blog post, accessed 2025-11-08.