Uma Arquitetura Não-Invasiva para Adoção de Criptografia Pós-Quântica em Blockchains Permissionadas

Everaldo Alves[1], Leandro Tadeu[1], Marcelo Pimentel[1], Bruno Evaristo[1]

[1]Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPQD)
Campinas – SP – Brazil

marcelorebellopimentel,leandro.tadeu.dcl,everaldoalves}@gmail.com

elderb@cpqd.com.br

Abstract. *The threat of quantum computing poses significant challenges to the security of distributed systems based on public-key cryptography, requiring the adoption of quantum-resistant primitives. In permissioned blockchains, this transition is hindered by the tight coupling between cryptographic mechanisms and system architecture, as well as compatibility requirements. This work proposes a non-invasive architecture for the adoption of post-quantum cryptography in Hyperledger Besu, based on the principle of cryptographic agility. The approach introduces post-quantum primitives incrementally at two levels: (i) the communication layer, by encapsulating RLPx within TLS 1.3 tunnels supporting post-quantum key exchange algorithms; and (ii) the block validation layer, using hybrid digital signatures integrated via JNI with the liboqs library. Experimental results demonstrate the feasibility of the approach in a real environment, highlighting performance impacts and associated trade-offs, particularly due to increased key and signature sizes. The results indicate that the proposed approach enables a secure and incremental transition to post-quantum cryptography in permissioned blockchains.*

Resumo. *A ameaça da computação quântica impõe desafios à segurança de sistemas distribuídos baseados em criptografia de chave pública, exigindo a adoção de primitivas resistentes. Em blockchains permissionadas, essa transição é dificultada pelo forte acoplamento entre criptografia e arquitetura, além de requisitos de compatibilidade. Este trabalho propõe uma arquitetura não-invasiva para adoção de criptografia pós-quântica no Hyperledger Besu, baseada em agilidade criptográfica. A abordagem introduz primitivas pós-quânticas de forma incremental em dois níveis: (i) no plano de comunicação, por meio do encapsulamento do RLPx em túneis TLS 1.3 com suporte a algoritmos pós-quânticos; e (ii) no plano de validação de blocos, utilizando assinaturas híbridas integradas via JNI com a biblioteca liboqs. Os resultados demonstram a viabilidade da proposta em ambiente real, evidenciando impactos em desempenho e trade-offs associados, especialmente no aumento do tamanho de chaves e assinaturas. Conclui-se que a abordagem permite uma transição incremental e segura para criptografia pós-quântica em blockchains permissionadas.*

1. Introdução

A segurança da criptografia assimétrica contemporânea baseia-se, em grande medida, na dificuldade computacional de problemas matemáticos clássicos, como a fatoração de inteiros e o cálculo do logaritmo discreto, considerados intratáveis em arquiteturas convencionais. No entanto, o advento da computação quântica modifica substancialmente esse cenário. O algoritmo de Shor demonstra que tais problemas podem ser resolvidos em tempo polinomial em computadores quânticos suficientemente escaláveis, comprometendo os fundamentos de segurança de esquemas amplamente utilizados na Internet e em sistemas distribuídos. Esse risco torna-se particularmente crítico em ecossistemas blockchain, nos quais propriedades como autenticidade, integridade e não repúdio dependem diretamente de primitivas criptográficas de chave pública [Ghosh 2025].

No contexto de blockchains permissionadas, como o Hyperledger Besu, a criptografia não desempenha um papel periférico, mas constitui um elemento transversal à arquitetura do sistema. No plano de comunicação entre pares, o protocolo RLPx estabelece canais autenticados e cifrados, empregando criptografia de curvas elípticas e mecanismos de acordo de chaves baseados em ECDH durante o processo de handshake. No plano transacional, a plataforma utiliza assinaturas digitais fundamentadas em curvas elípticas — tipicamente sobre a curva `secp256k1`, conforme o ecossistema Ethereum. Já no plano de consenso, especialmente em redes que adotam o protocolo QBFT, nós validadores são responsáveis por autenticar e assinar blocos antes de sua aceitação, fazendo com que a confiança sistêmica dependa diretamente da robustez das primitivas criptográficas subjacentes [Hyperledger Foundation 2024].

Diante desse contexto, uma abordagem imediata seria a substituição direta dos algoritmos clássicos por alternativas pós-quânticas. Contudo, em sistemas consolidados e em produção, essa estratégia tende a negligenciar custos relevantes de engenharia, tais como impacto no desempenho, aumento significativo no tamanho de chaves e assinaturas, desafios de compatibilidade retroativa e maior complexidade de manutenção. Paralelamente, o NIST consolidou, em agosto de 2024, os primeiros padrões finais de criptografia pós-quântica — FIPS 203, FIPS 204 e FIPS 205, passando a recomendar explicitamente o início de processos de transição em sistemas reais. Mais do que uma simples substituição de algoritmos, diretrizes técnicas do próprio NIST[1] enfatizam a necessidade de *agilidade criptográfica*, entendida como a capacidade de sistemas suportarem múltiplas primitivas e realizarem sua substituição de forma controlada ao longo do tempo [NIST 2023a].

Nesse cenário, abordagens híbridas, que combinam algoritmos clássicos e pós-quânticos, emergem como uma alternativa pragmática para mitigar riscos durante a transição, preservando a compatibilidade com sistemas existentes ao mesmo tempo em que introduzem resiliência frente a adversários quânticos. No contexto do Hyperledger Besu, essa estratégia mostra-se particularmente adequada: ao evitar modificações profundas no núcleo do cliente e ao explorar pontos de extensão bem definidos, torna-se possível incorporar mecanismos pós-quânticos de forma incremental, mensurável e reversível.

Este artigo está organizado da seguinte forma. A Seção 2 apresenta a motivação e o problema de pesquisa. A Seção 3 discute os trabalhos relacionados. A Seção 4 descreve

[1]NIST IR 8413: *Migration to Post-Quantum Cryptography*. NIST, 2023. Disponível em: `https://doi.org/10.6028/NIST.IR.8413`

a arquitetura proposta e os mecanismos de integração de criptografia pós-quântica, além de detalhar o ambiente,a metodologia experimental adotados. A Seção 5 apresenta e analisa os resultados obtidos. Por fim, a Seção 7 apresenta as conclusões e direções para trabalhos futuros.

2. Motivação e Problema

Embora o Hyperledger Besu apresente uma arquitetura modular, componentes críticos associados à criptografia permanecem fortemente acoplados às premissas do protocolo Ethereum. O transporte entre pares, baseado no protocolo RLPx, depende da pilha devp2p e de mecanismos criptográficos específicos, como o acordo de chaves via ECDH. No plano transacional, o formato e a validação de assinaturas seguem o padrão do ecossistema, centrado na curva `secp256k1`. Já no plano de consenso, especialmente em redes QBFT, validadores autorizados devem assinar blocos para que estes sejam aceitos por supermaioria. Como consequência, alterações nesses pontos extrapolam uma simples substituição de bibliotecas criptográficas, impactando diretamente o comportamento funcional do cliente.

Intervenções profundas nesses componentes introduzem riscos técnicos relevantes. Primeiramente, aumentam a probabilidade de regressões em módulos sensíveis [Mens and Demeyer 2008]. Além disso, podem comprometer a compatibilidade com ferramentas, clientes e fluxos já aderentes ao padrão Ethereum/Besu [Buterin 2015, Hyperledger Foundation 2024]. Por fim, ampliam significativamente o custo de manutenção evolutiva em uma base de código ativa [Lehman 1980]. Em ambientes corporativos e institucionais, nos quais estabilidade, auditabilidade e previsibilidade operacional são requisitos essenciais, tais fatores tornam abordagens altamente intrusivas pouco atrativas, especialmente em processos de transição criptográfica [NIST 2023b].

Diante desse cenário, este trabalho investiga a seguinte questão: *é possível introduzir mecanismos de criptografia pós-quântica em uma blockchain permissionada baseada em Hyperledger Besu sem modificações profundas em seu núcleo?* A hipótese adotada é que sim, desde que a inserção de novas primitivas seja orientada pelo princípio da agilidade criptográfica e concentrada em pontos arquiteturais de menor acoplamento. Essa estratégia permite preservar a compatibilidade funcional do cliente, reduzir riscos de integração e viabilizar a avaliação experimental de algoritmos pós-quânticos em um ambiente realista.

3. Trabalhos Relacionados

A literatura recente sobre resiliência pós-quântica em blockchains concentra-se majoritariamente na substituição de assinaturas no ecossistema Ethereum ou na avaliação de primitivas PQC por meio de benchmarks e simulações, frequentemente dissociadas de clientes reais em operação. Trabalhos como o de Asanso [Asanso 2024] exploram a adoção de assinaturas pós-quânticas por meio de mecanismos como *Account Abstraction* e novos formatos de transação, mas evidenciam limitações práticas relacionadas a custos computacionais, restrições da EVM e impactos na compatibilidade do ecossistema. De forma semelhante, discussões recentes na comunidade Ethereum [Community 2024] apontam desafios significativos para a integração de assinaturas pós-quânticas no protocolo base sem alterações estruturais profundas.

Por outro lado, estudos como o de Zorzo et al. [Zorzo 2023] apresentam metodologias robustas para avaliação de desempenho de algoritmos pós-quânticos, comparando esquemas como ML-DSA e Falcon sob diferentes métricas computacionais. No entanto, tais abordagens, em geral, não consideram os efeitos sistêmicos decorrentes da integração desses algoritmos em ambientes distribuídos reais, como redes blockchain em operação.

Revisões mais amplas indicam que muitas propostas ainda permanecem em nível conceitual ou dependem de infraestruturas emergentes, como *Quantum Key Distribution (QKD)* em larga escala [Allende 2023, Reddy 2025].

Nesse contexto, este trabalho diferencia-se ao priorizar uma abordagem pragmática baseada em intervenção mínima, combinando a introdução de mecanismos de encapsulamento de chaves pós-quânticos no canal de comunicação entre nós e o uso de uma camada JNI para integração da biblioteca *liboqs* no processo de assinatura e verificação. Ao preservar a lógica original do cliente e atuar em pontos de menor acoplamento, a proposta permite avaliar impactos operacionais reais em um cliente Besu, contribuindo para a análise da viabilidade de adoção incremental de primitivas pós-quânticas.

4. Proposta Arquitetural

A estratégia adotada neste trabalho baseia-se no princípio de agilidade criptográfica, buscando introduzir mecanismos pós-quânticos com impacto mínimo na base de código do Hyperledger Besu. Em vez de modificar diretamente componentes internos críticos — como o protocolo RLPx ou o mecanismo de consenso — a abordagem proposta concentra-se na inserção de uma camada externa de proteção criptográfica.

Especificamente, a troca de chaves entre nós é realizada por meio do encapsulamento do tráfego RLPx em um túnel TLS 1.3 configurado com suporte a algoritmos pós-quânticos. Nesse modelo, o protocolo RLPx permanece completamente inalterado e continua operando sobre um canal lógico seguro, enquanto a negociação de chaves e a proteção criptográfica do transporte passam a ser realizadas pelo TLS. A camada TLS é configurada para utilizar mecanismos de encapsulamento de chaves pós-quânticos, possibilitando o estabelecimento de segredos compartilhados resistentes a adversários quânticos.

Ao deslocar a complexidade criptográfica para fora do núcleo do cliente Besu, a solução preserva compatibilidade com a pilha existente, reduz riscos de regressão e facilita a experimentação controlada de diferentes primitivas.

Do ponto de vista arquitetural, a intervenção ocorre exclusivamente na camada de transporte, abaixo do protocolo RLPx, conforme ilustrado na Figura 1. Dessa forma, o cliente Besu permanece funcionalmente inalterado, enquanto o canal de comunicação passa a usufruir de proteção pós-quântica. Essa separação de responsabilidades reforça o caráter não intrusivo da proposta e evidencia sua aderência ao princípio de agilidade criptográfica.

No plano de autenticação e integridade dos blocos, a proposta segue o mesmo princípio de mínima intrusão, concentrando a introdução de mecanismos pós-quânticos no módulo de validação de blocos (*Block Validator*), sem alterações no mecanismo de consenso. Conforme ilustrado na Figura 2, o fluxo original baseado no algoritmo ECDSA é preservado integralmente, sendo estendido por meio da inclusão de uma assinatura pós-

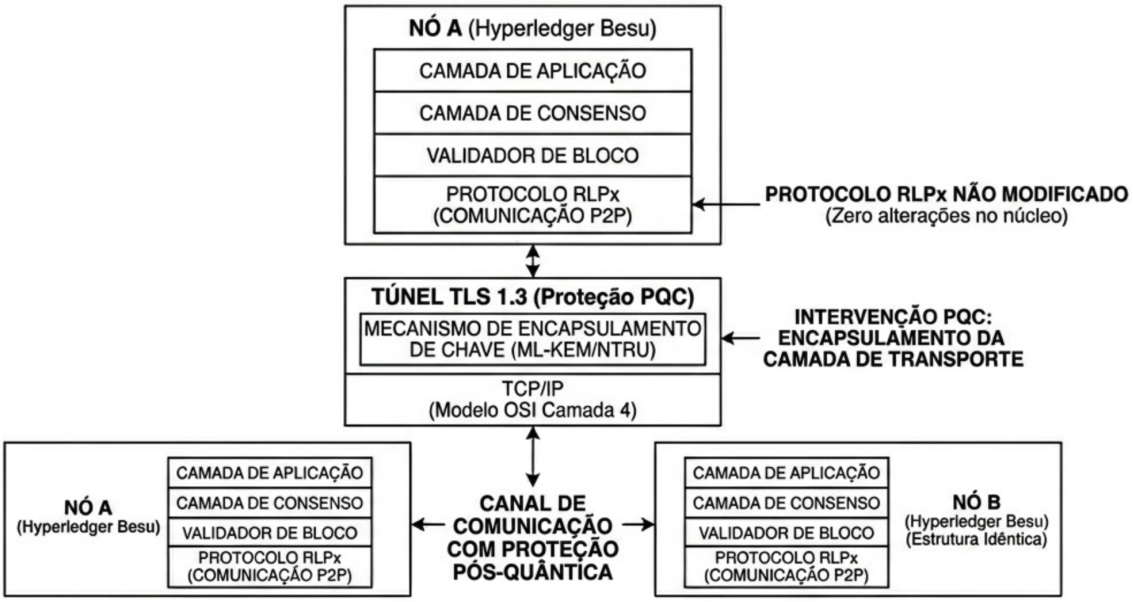

Figura 1. Arquitetura proposta com encapsulamento TLS 1.3 para proteção pós-quântica no canal RLPx.

quântica adicional, formando um esquema híbrido de autenticação.

Durante a criação do bloco, o nó remetente realiza o processo tradicional de assinatura ECDSA sobre os dados originais. Em seguida, uma assinatura pós-quântica é gerada sobre uma representação equivalente dos dados, sendo anexada ao bloco como um campo adicional. Esse procedimento resulta em um bloco logicamente ampliado, no qual a estrutura original permanece intacta, enquanto a informação criptográfica adicional é incorporada de forma não disruptiva. Importante destacar que não há alteração no formato canônico esperado pelo protocolo Ethereum, mas sim a extensão controlada do objeto em trânsito.

No nó receptor, o processo de verificação também ocorre de forma incremental. Inicialmente, a assinatura pós-quântica é validada por meio de uma camada de integração baseada em JNI (*liboqs-java*), que atua como ponte entre o ambiente Java do Besu e a biblioteca nativa *liboqs*. Uma vez validada a assinatura pós-quântica, o bloco é restaurado ao seu formato original, removendo-se os campos adicionais, e então submetido ao fluxo tradicional de verificação ECDSA já implementado no cliente. Dessa forma, a compatibilidade com o pipeline legado é preservada, e o mecanismo de consenso permanece inalterado.

Essa estratégia apresenta três vantagens fundamentais. Primeiro, mantém a separação entre lógica de consenso e mecanismos criptográficos, evitando impactos em protocolos como IBFT e QBFT. Segundo, permite a introdução e substituição de algoritmos pós-quânticos de forma modular, via camada JNI, sem necessidade de refatoração do núcleo do cliente. Terceiro, viabiliza um modelo híbrido no qual a aceitação de blocos pode, dependendo da política adotada, considerar uma ou ambas as assinaturas, oferecendo flexibilidade para diferentes cenários de transição. Em conjunto, esses fatores reforçam o caráter não intrusivo da proposta e evidenciam sua aderência ao princípio de

agilidade criptográfica no contexto de blockchain.

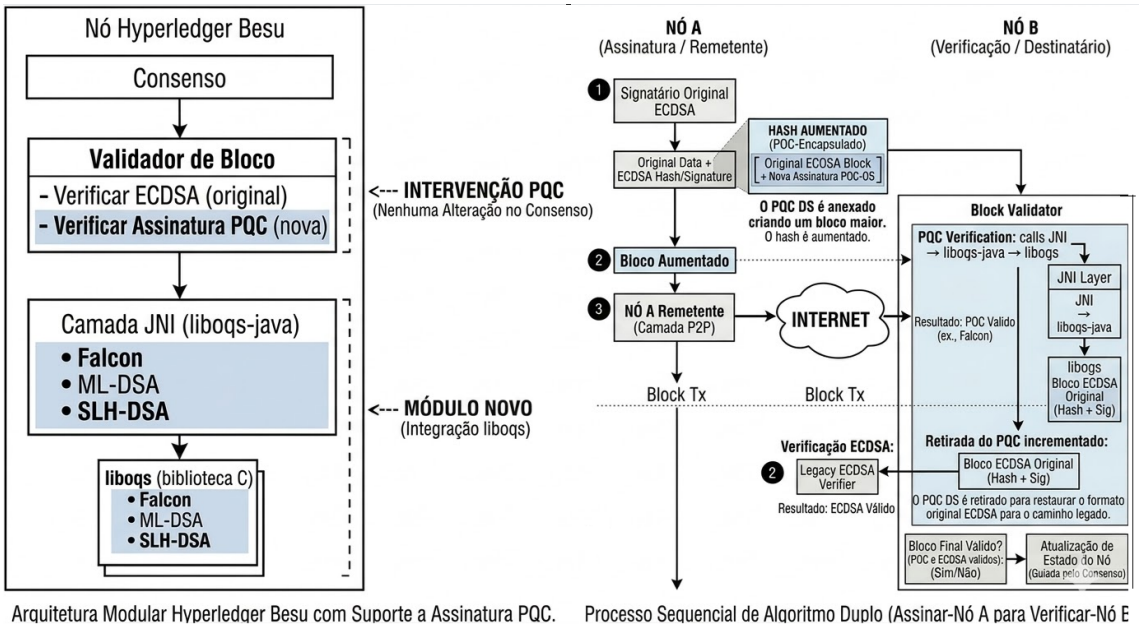

Figura 2. Fluxo de assinatura híbrida com inclusão de mecanismo pós-quântico no módulo Validador de Blocos.

4.1. Algoritmos Pós-Quânticos Avaliados

Os experimentos conduzidos neste trabalho consideram um conjunto representativo de algoritmos pós-quânticos padronizados ou finalistas do processo de padronização do NIST, todos acessados por meio da biblioteca *liboqs*. A seleção buscou contemplar diferentes famílias criptográficas, de modo a capturar *trade-offs* relevantes entre desempenho, tamanho de chaves e maturidade das construções.

Para o estabelecimento de chaves no túnel TLS, foi utilizado o ML-KEM-512 (padronizado no FIPS 203), uma construção baseada em reticulados que representa atualmente a principal escolha do NIST para mecanismos de encapsulamento de chaves. Como alternativa, foi avaliado o algoritmo NTRU, também baseado em reticulados, porém com características estruturais distintas, permitindo observar variações de desempenho e consumo de recursos dentro da mesma classe de problemas matemáticos.

No que se refere às assinaturas digitais, foram considerados três esquemas pós-quânticos com propriedades complementares. O ML-DSA-44 (FIPS 204), também baseado em reticulados, foi selecionado por representar a solução padrão recomendada pelo NIST para assinaturas digitais. O Falcon-512, igualmente baseado em reticulados, foi incluído por apresentar assinaturas significativamente menores, sendo frequentemente apontado como alternativa promissora em cenários com restrições de largura de banda. Por fim, o SLH-DSA-SHA2-128f (FIPS 205), baseado em funções hash, foi avaliado como representante de construções estateless com forte segurança teórica, ainda que com custos computacionais e tamanhos de assinatura mais elevados.

Essa diversidade de algoritmos permite analisar, de forma comparativa, diferentes abordagens criptográficas sob o ponto de vista de sua aplicabilidade em ambientes blockchain.

4.2. Ambiente Experimental

Os experimentos foram conduzidos em um ambiente controlado composto por três nós validadores Besu, distribuídos em máquinas virtuais Linux ARMv9 com Ubuntu 24, interconectadas por rede local dedicada. Cada nó executou uma instância Besu, um processo de túnel TLS pós-quântico e serviços auxiliares de monitoramento.

As configurações de consenso, tamanho de bloco e parâmetros de rede foram mantidas constantes em todos os cenários. Para cada algoritmo pós-quântico, foram realizados experimentos independentes, além de um cenário de referência utilizando exclusivamente ECDSA e TLS clássico.

4.3. Metodologia Experimental

Os experimentos foram conduzidos com foco na avaliação do custo do núcleo criptográfico, considerando as operações de geração de chaves, assinatura e verificação. Como baseline clássico, foi utilizado o ECDSA sobre a curva secp256k1, com mensagens previamente hasheadas via Keccak-256, em alinhamento com o modelo adotado no ecossistema Ethereum/Besu. Os algoritmos pós-quânticos foram avaliados por meio da biblioteca *liboqs*, integrada via JNI.

Cada experimento foi precedido por uma fase de aquecimento (warm-up), composta por 50 execuções não contabilizadas, com o objetivo de mitigar efeitos de inicialização da JVM, otimização dinâmica (JIT) e carregamento de bibliotecas nativas. Em seguida, foram realizadas 1000 execuções efetivas por operação, cujos resultados foram utilizados para cálculo da média e do desvio padrão, garantindo consistência estatística e reprodutibilidade das medições. O tempo de execução foi obtido com resolução de nanossegundos por meio da função `System.nanoTime()`.

Os testes foram executados em ambiente dedicado, com afinidade de CPU fixada em um único núcleo e parâmetros de execução da JVM controlados, reduzindo interferências externas.

5. Resultados

Esta seção apresenta os resultados experimentais obtidos a partir da avaliação da arquitetura proposta. Os resultados são organizados de acordo com os dois planos principais do sistema: (i) o plano de comunicação, responsável pela troca de chaves e proteção do tráfego entre nós, e (ii) o plano de dados, responsável pela geração e verificação de evidências pós-quânticas associadas às transações. Todos os resultados são comparados com um cenário de referência baseado exclusivamente em TLS clássico e assinaturas ECDSA.

5.1. Impacto da Troca de Chaves Pós-Quântica

Inicialmente avaliamos o impacto da utilização de mecanismos de troca de chaves pós-quânticos no estabelecimento de sessões TLS entre os nós validadores. Foram avaliados os algoritmos ML-KEM-512 e NTRU-HPS-509, empregados em um túnel TLS configurado com OpenSSL 3 e `oqs-provider`. Como baseline, utilizou-se o ECDHE sobre a curva secp256k1. As métricas analisadas incluem tempo de execução das operações criptográficas (geração de chaves, encapsulamento e desencapsulamento) e sua equivalência em ciclos de CPU, em arquiteturas x86 e ARMv9.

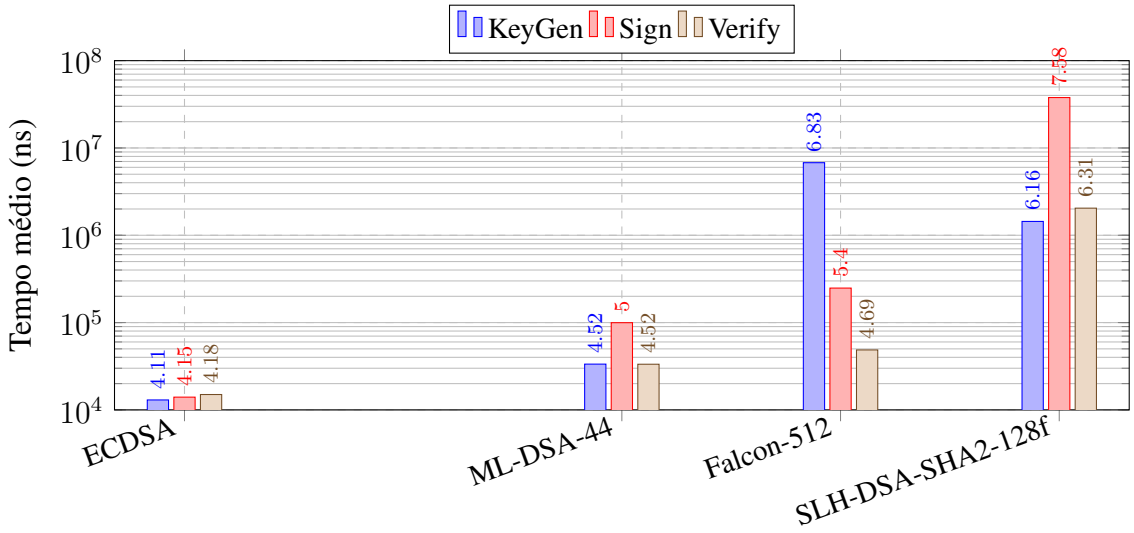

Figura 3. Tempo médio das operações de assinatura digital.

A Tabela 1 apresenta os resultados médios observados para cada algoritmo.

Os resultados demonstram que o comportamento dos algoritmos pós-quânticos não é uniforme. O ML-KEM-512 apresentou desempenho significativamente superior ao baseline clássico, com tempos na ordem de dezenas de microssegundos (e.g., 14.288 ns para KeyGen em x86), representando uma redução de até duas ordens de grandeza em relação ao ECDHE-secp256k1. Esse comportamento também se reflete no consumo de CPU, indicando alta eficiência computacional do esquema baseado em lattice para operações de estabelecimento de segredo.

Por outro lado, o NTRU-HPS-509 apresentou desempenho intermediário, com tempos inferiores ao ECDHE, porém significativamente superiores ao ML-KEM-512. Ainda assim, observa-se uma redução consistente de custo computacional em relação ao baseline clássico, especialmente em arquitetura x86.

Adicionalmente, verifica-se que a arquitetura ARMv9 apresenta um aumento expressivo no número de ciclos para todas as primitivas, especialmente no ECDHE, sugerindo maior sensibilidade a operações de aritmética de curva elíptica nessa arquitetura. Em contrapartida, os algoritmos pós-quânticos mantêm uma relação mais estável entre tempo e ciclos, reforçando sua adequação para plataformas heterogêneas.

Diferentemente do que se observa em análises teóricas focadas em tamanho de chaves e mensagens, os resultados experimentais indicam que o custo computacional da troca de chaves pós-quântica, em especial com ML-KEM-512, pode ser inferior ao dos mecanismos clássicos. Isso sugere que o principal impacto desses algoritmos no handshake TLS tende a estar mais associado ao aumento do volume de dados transmitidos do que ao processamento criptográfico em si.

Por fim, observa-se que a substituição do mecanismo de troca de chaves no túnel TLS não introduz impacto relevante no comportamento do consenso após o estabelecimento das sessões seguras, corroborando a viabilidade da abordagem de tunelamento como estratégia de adoção incremental de criptografia pós-quântica em redes permissionadas.

Tabela 1. Comparação entre o baseline clássico ECDHE e algoritmos pós-quânticos para troca de chaves

Algoritmo	Arq.	KeyGen		Encap		Decap	
		ns	cycles	ns	cycles	ns	cycles
ECDHE-secp256k1	x86	1 239 552	991 642	1 045 358	836 286	1 175 041	940 033
	ARMv9	1 401 849	3 504 623	1 303 094	3 257 735	1 564 793	3 911 983
ML-KEM-512	x86	14 288	11 430	23 492	18 794	30 654	24 523
	ARMv9	19 635	49 088	32 009	80 023	46 470	116 175
NTRU-HPS-509	x86	422 387	337 910	446 069	356 855	474 058	379 246
	ARMv9	554 961	1 387 403	581 991	1 454 978	631 689	1 579 223

5.2. Impacto das Assinaturas Digitais Pós-Quântica

Nesta etapa, avaliamos o impacto da utilização de assinaturas digitais pós-quânticas no contexto do Hyperledger Besu, por meio de uma integração via JNI com a biblioteca `liboqs`. Essa abordagem permite a adoção de algoritmos pós-quânticos sem modificações invasivas no núcleo do cliente, mantendo a compatibilidade com o formato de transações e o mecanismo de consenso existentes.

Foram avaliados os algoritmos ML-DSA-44, Falcon-512 e SLH-DSA-128f, tendo como baseline o ECDSA-secp256k1. As métricas consideradas incluem os tempos médios de geração de chaves (KeyGen), assinatura (Sign) e verificação (Verify), em arquiteturas x86 e ARMv9.

As Tabelas 2 e 3 apresentam os resultados experimentais obtidos.

Os resultados evidenciam diferenças significativas de desempenho entre os algoritmos pós-quânticos. O ML-DSA-44 apresentou desempenho amplamente superior ao baseline clássico, com tempos de assinatura e verificação uma ordem de grandeza menores que o ECDSA em ambas as arquiteturas. Esse comportamento indica que esquemas baseados em reticulados podem não apenas ser viáveis, mas também mais eficientes do que soluções clássicas em cenários práticos.

Em contraste, o Falcon-512 apresentou custos significativamente mais elevados, com tempos de assinatura e verificação na ordem de milissegundos. Embora ofereça vantagens em termos de tamanho de assinatura, seu custo computacional elevado pode impactar diretamente a vazão de transações e o tempo de validação de blocos em redes blockchain.

O algoritmo SLH-DSA-128f, baseado em hash, apresentou comportamento assimétrico: enquanto a geração de chaves mantém valores próximos ao ECDSA, as operações de assinatura e verificação são significativamente mais custosas, alcançando dezenas de milissegundos. Esse perfil reforça seu posicionamento como uma alternativa de alta segurança, porém com impacto relevante em desempenho.

Adicionalmente, observa-se que a arquitetura ARMv9 apresenta degradação mais acentuada para algoritmos pós-quânticos, especialmente nos esquemas baseados em hash e em estruturas mais complexas, como Falcon. Ainda assim, o ML-DSA mantém vantagem significativa mesmo nesse ambiente, indicando maior robustez a variações de arquitetura.

Do ponto de vista da integração via JNI, os resultados indicam que o overhead introduzido pela interface nativa não compromete a análise comparativa entre os algoritmos, uma vez que as diferenças observadas são dominadas pelo custo das primitivas criptográficas. Isso valida a abordagem como uma estratégia viável para experimentação e adoção incremental de assinaturas pós-quânticas em clientes blockchain existentes.

Por fim, os resultados permitem identificar combinações práticas de algoritmos pós-quânticos para uso em redes permissionadas baseadas em Hyperledger Besu. Em particular, o ML-DSA-44 se destaca como uma alternativa com excelente equilíbrio entre segurança e desempenho, enquanto Falcon-512 e SLH-DSA-128f podem ser considerados em cenários específicos onde requisitos adicionais, como tamanho de assinatura ou níveis mais conservadores de segurança, sejam prioritários.

Tabela 2. Desempenho dos algoritmos em arquitetura ARMv9 (Neoverse-V2)

Algoritmo	KeyGen (ns)	Sign (ns)	Verify (ns)
ECDSA-secp256k1	828 095	1 121 587	1 729 290
ML-DSA-44	41 899	140 675	187 258
Falcon-512	5 291 853	5 389 059	5 412 748
SLH-DSA-128f	848 636	20 618 278	21 818 647

Tabela 3. Desempenho dos algoritmos em arquitetura x86

Algoritmo	KeyGen (ns)	Sign (ns)	Verify (ns)
ECDSA-secp256k1	765 676	1 152 021	1 544 509
ML-DSA-44	19 218	76 110	96 847
Falcon-512	4 266 159	4 320 164	4 456 887
SLH-DSA-128f	752 110	18 262 188	20 158 610

6. Discussão dos Resultados

A análise comparativa revela que a transição para uma blockchain quantum-resistant impõe um trade-off de performance heterogêneo entre as arquiteturas testadas. O ML-KEM-512 demonstrou uma superioridade temporal disruptiva em relação ao ECDH-secp256k1, sendo aproximadamente 86 vezes mais rápido no processo de Key Generation e 44 vezes mais veloz no encapsulamento em ambiente x86. Essa aceleração drástica em nanossegundos sugere que, embora os algoritmos pós-quânticos lidem com estruturas matemáticas mais complexas, sua execução computacional é altamente otimizada para CPUs modernas. Entretanto, essa vantagem é atenuada em arquiteturas ARMv9, onde o ML-KEM exige um volume de ciclos de CPU significativamente maior pela provável ausência do aproveitamento de instruções vetoriais, evidenciando que a eficiência da rede permissionada dependerá diretamente do alinhamento entre o algoritmo escolhido e o conjunto de instruções do hardware hospedeiro.

Por outro lado, o NTRU-HPS-509 apresenta um perfil de desempenho mais conservador quando comparado ao baseline clássico. Embora ainda consiga superar o ECDHE em tempo de execução (sendo cerca de 2.9 vezes mais rápido no KeyGen em x86), seu custo operacional é consideravelmente mais elevado que o do ML-KEM,

o que o posiciona como uma alternativa de segurança robusta, porém menos eficiente para cenários de alto rendimento (throughput) no Besu. Em termos de infraestrutura, a substituição do ECDH por qualquer uma das alternativas pós-quânticas implica em um aumento inevitável no tamanho das chaves públicas e dos *ciphertexts*, passando de 65 bytes no ECDHE para até 800 bytes no ML-KEM. Assim, a viabilidade prática da blockchain pós-quântica não reside apenas na velocidade de processamento, mas na capacidade da rede em suportar o aumento do payload nas transações sem degradar a latência do consenso.

Nesse contexto, ao considerar o impacto direto no tamanho dos blocos, observa-se uma expansão significativa do *payload* criptográfico. No baseline com *ECDSA-secp256k1*, as assinaturas possuem tipicamente 64–72 bytes, permitindo uma alta densidade de transações em blocos de 1MB. Em contraste, o ML-DSA-44 (FIPS 204) apresenta assinaturas de aproximadamente 2,4 KB, reduzindo a capacidade teórica do bloco em cerca de 35 a 40 vezes. O Falcon-512 (FIPS 206), por sua vez, mantém assinaturas compactas (666 bytes), implicando uma redução mais moderada, da ordem de 8 a 10 vezes em relação ao baseline. Já o SLH-DSA-128f (FIPS 205) apresenta assinaturas substancialmente maiores (8 a 17 KB, dependendo da parametrização), o que pode reduzir a quantidade de transações por bloco em até duas ordens de grandeza. Dessa forma, embora algoritmos como ML-DSA apresentem excelente desempenho computacional, o aumento no tamanho das assinaturas impõe uma limitação estrutural ao throughput da rede. Esse resultado evidencia que a adoção de criptografia pós-quântica em blockchains permissionadas deve considerar não apenas o custo de CPU, mas também a eficiência de utilização do espaço em bloco, sendo Falcon-512 uma alternativa particularmente equilibrada quando a restrição de banda e armazenamento se torna fator crítico.

7. Conclusão e Trabalhos Futuros

Este trabalho investigou a viabilidade de introdução de criptografia pós-quântica em uma blockchain permissionada baseada no Hyperledger Besu, adotando uma abordagem não-invasiva fundamentada em agilidade criptográfica. A proposta combinou o uso de túneis TLS 1.3 com algoritmos pós-quânticos no plano de comunicação e a extensão do processo de validação de blocos por meio de assinaturas híbridas integradas via JNI.

Os resultados demonstraram que a adoção de primitivas pós-quânticas é viável em ambientes reais, embora introduza trade-offs relevantes. Enquanto mecanismos de encapsulamento de chaves baseados em reticulados apresentaram desempenho competitivo, o uso de assinaturas pós-quânticas evidenciou impactos significativos, sobretudo no tamanho das assinaturas e no custo computacional. Esses fatores afetam diretamente o throughput e a eficiência de armazenamento da rede, reforçando a necessidade de uma avaliação sistêmica.

A abordagem proposta preserva a compatibilidade com o cliente Besu e evita modificações intrusivas, reduzindo riscos de regressão e custos de manutenção, o que a torna adequada para cenários de transição incremental.

Como trabalhos futuros, destacam-se a avaliação em ambientes de larga escala, a investigação de técnicas de otimização para redução de overhead (como agregação e compressão de assinaturas) e a análise do impacto em diferentes protocolos de consenso e arquiteturas de hardware. Adicionalmente, pretende-se explorar a generalização da abor-

dagem para outras plataformas blockchain e sistemas distribuídos.

8. Agradecimentos

Os autores agradecem o apoio concedido pelo Ministerio da Ciencia, Tecnologia e Inovação (MCTI) por meio de recursos da Lei no 8.248, de 23 de outubro de 1991, no âmbito do PPI SOFTEX (coordenado pela Softex e publicado como Residencia em TIC 11, DOU 01245.011733/2022-83).

Referências

Allende, e. a. (2023). Quantum-safe cryptography in distributed systems. *Scientific Reports*.

Asanso, e. a. (2024). Post-quantum signatures in ethereum via account abstraction. In *Proceedings of Springer Conference*.

Buterin, V. (2015). Ethereum white paper. `https://ethereum.org/en/whitepaper/`.

Community, E. R. (2024). So you wanna post-quantum ethereum transaction signature.

Ghosh, S. (2025). Quantum blockchain survey: Foundations, trends, and gaps. *arXiv preprint arXiv:2507.13720*.

Hyperledger Foundation (2024). Hyperledger besu documentation. `https://besu.hyperledger.org/`. Accessed: 2026.

Lehman, M. M. (1980). Programs, life cycles, and laws of software evolution. *Proceedings of the IEEE*.

Mens, T. and Demeyer, S. (2008). Software evolution. *Springer*.

NIST (2023a). Migration to post-quantum cryptography. Technical Report NIST IR 8413, National Institute of Standards and Technology.

NIST (2023b). Migration to post-quantum cryptography. Technical Report NIST IR 8413, National Institute of Standards and Technology.

Reddy, e. a. (2025). Advances in post-quantum cryptography applications. *Scientific Reports*.

Zorzo, e. a. (2023). Performance evaluation of post-quantum cryptographic algorithms. *Scientia Reports*.