Avaliação Multidimensional de Infraestruturas Blockchain: Metodologia Experimental e Análise de Trade-offs

Bruno Evaristo[1,2], **Antonio Mateus de Sousa** [1], **Jeffson Celeiro Sousa**[1,2], **Ismael Ávila**[1]

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

[2]Universidade Federal do Pará (UFPA)
Belém – PA – Brasil

{elderb, amateus, jcsousa, avila_an}@cpqd.com.br

Abstract. *Blockchain technologies have consolidated as critical trust and coordination infrastructures in modern distributed systems. However, traditional evaluation methods fail by focusing on isolated metrics, ignoring the systemic trade-offs inherent in these architectures. To bridge this gap, this paper proposes a multidimensional experimental methodology for evaluating blockchain infrastructures, integrating dimensions of performance, cryptographic resilience, interoperability, security, and governance. The empirical validation was conducted across six heterogeneous testbeds from the Ilíada Project. The trade-off analysis reveals that gains in security, auditability, and interchain communication impose a direct computational cost, heavily impacting latency and throughput. The results prove that evaluating isolated metrics, such as transactions per second (TPS) in a laboratory, is an illusory metric if not coupled with the actual security and governance costs demanded by the application, thus enabling a systemic and reproducible characterization of these networks under realistic operational conditions.*

Resumo. *As tecnologias de blockchain consolidaram-se como infraestruturas críticas de confiança e coordenação em sistemas distribuídos. Contudo, os métodos tradicionais de avaliação falham ao focar em métricas isoladas, ignorando os compromissos sistémicos inerentes a estas arquiteturas. Para suprir esta lacuna, este artigo propõe uma metodologia experimental multidimensional para a avaliação de infraestruturas blockchain, integrando as dimensões de desempenho, resiliência criptográfica, interoperabilidade, segurança e governança. A validação empírica foi conduzida em seis testbeds heterogéneos do Projeto Ilíada. A análise de trade-offs revela que ganhos em segurança, auditabilidade e comunicação entre cadeias impõem um custo computacional direto, impactando fortemente a latência e a vazão. Os resultados comprovam que avaliar apenas transações por segundo (TPS) em laboratório é uma métrica ilusória se não estiver acoplada aos custos reais de segurança e governança, viabilizando assim uma caracterização sistémica e reprodutível destas redes sob condições operacionais realistas.*

1. Introdução

As tecnologias de blockchain e de livros-razão distribuídos (Distributed Ledger Technologies - DLTs) evoluíram de plataformas experimentais voltadas a criptomoedas para

se tornarem componentes centrais de diversos sistemas em rede [Zheng et al. 2020]. Nesses cenários, as redes blockchain passam a atuar como elementos críticos do plano de controle, sendo responsáveis por coordenar acesso a recursos, estabelecer relações de confiança e manter consistência global em ambientes altamente distribuídos [Enaya 2025].

À medida que essas tecnologias se integram a infraestruturas reais, torna-se evidente a necessidade de metodologias de avaliação sistemáticas e rigorosas. Abordagens tradicionais de análise de desempenho mostram-se insuficientes para capturar os compromissos introduzidos por arquiteturas blockchain, que exigem a consideração simultânea de métricas clássicas (latência, vazão, tolerância a falhas) e dimensões adicionais, como sobrecarga criptográfica, mecanismos de consenso, interoperabilidade entre cadeias, segurança de contratos inteligentes e auditabilidade operacional [Enaya 2025] .

Grande parte da literatura aborda essas dimensões de forma fragmentada, analisando desempenho, segurança ou interoperabilidade isoladamente. Embora relevantes, tais abordagens não capturam o comportamento sistêmico das redes blockchain, nas quais melhorias em uma dimensão frequentemente implicam penalidades em outras [Wang et al. 2024]. Como consequência, carece-se de um arcabouço experimental unificado que permita análises holísticas, comparáveis e reprodutíveis.

Este trabalho busca preencher essa lacuna ao propor uma *metodologia experimental multidimensional* para a avaliação de redes blockchain, integrando métricas, dimensões e procedimentos experimentais em um único processo de análise. A metodologia permite caracterizar trade-offs estruturais entre desempenho, segurança, interoperabilidade e resiliência criptográfica sob a ótica da engenharia de sistemas distribuídos.

Para validação, conduzimos um estudo experimental utilizando seis infraestruturas reais desenvolvidas no contexto do Projeto Ilíada [1], abrangendo diferentes arquiteturas, mecanismos de consenso, protocolos interchain, integrações com criptografia pós-quântica, identidade descentralizada e ferramentas de auditoria. Esses ambientes fornecem um cenário realista e heterogêneo para aplicação da metodologia proposta.

As principais contribuições deste trabalho são: (i) a definição de uma metodologia experimental multidimensional para avaliação de blockchains; (ii) sua validação empírica em múltiplos testbeds heterogêneos; e (iii) uma análise dos compromissos estruturais que caracterizam sistemas blockchain enquanto infraestruturas computacionais de confiança distribuída.

O restante deste artigo está organizado da seguinte forma. A Seção 2 apresenta os trabalhos relacionados. A Seção 3 descreve a metodologia experimental multidimensional. A Seção 4 discute os resultados experimentais segundo as principais dimensões de avaliação. Por fim, a Seção 5 apresenta as conclusões e direções para trabalhos futuros.

2. Trabalhos Relacionados

A avaliação experimental de redes blockchain tem sido abordada na literatura sob diferentes perspectivas, refletindo a diversidade de arquiteturas e aplicações desses sistemas. De forma geral, os trabalhos existentes podem ser organizados em quatro categorias principais: (i) desempenho e escalabilidade, (ii) mecanismos de consenso, (iii) segurança e

[1] https://iliadablockchain.org.br/

Tabela 1. Cobertura das dimensões de avaliação de blockchain na literatura. Símbolos: ✓ indica que a dimensão é explicitamente avaliada; – indica ausência de avaliação.

Abordagem	Desempenho	Segurança	Interoperabilidade	PQC
Blockbench / Caliper	✓	–	–	–
Estudos de Consenso	✓	–	–	–
Auditoria de Contratos Inteligentes	–	✓	–	–
Frameworks Interchain	–	–	✓	–
Avaliações Pós-Quânticas	–	✓	–	✓
Metodologia Proposta	✓	✓	✓	✓

auditoria de contratos inteligentes, e (iv) interoperabilidade entre blockchains. Embora cada uma dessas linhas contribua para o entendimento do comportamento de sistemas blockchain, observa-se que a maioria dos estudos trata essas dimensões de maneira isolada, sem uma abordagem integrada. A Tabela 1 sintetiza essas linhas e evidencia que, enquanto os trabalhos existentes concentram-se em dimensões específicas, a proposta deste artigo integra múltiplos aspectos em uma única metodologia experimental.

No contexto de desempenho e escalabilidade, ferramentas como *Blockbench e Hyperledger Caliper*[2] têm sido amplamente utilizadas para mensurar métricas clássicas, como latência, vazão e taxa de falhas, tanto em blockchains públicas quanto permissionadas [Foundation 2024]. Esses trabalhos fornecem mecanismos importantes de instrumentação, porém concentram-se predominantemente em aspectos quantitativos de desempenho, sem incorporar dimensões como sobrecarga criptográfica, interoperabilidade ou segurança sistêmica [Zheng et al. 2020]. Em relação aos mecanismos de consenso, a literatura apresenta diversos estudos comparando algoritmos como *Proof-of-Work (PoW), Proof-of-Stake (PoS)* e variantes de *Byzantine Fault Tolerance (BFT)*, analisando seu impacto sobre desempenho, consumo energético e tolerância a falhas. Apesar de relevantes, esses trabalhos geralmente assumem modelos de rede homogêneos e não consideram explicitamente efeitos introduzidos por camadas superiores, como contratos inteligentes ou integrações Interchain [Li et al. 2022].

A segurança de contratos inteligentes constitui outra linha consolidada, com o uso de ferramentas como *Slither, Mythril, Oyente e ConFuzzius* para análise estática e dinâmica de vulnerabilidades na *Ethereum Virtual Machine(EVM)*. Esses estudos demonstram a viabilidade da automação de auditorias, porém focam principalmente na corretude do código, sem relacionar os resultados com métricas de desempenho ou impacto operacional na infraestrutura blockchain como um todo [Atzei et al. 2021]. Por fim, no domínio da interoperabilidade, frameworks como Cosmos, Polkadot e Hyperledger Cacti exploram mecanismos baseados em notários, provas criptográficas, *sidechains* e HTLC para comunicação entre cadeias heterogêneas. Embora essas abordagens avancem no aspecto funcional, ainda faltam avaliações sistemáticas que quantifiquem custos operacionais, latência e efeitos sistêmicos das operações interchain [Belchior et al. 2023].

Mais recentemente, alguns estudos têm investigado a integração de criptogra-

[2]Ferramenta oficial do Hyperledger para benchmark e avaliação de desempenho de blockchains: https://www.hyperledger.org/use/caliper

fia pós-quântica (PQC) em blockchains, como os trabalhos de [Fernandes et al. 2022] e [Sinai 2024], analisando o impacto da substituição de algoritmos de assinatura e troca de chaves sobre tempo de processamento e tamanho das transações. Embora relevantes para a resiliência criptográfica, essas avaliações são geralmente conduzidas de forma isolada, sem considerar efeitos combinados com consenso, interoperabilidade ou mecanismos de auditoria [Fernandes et al. 2022].

Em síntese, a literatura existente apresenta avanços importantes em dimensões específicas, mas carece de uma metodologia experimental unificada que integre múltiplos aspectos em um único arcabouço analítico. Diferentemente dos trabalhos relacionados, este artigo propõe uma abordagem multidimensional que combina desempenho, segurança, interoperabilidade e robustez criptográfica em uma metodologia experimental única, validada em múltiplas infraestruturas reais, permitindo a análise sistêmica de compromissos entre camadas sob condições realistas de operação.

3. Proposta de Metodologia experimental multidimensional

Esta seção apresenta a base conceitual da metodologia proposta para a avaliação experimental de redes blockchain. A abordagem fundamenta-se na premissa de que infraestruturas blockchain devem ser analisadas como sistemas distribuídos complexos, cujo comportamento emerge da interação entre múltiplas camadas arquiteturais, incluindo rede, consenso, criptografia e aplicação. Nesse contexto, métricas isoladas são insuficientes para caracterizar adequadamente as propriedades operacionais do sistema, sendo necessária uma abordagem multidimensional.

Figura 1. Modelo Conceitual de Camadas em Sistemas Blockchain

A Figura 1 apresenta o modelo conceitual em camadas de um sistema blockchain, evidenciando o fluxo de processamento de transações desde a geração de carga até a execução de contratos inteligentes e atualização do estado global. Esse modelo abstrai os principais componentes funcionais da infraestrutura, permitindo analisar como protocolos de comunicação, mecanismos de consenso e primitivas criptográficas contribuem de forma integrada para o comportamento observado.

Com base nessa abstração, a Figura 2 detalha a instrumentação da arquitetura, ilustrando os pontos de coleta e o fluxo de dados para análise. Esse mapeamento fundamenta a metodologia, vinculando diretamente os componentes arquiteturais às dimensões de avaliação. A abordagem integra métricas clássicas de desempenho (latência, vazão, taxa de falhas) a propriedades intrínsecas de blockchains, como segurança, interoperabilidade, governança e resiliência criptográfica, fornecendo uma caracterização sistêmica e unificada do comportamento operacional da infraestrutura.

3.1. Dimensões de Avaliação

O primeiro componente do *framework* consiste na definição de um espaço de avaliação multidimensional, composto por cinco dimensões centrais: desempenho, segurança, interoperabilidade, confiança e governança, e resiliência criptográfica. Cada dimensão con-

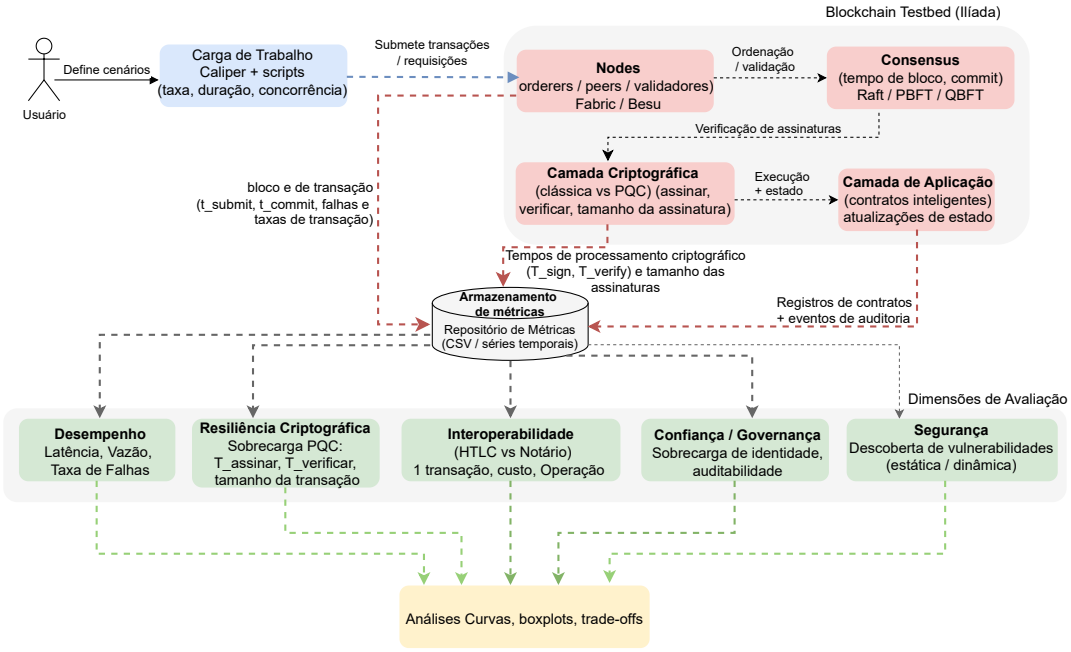

Figura 2. Arquitetura conceitual da metodologia experimental multidimensional.

templa um conjunto específico de propriedades do sistema, conforme resumido na Tabela 2.

Tabela 2. Dimensões de avaliação e propriedades sistêmicas correspondentes.

Dimensão	Propriedades Avaliadas
Desempenho	Latência, vazão, tempo de geração de blocos, taxa de falhas.
Segurança	Robustez criptográfica, vulnerabilidades em contratos inteligentes, superfície de ataque.
Interoperabilidade	Custo de transações interchain, consistência, atomicidade.
Confiança e Governança	Gerenciamento de identidades, auditabilidade, rastreabilidade.
Resiliência Criptográfica	Sobrecarga criptográfica pós-quântica, tamanho de assinaturas, tempo de verificação.

A dimensão de Desempenho contempla métricas clássicas de sistemas distribuídos, como latência ponta a ponta, vazão, tempo de bloco e taxa de falhas, analisadas como séries temporais para identificar gargalos associados ao consenso, à comunicação e à execução de contratos. A dimensão de segurança avalia a resistência a falhas e ataques, incluindo robustez criptográfica e vulnerabilidades em contratos inteligentes, mensuradas por ferramentas de análise estática e dinâmica e seu impacto no desempenho [Zheng et al. 2020].

A dimensão de Interoperabilidade mede a capacidade de blockchains heterogêneas

trocarem dados e ativos, considerando número de transações interchain, custo agregado e latência, permitindo comparar estratégias como *Hash Time-Locked Contract*(HTLC) e esquemas notariais. A dimensão de Confiança e Governança aborda identidade, autenticação e auditabilidade, por meio de métricas de custo operacional de DIDs, persistência de eventos *on-chain* e volume de dados para rastreabilidade [Zhao et al. 2022]. Por fim, a dimensão de Resiliência Criptográfica quantifica o impacto da criptografia pós-quântica, avaliando aumento de tamanho de assinaturas, tempo de verificação e sobrecarga computacional, analisando o *trade-off* entre segurança de longo prazo e eficiência operacional [Sinai 2024].

3.2. Métricas, Instrumentação e Ambientes Experimentais

A instrumentação da validação empírica adota uma abordagem híbrida. A coleta primária de desempenho (latência, vazão, taxa de falhas) utiliza o *Hyperledger Caliper*, complementado por *scripts* que capturam dados temporais dos nós validadores. Métricas de segurança, criptografia (vulnerabilidades, tempos de operação, tamanho de assinaturas) e interoperabilidade (latência *interchain*, transações, gás) são extraídas via ferramentas de auditoria especializadas e instrumentação de protocolos.

A validação ocorreu em seis *testbeds* do Projeto Ilíada (Tabela 3), compostos estruturalmente por nós blockchain, clientes de carga, instrumentação e módulo de análise. Para garantir rigor e reprodutibilidade, os cenários operam em topologia distribuída usando *contêineres Docker* em VMs padronizadas (8 vCPUs, 16 GB RAM, SSD, rede local *Gigabit*). Executaram-se 30 réplicas por experimento, reportando métricas agregadas com intervalo de confiança de 95% ou desvio padrão.

A alocação das dimensões em seis *testbeds* distintos foi uma decisão deliberada para evitar ruídos cruzados. Mantendo constantes parâmetros como número de nós e topologia, criaram-se ambientes especializados, e.g., o *DroneChain* isola gargalos de consenso, enquanto o *GT-Inter* foca na latência entre cadeias. Essa estratégia isola as variáveis, estabelece relações causais precisas e permite que o *framework* avalie sistemicamente como desempenho, segurança e interoperabilidade operam de forma acoplada no plano de controle da blockchain.

4. Resultados Experimentais e Discussão

Esta seção apresenta e discute os resultados obtidos a partir da aplicação do *framework* experimental multidimensional proposto sobre os seis ambientes blockchain descritos na Seção 3. Diferentemente de abordagens tradicionais, que analisam métricas isoladas, os resultados são organizados segundo quatro dimensões sistêmicas fundamentais: desempenho, sobrecarga criptográfica, interoperabilidade e segurança/auditabilidade. Além disso, são introduzidas métricas compostas que permitem caracterizar propriedades emergentes típicas de sistemas descentralizados.

4.1. Resultados de Desempenho

A dimensão de desempenho avalia a capacidade das infraestruturas blockchain em sustentar cargas concorrentes de requisições, considerando métricas clássicas de engenharia de sistemas distribuídos: latência, vazão *(throughput)*, taxa de falhas e tempo de confirmação de transações.

Tabela 3. Testbeds experimentais e dimensões avaliadas.

Testbed	**Dimensão**	**Escopo de Avaliação**
DroneChain	Desempenho	Latência, vazão, tempo de bloco, taxa de falhas sob carga (Fabric vs Besu).
BBPQ	Resiliência Criptográfica	Tamanho de assinatura, tempo de verificação, custo computacional, overhead PQC.
GT-Inter	Interoperabilidade	Número de transações interchain, latência total, custo, atomicidade (HTLC vs Notary).
PIDDF	Confiança e Governança	Custo de registro de identidade, tempo de resolução de DID, sobrecarga de autenticação.
Audita	Auditabilidade	Volume de logs, impacto no tempo de bloco, custo de transações, reconstrução de estado.
SmartSeg	Segurança	Número de vulnerabilidades, tempo de análise, taxa de falsos positivos, cobertura.

Os experimentos de desempenho foram conduzidos principalmente no ambiente *DroneChain*, focado no gerenciamento de tráfego de drones (UTM - *Unmanned Traffic Management*). Para a avaliação comparativa da Figura 3, utilizou-se como linha de base o sistema *InterUSS (Inter Unmanned Aerial System Service Supplier)*, um padrão de código aberto amplamente adotado para coordenação de espaço aéreo, confrontando o seu desempenho com as implementações baseadas em *Hyperledger Fabric* e *Hyperledger Besu*. A instrumentação foi realizada com a ferramenta *Hyperledger Caliper* e a carga foi gerada de forma sintética, variando progressivamente o número de requisições por segundo, de modo a caracterizar regimes de operação desde a baixa utilização até à saturação do sistema.

A latência média e os percentuais (P50, P95 e P99) revelam um fenômeno de degradação progressiva, no qual a latência cresce de forma não linear à medida que o sistema se aproxima da saturação. Esse comportamento está diretamente associado ao acoplamento entre o plano de consenso e a camada de execução de contratos inteligentes, característica inerente a arquiteturas blockchain.

Formalmente, a vazão instantânea do sistema pode ser expressa como:

$$TP_{inst} = \frac{N_{tx}}{\Delta t} \tag{1}$$

onde N_{tx} representa o número de transações confirmadas em um intervalo Δt. Observa-se empiricamente que TP_{inst} converge para um valor máximo TP_{max} determinado pela capacidade do mecanismo de consenso e pela configuração da rede.

Esses resultados confirmam que blockchains operam como sistemas distribuídos fortemente acoplados, nos quais latência, vazão e confiabilidade estão intrinsecamente relacionadas, impossibilitando a otimização isolada de uma única métrica sem impactos colaterais.

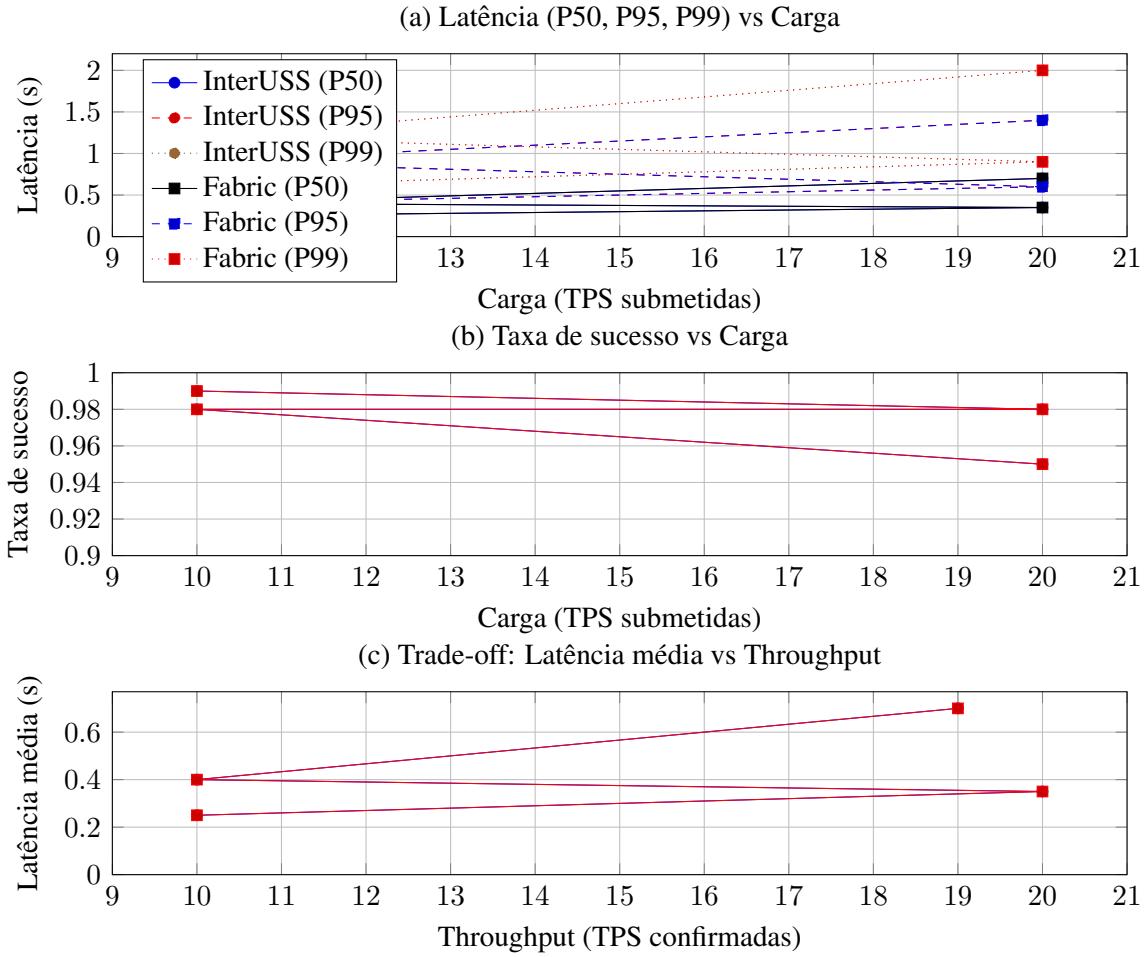

Figura 3. Resultados de desempenho no testbed DroneChain. (a) Latência (P50, P95 e P99) em função da carga. (b) Taxa de sucesso sob aumento de carga. (c) Trade-off entre latência (P50) e throughput, evidenciando o acoplamento entre execução e consenso.

4.2. Sobrecarga Criptográfica

A dimensão de sobrecarga criptográfica avalia o impacto da substituição de primitivas criptográficas clássicas por algoritmos pós-quânticos (PQC - *Post-Quantum Cryptography*) no desempenho operacional da blockchain. Essa análise foi conduzida no ambiente *BBPQ*[3], que integra algoritmos PQC híbridos diretamente ao *Hyperledger Fabric*. Foram medidas as seguintes métricas fundamentais: tempo de assinatura digital, tempo de verificação, tamanho das chaves, tamanho das assinaturas e o impacto no *throughput* global do sistema.

Como mostra a Figura 4, a análise compara primitivas clássicas (baseadas em curvas elípticas, como P256 e Ed25519) com algoritmos PQC padronizados ou em processo de padronização, como o ML-DSA (baseado em reticulados), Mayo (baseado em equações multivariadas) e o CROSS (baseado em códigos limitados). Avaliam-se também arranjos híbridos (ex.: ML-DSA+P256), que combinam a segurança testada da criptogra-

[3]https://observatorioblockchain.org.br/blockchain-pos-quantica/

fia clássica com a resistência quântica, gerando assinaturas duplas.

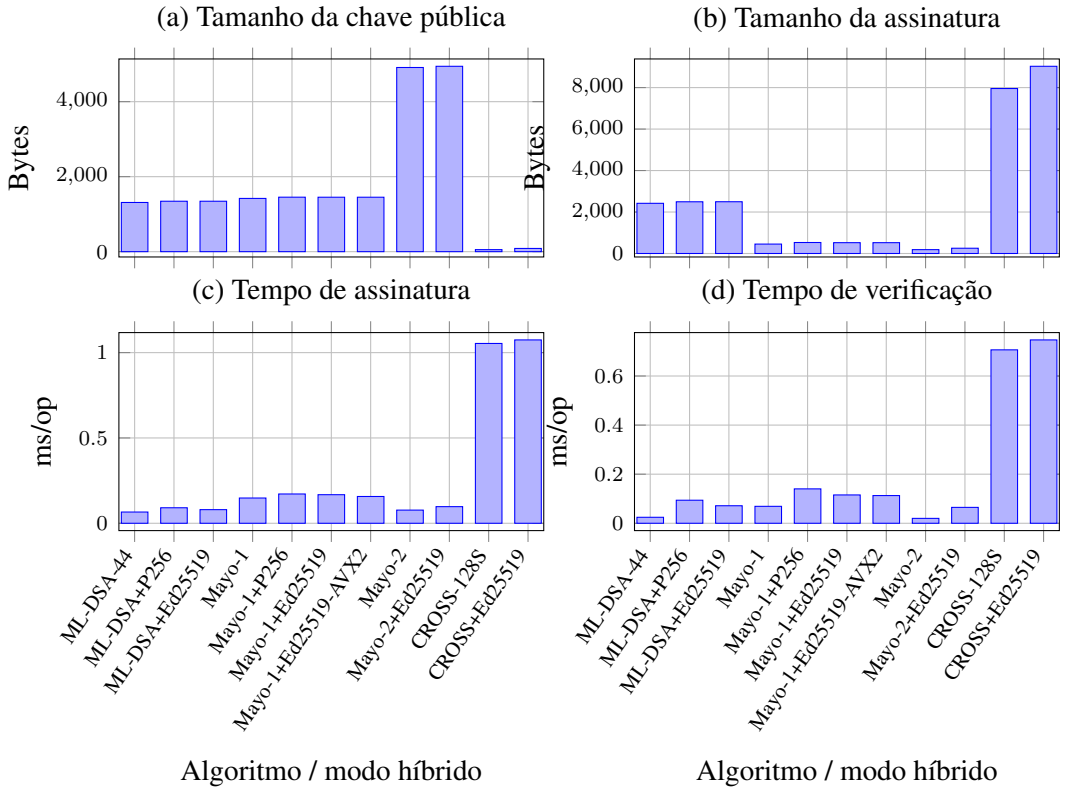

Figura 4. Sobrecarga criptográfica no ambiente BBPQ (benchmark local desacoplado do Fabric). (a) tamanho da chave pública, (b) tamanho da assinatura, (c) tempo médio de assinatura (ms/op) derivado de assinaturas/s, e (d) tempo médio de verificação (ms/op) derivado de verificações/s.

Os resultados evidenciam um aumento consistente no custo computacional das operações criptográficas. Conforme ilustrado nas Figuras 4(c) e 4(d), o algoritmo CROSS apresenta tempos de assinatura e verificação ordens de grandeza superiores aos esquemas clássicos e ao ML-DSA. Isso ocorre devido à natureza matemática dos problemas baseados em códigos criptográficos adotados pelo CROSS, que exigem operações matriciais densas e geram chaves significativamente maiores. De forma geral, os algoritmos PQC apresentam assinaturas maiores e tempos de verificação superiores, impactando diretamente o tempo total de confirmação das transações.

A sobrecarga relativa introduzida pela migração criptográfica pode ser formalizada como:

$$Overhead_{PQC} = \frac{T_{PQC} - T_{classico}}{T_{classico}} \tag{2}$$

onde T_{PQC} representa o tempo médio de uma operação criptográfica no modo pós-quântico, e $T_{classico}$ o tempo correspondente no modo tradicional.

Entretanto, observa-se que o uso de modos híbridos mitiga os riscos de segurança sem inviabilizar a operação do sistema, mantendo o *throughput* em níveis aceitáveis para

aplicações institucionais [Sinai 2024]. O contraste explícito com os modos clássicos demonstra que o orçamento computacional para a validação de blocos precisará ser revisto arquiteturalmente em redes de próxima geração. Do ponto de vista sistêmico, a criptografia deixa de ser um custo marginal e passa a constituir um componente estrutural do orçamento computacional do sistema distribuído.

4.3. Custos de Interoperabilidade

A interoperabilidade entre blockchains foi avaliada no ambiente *GT-Inter* [4], que implementa dois paradigmas distintos: mecanismos notariais e contratos HTLC. O objetivo foi quantificar o custo operacional e temporal associado à transferência de ativos entre as redes heterogêneas *Polygon Amoy e Avalanche* (ambas configuradas como testnets públicas para fins de experimentação), como definidos na Figura 5.

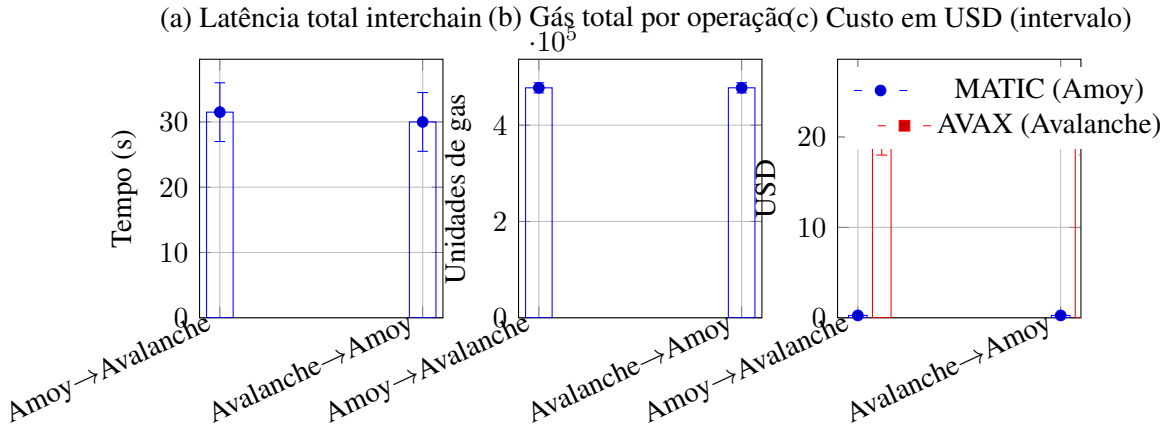

Figura 5. Custos de interoperabilidade no ambiente GT-Inter. (a) Latência total ponta-a-ponta por fluxo de transferência (média com intervalo). (b) Gás total consumido por operação completa (média com intervalo). (c) Custo estimado em USD para cada moeda de rede (média com intervalo). Valores reportados a partir dos KPIs do GT-Inter.

Os principais indicadores analisados foram: latência interchain, número total de transações envolvidas por operação, custo financeiro (em gas ou taxas) e taxa de falhas. Os gráficos demonstram que uma única transferência interchain exige múltiplas transações distribuídas, incluindo bloqueio do ativo na cadeia de origem, verificação externa e criação do ativo correspondente na cadeia de destino.

O custo total de uma operação interchain pode ser formalizado como:

$$C_{interchain} = \sum_{i=1}^{n} C_{tx_i} \tag{3}$$

Na formulação, $C_{interchain}$ é o custo total da operação de interoperabilidade, calculado pela agregação ($\sum_{i=1}^{n}$) do custo individual C_{tx_i} de cada transação i do protocolo. Esta equação evidencia que a comunicação *interchain* não possui custo único, mas acumula taxas a cada etapa distribuída. Por exigirem mais passos neste somatório (verificação

[4] https://observatorioblockchain.org.br/wp-content/uploads/2025/11/Final$_GT - Inter - 1.pdf$

e bloqueio), os mecanismos HTLC reduzem a dependência externa, mas impõem maior complexidade criptográfica e latência total. Em contraste, o modelo notarial reduz a latência, mas introduz um ponto de centralização lógico. Logo, a interoperabilidade transcende a integração funcional, atuando como um fator estrutural que redefine custos, latência e o modelo de confiança do sistema.

A aplicação integrada desta metodologia aos diversos *testbeds* revela o comportamento da blockchain como um sistema dinâmico de vasos comunicantes. Identificamos que a adoção de algoritmos seguros (PQC, analisados na Seção 4.2) ou o aumento da auditabilidade e interoperabilidade (Seções 4.3 e 4.4) cobram um ”imposto”direto sobre o desempenho bruto do sistema (Seção 4.1). Assim, a metodologia proposta comprova que a avaliação isolada de TPS (*Transactions Per Second*) em laboratório é uma métrica ilusória se não estiver acoplada aos custos de segurança e governança reais exigidos pela aplicação.

4.4. Segurança e Auditabilidade

A dimensão de segurança e auditabilidade foi analisada a partir dos ambientes *SmartSeg* [5], *Audita* [6] e *PIDDF*, cobrindo desde vulnerabilidades de contratos inteligentes até rastreabilidade de eventos operacionais e identidade descentralizada.

No *SmartSeg*, foram utilizados mecanismos automatizados de análise estática e dinâmica para detectar vulnerabilidades em contratos Solidity, avaliando-se o tempo de execução das ferramentas *Slither, Mythril e ConFuzzius*, conforme a Figura 6. Os resultados, em escala logarítmica, evidenciam diferenças significativas de custo computacional, com o Slither apresentando latências na ordem de milissegundos, enquanto Mythril e ConFuzzius alcançam tempos na ordem de segundos, devido ao uso de técnicas mais intensivas, como execução simbólica e *fuzzing*. Esses achados confirmam o *trade-off* entre custo computacional e poder de detecção, bem como a persistência de falsos positivos e limitações na identificação de falhas lógicas complexas, indicando a necessidade de pipelines híbridos que combinem análises rápidas e abordagens mais profundas.

No ambiente *Audita*, avaliou-se o impacto da persistência de *hashes* de *logs* de rede na blockchain, conforme a Figura 7. Os resultados indicam taxa de sucesso predominante nas operações de auditoria, com falhas, eventos nulos e perdas representando uma fração marginal das requisições. Embora a auditabilidade *on-chain* introduza sobrecarga em termos de latência e consumo de recursos, associada às etapas de validação, consenso e escrita imutável, o sistema mantém elevada confiabilidade operacional, sendo a sobrecarga compensada por garantias de integridade, rastreabilidade e não-repúdio.

No *PIDDF*[7], avaliou-se o tempo de resposta das operações de criação e resolução de DIDs e da autenticação federada, conforme a Figura 8. Os resultados, em escala logarítmica, evidenciam diferenças de ordem de grandeza entre as plataformas, com soluções permissionadas (*Fabric e Besu*) apresentando latências na faixa de milissegundos, enquanto redes públicas (*Ethereum*) atingem tempos na ordem de segundos.

Esses resultados confirmam que mecanismos de identidade *on-chain* impõem maior sobrecarga computacional devido aos custos de consenso, validação distribuída

[5]https://observatorioblockchain.org.br/auditoria-automatizada-em-contratos-inteligentes/

[6]https://observatorioblockchain.org.br/auditoria-e-rastreabilidade-em-redes/

[7]https://observatorioblockchain.org.br/tag/gt-piddf/

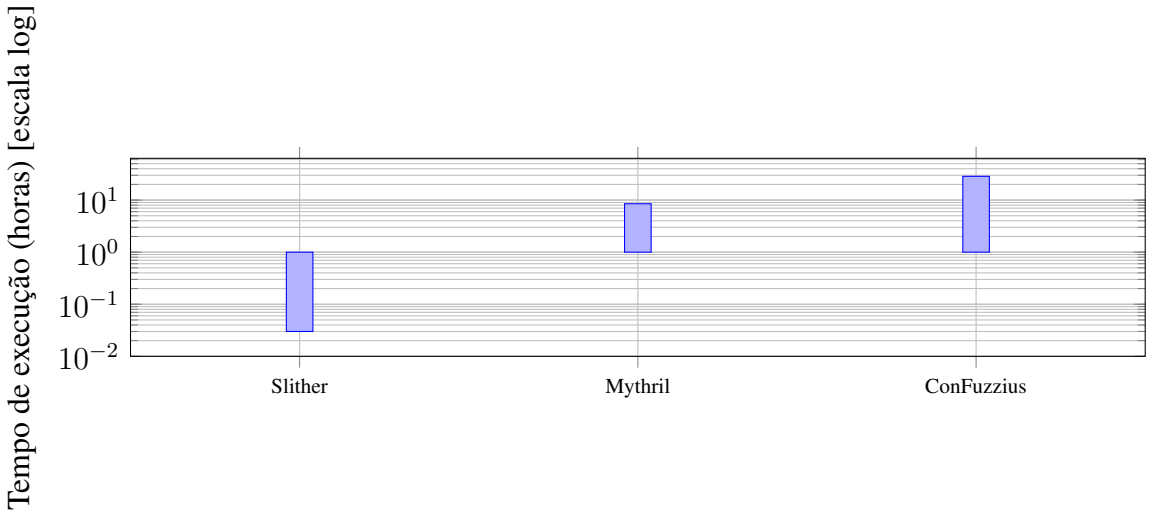

Figura 6. SmartSeg: comparação do tempo de execução entre analisadores em um contrato vulnerável (escala logarítmica).

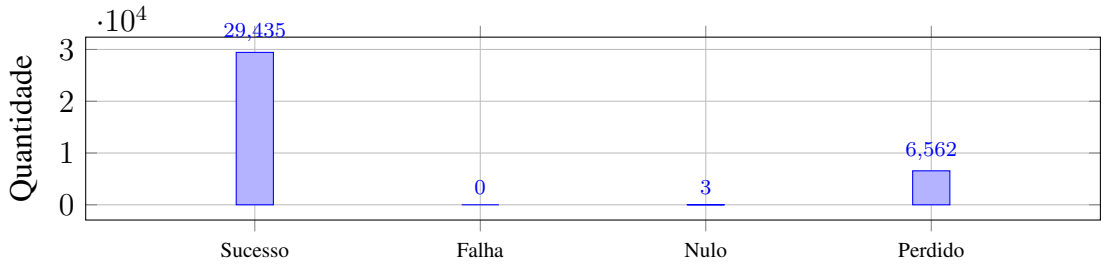

Figura 7. Audita: resultados das sondagens no teste de escalabilidade (36.000 sondas).

e persistência imutável, a qual é compensada por garantias de rastreabilidade, auditabilidade e soberania dos dados.

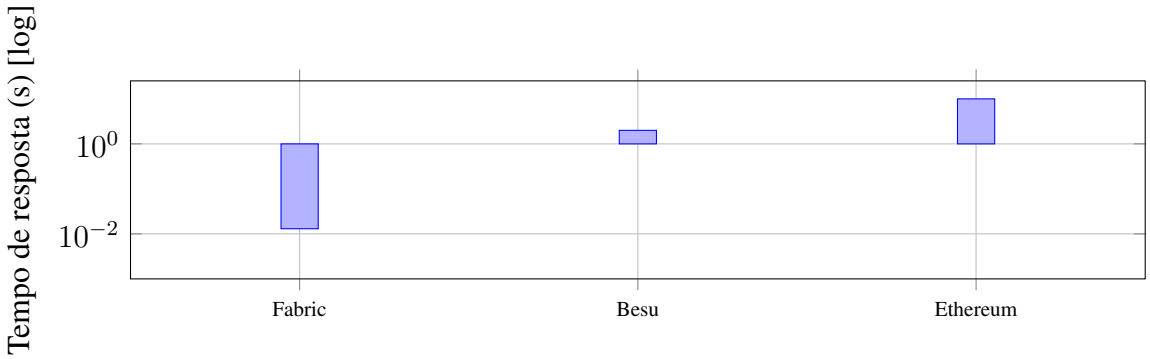

Figura 8. PIDDF: comparação do tempo de resposta entre Fabric, Besu e Ethereum (escala logarítmica).

De forma agregada, essas evidências confirmam que segurança e auditabilidade não são propriedades gratuitas: elas emergem como *trade-offs* explícitos entre custo computacional, desempenho e garantias formais de confiança. Além das métricas clássicas

utilizadas nesta dimensão, introduzimos ainda indicadores compostos que permitem capturar propriedades sistêmicas emergentes de ambientes descentralizados, particularmente associadas à governança, à confiança e ao grau efetivo de descentralização operacional.

O **Índice de Descentralização Operacional (IDO)** é definido como:

$$IDO = \frac{N_{validadores\ ativos}}{N_{total\ de\ nós}} \tag{4}$$

Esse índice expressa o grau efetivo de participação distribuída no processo de consenso, permitindo distinguir arquiteturas formalmente descentralizadas de sistemas com centralização operacional implícita.

O **Custo de Governança Distribuída (CGD)** quantifica a fração de recursos consumida por operações de coordenação e controle:

$$CGD = \frac{TX_{governan\c{c}a}}{TX_{totais}} \tag{5}$$

Essa métrica permite mensurar o impacto operacional de mecanismos de registro, auditoria, identidade e validação institucional sobre a carga total do sistema.

A **Latência de Confiança** mede o tempo entre a ocorrência de um evento real e sua confirmação imutável no livro-razão distribuído:

$$L_{confian\c{c}a} = t_{confirma\c{c}\tilde{a}o} - t_{evento} \tag{6}$$

Essa métrica captura diretamente o custo temporal associado à construção de confiança em ambientes distribuídos.

Por fim, o **Custo Computacional por Operação de Confiança (ECT)** é definido como:

$$ECT = \frac{CPU_{time} + CryptoOps}{N_{trust\ ops}} \tag{7}$$

Esse indicador expressa o esforço computacional médio necessário para sustentar propriedades de confiança, incluindo autenticação, verificação criptográfica e persistência de estado. Em conjunto, essas métricas permitem caracterizar blockchains não apenas como sistemas de processamento de transações, mas como infraestruturas computacionais de confiança distribuída, nas quais desempenho, segurança, governança e criptografia se combinam em um único plano de controle operacional.

5. Agradecimentos

Este trabalho foi realizado com o apoio institucional e financeiro do Projeto ILIADA, em parceria com o CPQD, por meio do Termo de Parceria nº TPA/184/SOFTEX/CPQD. Os autores agradecem ao MCTI (Processo nº 01245.023862/2022-14) pelo fomento, essencial para o desenvolvimento das atividades de pesquisa, inovação e validação tecnológica apresentadas.

6. Conclusão e Trabalhos Futuros

Este trabalho propôs uma metodologia experimental multidimensional para avaliar infraestruturas blockchain, integrando métricas de desempenho, resiliência criptográfica, interoperabilidade, segurança e governança. A validação em seis *testbeds* do Projeto Ilíada permitiu caracterizar essas redes como infraestruturas computacionais de confiança distribuída. Os resultados evidenciam *trade-offs* estruturais inevitáveis: latência, vazão, interoperabilidade e segurança são dimensões fortemente acopladas, inviabilizando otimizações isoladas. O consenso e a criptografia assumem papel central no orçamento computacional, comprovando que propriedades abstratas, como confiança e descentralização, traduzem-se em métricas operacionais sujeitas à degradação sob carga. Contudo, ressalta-se que as conclusões refletem um escopo baseado majoritariamente em redes permissionadas e cargas sintéticas.

Como trabalhos futuros, planeja-se estender a metodologia para blockchains públicas e incorporar métricas energéticas, aspectos econômicos (modelos de incentivo) e *workloads* reais de produção. Esses avanços consolidarão a caracterização sistêmica dessas infraestruturas sociotécnicas de coordenação.

Referências

Atzei, N., Bartoletti, M., and Cimoli, T. (2021). Smart contract risks and security: A systematic survey. *IEEE Transactions on Dependable and Secure Computing*, 18(2):711–727.

Belchior, R., Scuri, S., Silva, A., Nunes, N., and Vasconcelos, A. (2023). A survey on blockchain interoperability: Past, present, and future trends. *ACM Computing Surveys*, 56(3):1–41.

Enaya, A. (2025). Survey of blockchain-based applications for iot. *Applied Sciences*, 15:4562.

Fernandes, D., Sousa, J., and Cerqueira, E. (2022). Post-quantum cryptography in blockchain systems: Challenges and opportunities. *IEEE Communications Magazine*.

Foundation, H. (2024). Hyperledger caliper: Blockchain benchmarking tool. `https://www.hyperledger.org/use/caliper`.

Li, Q., Wang, P., Wang, R., and Zhang, X. (2022). Scalability analysis of pbft-based consensus protocols in permissioned blockchains. *Future Generation Computer Systems*, 132:14–29.

Sinai, N. K. (2024). Performance evaluation of a quantum-resistant blockchain. Empirical evaluation of PQC algorithms (e.g., Falcon) vs classical in blockchain context.

Wang, T., Zhang, K., Wang, J., and Chen, Y. (2024). Blockchain security and privacy: A survey on recent advances and future directions. *ACM Computing Surveys*, 56(4):1–37.

Zhao, J., Chen, Y., and Zhang, K. (2022). A survey on cross-chain communication of blockchain systems. *IEEE Access*.

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., and Wang, H. (2020). An overview of blockchain technology: Architecture, consensus, and future trends. *IEEE Big Data*.