Universidade Federal do Piauí
Centro de Ciências da Natureza
Programa de Pós-Graduação em Ciência da Computação

Análise de Custo e Desempenho de Protocolos para Interoperabilidade de Tokens em Redes Blockchain

Fredison Muniz de Sousa

Número de Ordem PPGCC: M001

Teresina-PI, setembro de 2025

Fredison Muniz de Sousa

Análise de Custo e Desempenho de Protocolos para Interoperabilidade de Tokens em Redes Blockchain

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação da UFPI (área de concentração: Sistemas de Computação), como parte dos requisitos necessários para a obtenção do Título de Mestre em Ciência da Computação.

Universidade Federal do Piauí – UFPI

Centro de Ciências da Natureza

Programa de Pós-Graduação em Ciência da Computação

Orientador: Glauber Dias Gonçalves

Teresina-PI

setembro de 2025

FICHA CATALOGRÁFICA
Universidade Federal do Piauí
Biblioteca Comunitária Jornalista Carlos Castello Branco
Serviço de Processos Técnicos

S725a Sousa, Fredison Muniz de.
Análise de Custo e Desempenho de Protocolos para Interoperabilidade de Tokens em Redes Blockchain / Fredison Muniz de Sousa. – 2025.
43 f. : il.

Dissertação (Mestrado) – Universidade Federal do Piauí, Centro de Ciências da Natureza, Programa de Pós-Graduação em Ciências da Computação, Teresina, 2025.
"Orientador: Glauber Dias Gonçalves."

1. Blockchain. 2. Interoperabilidade. 3. Computação. 4. Mecanismo notarial. 5. Chainlink. 6. CCIP. 7. HTLC. I. Gonçalves, Glauber Dias. II. Título.

CDD 005.74

Bibliotecário: Gésio dos Santos Barros - CRB3/1469

Fredison Muniz de Sousa

Análise de Custo e Desempenho de Protocolos para Interoperabilidade de Tokens em Redes Blockchain

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação da UFPI (área de concentração: Sistemas de Computação), como parte dos requisitos necessários para a obtenção do Título de Mestre em Ciência da Computação.

Documento assinado digitalmente
gov.br
GLAUBER DIAS GONCALVES
Data: 23/10/2025 08:59:47-0300
Verifique em https://validar.iti.gov.br

Glauber Dias Gonçalves (UFPI)
Orientador

Documento assinado digitalmente
gov.br
FRANCISCO AIRTON PEREIRA DA SILVA
Data: 20/10/2025 09:12:33-0300
Verifique em https://validar.iti.gov.br

Professor/Pesquisador
Francisco Airton Pereira da Silva (UFPI)

Documento assinado digitalmente
gov.br
ALEX BORGES VIEIRA
Data: 20/10/2025 15:11:02-0300
Verifique em https://validar.iti.gov.br

Professor/Pesquisador
Alex Borges Vieira (UFJF)

JOSE AUGUSTO MIRANDA
NACIF:03635794600
Assinado de forma digital por JOSE AUGUSTO MIRANDA NACIF:03635794600
Dados: 2025.10.18 06:15:18 -03'00'

Professor/Pesquisador
José Augusto Miranda Nacif (UFV)

Teresina-PI
setembro de 2025

Resumo

A interoperabilidade entre *blockchains* é um dos principais desafios para a consolidação de ecossistemas distribuídos e aplicações descentralizadas. Este trabalho tem como objetivo analisar o custo e o desempenho de protocolos voltados à transferência de *tokens* entre diferentes redes, com ênfase no CCIP (*Chainlink Cross-Chain Interoperability Protocol CCIP)*, que é uma das soluções comerciais de interoperabilidade mais populares e com maior cobertura em redes *blockchain* atualmente. Para tanto, foram conduzidos experimentos em redes *blockchain* de teste, especificamente as redes *Amoy* (da *Polygon*) e *Fuji* (da *Avalanche)*, utilizando o *token CCIP-BnM* padrão ERC-20 no modelo finalização-emissão (i.e., *burn-mint*) origem-destino respectivamente. Os experimentos envolveram 3.478 transações, executadas em intervalos regulares, a fim de mensurar a latência de operações da rede de origem até a rede de destino e custo dessas operações, considerando tarifas das redes que suportam a operação. Os resultados revelam que a escolha da rede de origem de uma operação via CCIP impacta significativamente no desempenho com aumento mediano de latência de 300 segundos, ao passo que essa escolha não tem impactos significativos no custo da operação. Por sua vez, em comparação com outros protocolos, o CCIP apresentou custos significativamente superiores, chegando a US$ 0,78 por operação, e latências até sete vezes maiores quando comparado a alternativas como o mecanismo notarial e o *Hash Time Lock* (HTLC). Conclui-se que, embora o *Chainlink* ofereça robustez e segurança, há espaço para melhorias no desempenho desse protocolo em temos de desempenho e custo, nos quais soluções mais simples podem se mostrar mais eficientes e competitivas no mercado de interoperabilidade de *tokens* em redes *blockchain*.

Palavras-chave: Blockchain; Interoperabilidade; Chainlink; CCIP; HTLC; Mecanismo notarial.

Abstract

Interoperability between blockchains is one of the main challenges for the consolidation of distributed ecosystems and decentralized applications. This work aims to analyze the cost and performance of protocols aimed at transferring tokens between different networks, with an emphasis on CCIP (Chainlink Cross-Chain Interoperability Protocol), which is one of the most popular commercial interoperability solutions with the widest coverage in blockchain networks today. To this end, experiments were conducted on test blockchain networks, specifically the Amoy (Polygon) and Fuji (Avalanche) networks, using the ERC-20 standard CCIP-BnM token in the source-destination finalization-issuance (i.e., burn-mint) model, respectively. The experiments involved 3,478 transactions, executed at regular intervals, in order to measure the latency of operations from the source network to the destination network and the cost of these operations, considering the fees of the networks supporting the operation. The results reveal that choosing the origin network for a CCIP transaction significantly impacts performance, with a median latency increase of 300 seconds, while this choice has no significant impact on transaction costs. In turn, compared to other protocols, CCIP presented significantly higher costs, reaching US$ 0,78 per transaction, and latencies up to seven times higher when compared to alternatives such as the notary mechanism and Hash Time Lock (HTLC). The conclusion is that, although Chainlink offers robustness and security, there is room for improvement in this protocol's performance and cost, where simpler solutions may prove more efficient and competitive in the token interoperability market on blockchain networks.

Keywords: Blockchains; Interoperability; Chainlink; CCIP; HTLC; Notarial mechanism.

Lista de ilustrações

Lista de tabelas

Sumário

1 Introdução

A tecnologia *blockchain*, desde a sua concepção, tem revolucionado diversos setores, oferecendo soluções inovadoras para problemas complexos de segurança, transparência e eficiência. Contudo, com a crescente adoção dessa tecnologia surge a necessidade imperativa de promover a interoperabilidade entre diferentes *blockchains* e Tecnologias de livro-razão distribuída, as DLTs (*Distributed Ledger Technologies*) (BELCHIOR et al., 2021).

A interoperabilidade, no contexto de *blockchain*, refere-se à capacidade de diferentes redes se comunicarem, compartilharem dados e utilizarem informações de forma integrada e eficiente. Considere, por exemplo, um cenário em que um ativo digital tokenizado em uma *blockchain* possa ser facilmente transferido e utilizado em outra, permitindo aplicações como investimentos, comércio ou financiamento de projetos. No entanto, à medida que a tecnologia *blockchain* evolui, a falta de interoperabilidade torna-se um obstáculo significativo, dificultando a colaboração entre redes descentralizadas e limitando a integração de dados, o que impede avanços importantes no ecossistema. (LUCENA HELUAN, 2024).

Um dos principais desafios inerentes à interoperabilidade em *blockchain* é a diversidade das arquiteturas, protocolos de consenso e protocolos de governança que caracterizam diferentes redes. Cada *blockchain* pode operar sob princípios distintos, com variações significativas em termos de projeto, segurança, privacidade e escalabilidade (ALVES et al., 2022). Este cenário fragmentado dificulta a tarefa de desenvolver soluções que permitam uma comunicação fluida e segura entre as diferentes plataformas. Além disso, a ausência de padronização e a falta de protocolos comuns para interoperabilidade aumentam a complexidade para a criação de soluções eficazes e universalmente aceitas.

O problema em questão nesse trabalho é analisar desempenho e custo de protocolos de interoperabilidade em diferentes *blockchains*, haja visto que estes fatores impactam diretamente na viabilidade e escalabilidade de diferentes redes. Protocolos de interoperabilidade podem adicionar taxas como custo da transação ou validação, e até mesmo custos para uso de pontes entre as redes. Esses protocolos não podem afetar negativamente a experiência do usuário, especialmente em casos de uso sensíveis ao tempo, como finanças descentralizadas (DeFi) e transferências de ativos em tempo real. Além disso, precisa de alto desempenho para lidar com um grande número de transações sem impedimento do volume de transações.

A maioria das propostas da literatura que lidam com essa questão, fazem avaliação de novos *frameworks* de aplicações, como é o caso de (ZHU; CHI; LIU, 2023) ou novas soluções de interoperabilidade (GHAEMI et al., 2021). Alguns trabalhos focam na análise

de desempenho individual até de protocolo novo (CAO et al., 2024), mas não avaliam o desempenho e custo da interoperabilidade através de comparativos entre os esquema Notarial e Bloqueio de *Hash* com uma solução já em uso, que é o caso do protocolo *Cross-Chain Interoperability Protocol* (CCIP)[1] da Chainlink.

1.1 Questão de pesquisa

Na constante evolução das tecnologias de *blockchain*, a interoperabilidade surge como um requisito relevante para maximizar o potencial das redes descentralizadas. Ela pode permitir que diferentes redes *blockchain* se comuniquem, troquem informações e realizem transações, ampliando as possibilidades de aplicações e negócios. No entanto, escolher a solução ideal de interoperabilidade requer uma análise criteriosa de diversos fatores.

Nesse sentido, a questão de pesquisa principal que esse trabalho busca responder é *como avaliar as principais soluções existentes para interoperabilidade entre redes blockchains na transferências de ativos (i.e., tokens), visando orientar usuários finais e desenvolvedores de aplicações sobre métricas e valores de referência da eficiência e impacto dessas soluções?*

Nessa dissertação, focamos nos fatores *desempenho* e *custo* e argumentamos que eles são de suma importância para guiar usuários e desenvolvedores de aplicações na avaliação da eficiência de protocolos de interoperabilidade.

Em termos de decisão estratégica, a análise de *custo* envolvidos é fundamental. No caso de soluções de interoperabilidade, é essencial entender as tarifas envolvidas em uma transação para transferir ativos (i.e., *tokens*) de uma rede *blockchain* de origem para outra rede *blockchain* de destino. Uma solução pode aparentar ser financeiramente viável inicialmente, mas seu custo pode se tornar proibitivo com o aumento do volume de transações. Logo, avaliações de custo em sistemas computacionais precisam ser amplas e conservadoras, considerando análises estatísticas dos custos de todas as partes envolvidas em uma transação que requer operabilidade de redes.

A interoperabilidade adiciona uma camada extra de complexidade às operações de redes *blockchain*, o que pode impactar no *desempenho* e das redes. O desempenho é um critério decisivo na escolha da solução ideal. A capacidade de lidar com grandes volumes de transações de forma rápida pode ser o diferencial entre o sucesso e o fracasso de um projeto. Portanto, a solução ideal, além de baixo custo, deve ter alto desempenho, ou ao menos minimamente aceitável para execução de operações. No caso de interoperabilidade, o tempo de conclusão de uma transação é uma forma prática de medir desempenho, permitindo análises estatísticas explorando várias abordagens da literatura (BOUDEC, 2022).

[1] https://docs.chain.link/ccip/concepts/cross-chain-tokens

1.2 Objetivos

O objetivo principal deste trabalho é avaliar a eficiência das principais soluções existentes para interoperabilidade entre redes blockchains em operações de transferências de tokens, visando orientar usuários finais e desenvolvedores de aplicações no conhecimento sobre os melhores valores de custo e desempenho alcançáveis por essas soluções atualmente.

Com base no objetivo geral definido, os seguintes objetivos específicos foram traçados:

- Desenvolver uma metodologia que permita avaliar de forma sistemática e reprodutível experimentalmente custo e desempenho de interoperabilidade em redes *blockchain*;
- Construir um ambiente experimental que viabilize a metodologia proposta, considerando a execução das soluções de interoperabilidade alvos do estudo de forma realista;
- Quantificar os custos em interoperabilidade entre redes *blockchain* considerando tarifas dessas redes;
- Quantificar desempenho em interoperabilidade entre redes *blockchain*, considerando tempo de execução de transações.
- Identificar protocolos que possam ser comparáveis ao protocolo CCIP em termos de custo e desempenho para a interoperabilidade entre redes *blockchain*;
- Identificar os principais fatores que impactam no custo e desempenho dos protocolos de interoperabilidade avaliados;

1.3 Contribuições e Organização da Dissertação

Neste trabalho buscamos preencher uma lacuna da literatura quanto a metodologias para avaliar soluções de interoperabilidade em redes blockchain e conhecer seus valores de referência em termos de custo e desempenho. Nesse sentido, apresentamos as seguintes contribuições:

1. Metodologia para comparar protocolos de interoperabilidade baseado em ambiente realista para aplicações descentralizadas;
2. Análise de aspectos de desempenho e custo de protocolos de modo a orientar usuários e desenvolvedores dessas aplicações a escolherem o compromisso entre ambos os aspectos.

Nesse sentido, implantamos três mecanismos de interoperabilidade em um ambiente realista, baseado em redes de testes *blockchains*. Em seguida, implementamos contratos inteligentes nesses mecanismos para operar transferência de *tokens* entre redes distintas nesse ambiente. Por fim, mensuramos os tempos e valores de tarifas dessas operações e mostramos a analise de desempenho e custo de interoperabilidade.

As contribuições e resultados acima elencados estão nos artigos técnicos abaixo, que foram apresentados em conferências e submetidos em jornais científicos especializadas no tema:

- Muniz, Fredison et al. Análise de Custo e Desempenho de Protocolos para Interoperabilidade de Tokens em Redes Blockchain. Workshop em Blockchain: Teoria, Tecnologias e Aplicações (WBlockchain). SBC, 2025. p. 1-14.
- Mendonça, Ronan et al. Performance and Cost Analysis of Protocols for Token Interoperability in Blockchain Networks. IEEE Internet Communication Magazine (artigo em colaboração com grupo de pesquisa e sob revisão)

Os próximos capítulos estão organizados como segue: No Capítulo 2, apresentamos o referencial teórico, e os trabalhos relacionados estado da arte na área de pesquisa. A metodologia utilizada para a análise é apresentada no Capítulo 3, ao passo que os resultados são apresentados no Capítulo 4. Finalmente, o Capítulo 5 expõe as considerações finais e trabalhos futuros.

2 Referencial Teórico

Neste capítulo, apresentamos os fundamentos teóricos que embasam esta pesquisa, com ênfase nos conceitos relacionados à tecnologia *blockchain* e à interoperabilidade entre diferentes redes. Primeiramente, discutimos os princípios básicos das *blockchains*, suas características estruturais e os mecanismos de consenso mais utilizados (Seção 2.1). Em seguida, abordamos os definições de contratos inteligentes e *tokens*, que são características fundamentais das redes *blockchain* (Seção 2.2). Continuamos com as principais abordagens existentes para interoperabilidade (*Chainlink*, HTLC e Notarial (Seção 2.3). Por fim, mostramos o estado da arte de interoperabilidade de *blockchain*, (Seção 2).

2.1 Blockchain

A tecnologia *blockchain* é definida como um livro-razão (*ledger*) distribuído e P2P (*peer-to-peer*), no qual as transações individuais são encadeadas e posteriormente agrupadas em blocos interligados. Essa estrutura confere à tecnologia características fundamentais, como descentralização, imutabilidade, integridade dos dados e transparência.

A popularidade da tecnologia *blockchain* (BCT) cresceu especialmente com o sucesso do Bitcoin, que demonstrou seu potencial como uma solução eficaz para revolucionar modelos de negócios, reduzir riscos e aprimorar o gerenciamento de dados. Estima-se que os gastos globais em soluções baseadas em *blockchain* alcancem 17,9% até 2024, com uma taxa de crescimento anual composta de 46,4% (DENTER; SEEGER; MOEHRLE, 2023).

Na estrutura de uma *blockchain*, os blocos são unidades fundamentais de armazenamento que contêm um conjunto de transações válidas, além de metadados, como o valor de *hash* do bloco anterior, um carimbo de tempo (*timestamp*) e um valor chamado *nonce*. As transações representam registros digitais de operações — por exemplo, transferências de ativos, execução de contratos inteligentes ou troca de informações — que são validadas e incluídas na cadeia de blocos. O *nonce* (*number used once*) é um número aleatório utilizado no processo de mineração para gerar um *hash* que satisfaça as condições de dificuldade impostas pela rede, garantindo a segurança e o controle do processo de validação de novos blocos.

A Figura 1 ilustra um exemplo de *blockchain* contendo algumas transações. Essa estrutura torna o sistema resistente a adulterações, pois qualquer modificação em um único bloco invalidaria os valores de *hash* daquele bloco e de todos os subsequentes. Assim, alterar dados em uma *blockchain* exigiria o recálculo dos *hashes* de todos os blocos a partir da alteração. Em uma *blockchain* centralizada, esse processo seria possível, ainda

que custoso; entretanto, em uma rede distribuída P2P, qualquer modificação requereria o consenso da maioria dos participantes, o que torna a manipulação praticamente inviável (TOSIC, 2024).

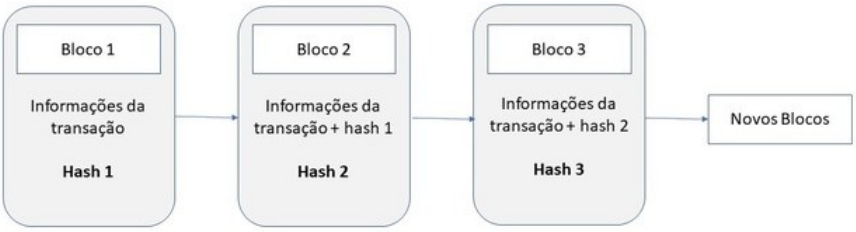

Figura 1 – Blockchain composta de blocos vinculados por valores de hash.

Segundo (LI; WU; CUI, 2023), com o desenvolvimento rápido da sociedade, a tecnologia *blockchain* tem se mostrado de forte potencial em muitas áreas, como Medicina, Finanças, Proteção de privacidade, indústrias relacionadas a cadeia de suprimentos, a indústria aeroportuária, indústria de alimentos.

2.2 Contratos Inteligentes e Tokens

Uma série de novas tecnologias ganharam vida após o surgimento das *blockchain*. Entre elas estão os contratos inteligentes, pedaços de códigos de computador que podem ser usados para emissão de *tokens*, construção de corretoras e até mesmo acordos no mercado imobiliário. Os contratos inteligentes (*smart contracts*) rodam em uma *blockchain*, e todas as cláusulas contidas neles são gravadas nessa rede. Uma vez que as regras, obrigações e penalidades são inseridas, os contratos são executados de forma automática conforme aquilo que foi combinado. O papel da *blockchain*, portanto, é garantir que esses acordos aconteçam de forma segura e verificável, e sem manipulação para benefício próprio. (Infomoney (2022)). Em comparação aos contratos convencionais, os contratos inteligentes conseguem reduzir o risco de transação, os custos de administração e serviço, além de aumentar a eficiência dos processos corporativos, uma vez que são frequentemente colocados e protegidos por *blockchain* (ZHENG et al., 2020)

De acordo com (TAHERDOOST, 2023), contratos inteligentes são simplesmente contêineres de código que encapsulam e replicam os termos de contratos do mundo real no domínio digital. Contratos são fundamentalmente um acordo juridicamente vinculativo entre duas ou mais partes, com cada parte comprometida a cumprir seus compromissos. É importante ressaltar que o acordo deve ser executável por lei, geralmente por meio de um órgão legal centralizado (organização). No entanto, contratos inteligentes substituem terceiros ou mediadores confiáveis entre as partes contratantes. Eles fazem uso disso com a assistência da execução de código que é automaticamente disseminada e verificada por nós de rede em um *blockchain* descentralizado.

Cada contrato tem código e armazenamento, além de endereço de conta, valor e *nonce* que também estão presentes para as contas de propriedade externa. A definição de um contrato inteligente tem dois componentes. O estado do contrato é definido especificando as variáveis de estado e seus tipos, e a estrutura dos eventos que podem ser emitidos por este contrato inteligente durante a execução do código. O segundo componente define pelo menos um construtor e as funções que podem ser acionadas enviando mensagens para o contrato. O construtor é chamado em um tipo especial de transação usado para criação de contrato e é responsável por inicializar e salvar as variáveis de estado no armazenamento do contrato. As funções podem alterar o estado do contrato atualizando as variáveis de estado e criando ou enviando mensagens para outras contas. Além da mensagem retornada, elas também podem emitir eventos.

Mais especificamente, um contrato inteligente é um programa de computador escrito em uma linguagem de alto nível, como ilustrado no Algoritmo 2.1, adaptado de (PALMA; MARTINA; VIGIL, 2022), que exemplifica um contrato inteligente escrito em Solidity. O contrato é chamado de `C` e possui uma variável de estado chamada de `nome` do tipo `bytes32` e duas funções. A função `get` recebe um parâmetro `_nome` e o atribui à variável `nome`, alterando o estado do contrato. A função `set` retorna o valor atual de `nome` sem modificar o estado, pois é marcada como `view`. O contrato demonstra operações básicas de leitura e escrita na *blockchain*, e a linha `pragma solidity >=0.7.0 <0.9.0;` especifica a versão do compilador compatível. Note que, após ser desenvolvido e testado, um contrato necessita ser implantado, ou seja, registrado de forma imutável, na *blockchain*.

```
1  // SPDX-License-Identifier: GPL-3.0
2  pragma solidity >=0.7.0 <0.9.0;
3
4  contract C{
5      bytes32 nome;
6      function get(bytes32 _nome) public{
7       nome = _nome;
8     }
9      function set() public view returns (bytes32) {
10      return nome;
11    }
12 }
```

Algoritmo 2.1 – Exemplo de código fonte de contrato inteligente tomando com referência a linguagem Solidity Ethereum, adaptado de (PALMA; MARTINA; VIGIL, 2022).

O contrato implantado na *blockchain*, junto com suas respectivas aplicações clientes, que transmitem as requisições dos usuários, constitui o que é conhecido como aplicação descentralizada ou DApp. Para interagir com o DApp, é necessário submeter uma transação à *blockchain*, especificando o endereço do contrato e a função desejada.

Conforme ilustrado na Figura 2 proposta por (PALMA; MARTINA; VIGIL, 2022), uma vez que o contrato inteligente é implantado, como demonstrado no bloco B_i pela transação *deploy* C, os usuários podem interagir com ele em blocos subsequentes, como B_{i+1} e B_{i+2}, através de funções específicas do contrato, como *get()* e *set(true)*. Essas interações são realizadas por meio de uma aplicação cliente conectada à rede *blockchain*, equipada com as interfaces de comunicação necessárias para enviar as transações, garantindo que as operações programadas sejam executadas e registradas de forma imutável na *blockchain*.

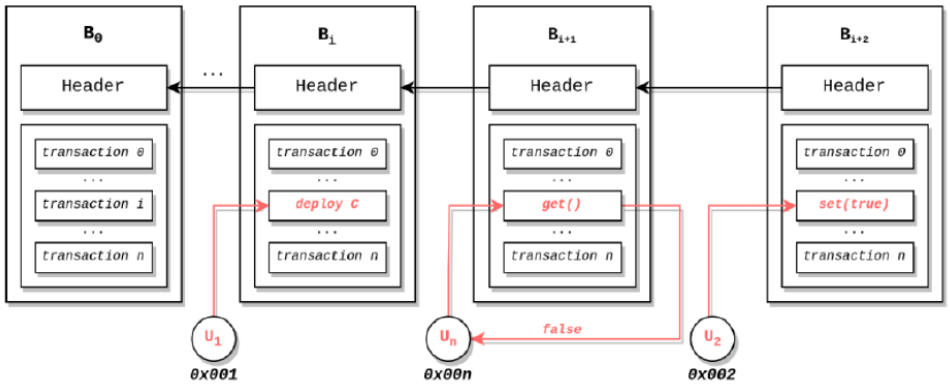

Figura 2 – Exemplo de execução de uma transação que modifica um estado definido pelas variáveis programadas no contrato (PALMA; MARTINA; VIGIL, 2022).

As principais propriedades de segurança dos contratos inteligentes e da *blockchain* são descentralização, transparência e imutabilidade. A descentralização é garantida pela replicação da *blockchain* em uma rede de pares (P2P), onde cada nó mantém uma cópia completa do histórico de transações. Essa estrutura descentralizada distribui o poder de decisão entre todos os participantes da rede, eliminando a possibilidade de controle centralizado e tornando o sistema resistente a falhas e ataques. Mesmo que alguns nós sejam comprometidos, a integridade da *blockchain* permanece intacta, pois a maioria dos nós segue as regras de consenso estabelecidas.

A transparência é assegurada pelo fato de que todas as transações e contratos registrados na *blockchain* são públicos e auditáveis por qualquer pessoa. Isso cria um ambiente em que todas as operações são visíveis e verificáveis, reduzindo significativamente o risco de fraudes ou manipulações. A transparência não apenas promove a confiança entre os usuários, mas também facilita a auditoria e a conformidade regulatória, elementos essenciais para a aceitação da tecnologia *blockchain* em sistemas mais amplos. A imutabilidade, garantida pelo uso de *hash* criptográficos, assegura que uma vez que um bloco é adicionado à *blockchain*, ele não pode ser alterado sem modificar todos os blocos subsequentes. Isso torna as transações e os contratos registrados permanentes e inalteráveis, garantindo a integridade dos acordos realizados. A imutabilidade elimina a possibilidade de alterações retroativas nos registros, garantindo que os dados armazenados permaneçam confiáveis ao longo do tempo.

Essas três propriedades — descentralização, transparência e imutabilidade — combinadas fornecem um ambiente seguro e confiável para a execução de contratos inteligentes. Eles não apenas aumentam a eficiência das transações, mas também democratizam o acesso a serviços financeiros e jurídicos, permitindo que indivíduos e organizações em qualquer parte do mundo participem de mercados globais de forma segura e eficiente.

Os *tokens* podem ser definidos de forma simplificada no contexto de redes *blockchain* como um objeto digital registrado na *blockchain*. Um *token* está associado a um usuário, que é o seu proprietário, e somente este pode transferir a propriedade do *token* a outro usuário. Isso garante a possibilidade de valor ao *token*, i.e., a sua escassez ou impossibilidade de posses duplicadas (gasto duplo). Diferentemente de objetos digitais tradicionais da web, o *token* sempre tem um proprietário. A ideia geral de *tokens* é tornar bens (i.e., ativos) tangíveis ou intangíveis mais acessíveis, assim como as transferências ou negociações desses ativos mais eficientes, assim um ativo do mundo real (dito tokenizado) pode ser representado na *blockchain* por um *token*, e uma transação que altere a propriedade deste *token* no livro-razão corresponderia a própria mudança de propriedade do ativo em si.

No contexto de Finanças Descentralizadas os *tokens* desempenham um papel central, atuando como objetos digitais registrados em uma *blockchain*. Esses *tokens* podem ser fungíveis ou não fungíveis, cada um com suas características e funcionalidades específicas. De forma simplificada, um *token* pode ser entendido como uma representação digital de um ativo, seja ele tangível ou intangível. Cada *token* é associado a um proprietário, e apenas este pode transferir sua propriedade a outro usuário, o que assegura a escassez e a impossibilidade de duplicações, evitando o problema do "gasto duplo". Essa propriedade exclusiva torna os *tokens* valiosos dentro do ecossistema *blockchain*.

A ideia geral dos *tokens* é tornar ativos mais acessíveis e facilitar as transferências ou negociações desses ativos de maneira eficiente e segura. Por exemplo, um ativo do mundo real pode ser representado na *blockchain* por um *token*, e a transação que altera a propriedade desse *token* refletirá a mudança de propriedade do próprio ativo no mundo real. Esses *tokens* podem ser transferidos globalmente em questão de segundos e podem ser utilizados por diversas aplicações descentralizadas, desde que estejam vinculados a contratos inteligentes que controlam sua emissão e transferência.

2.3 Protocolos de Interoperabilidade

Blockchain é considerado um sistema emergente, por conta disso, não há uma definição padronizada para Interoperabilidade de *blockchain* (REN et al., 2023). De acordo com (WANG, 2021) interoperabilidade entre *blockchain* refere-se a como diferentes *blockchain* se comunicam entre si ou como partes disjuntas de um blockchain realizam transações. Vitalik Buterin (fundador da Ethereum), listou três operações primárias em interoperabili-

dade de *blockchain*, da seguinte forma: (I) “mover ativos de uma plataforma para outra”, (II) “esquemas de pagamento contra pagamento e pagamento contra entrega”, e (III) “ acessando informações de uma *blockchain* dentro de outra”, (BUTERIN, 2016). Segundo (BESANÇON; SILVA; GHODOUS, 2019), a interoperabilidade da *blockchain* funciona em três níveis diferentes: (I) interoperabilidade entre diferentes *blockchain*, (II) interoperabilidade entre dApps (aplicativos descentralizados) rodando na mesma *blockchain*, e (III) interoperabilidade entre *blockchain* e outros sistemas, como plataformas de pagamento internacionais.

A definição de protocolo de interoperabilidade ainda é algo subjetivo, pois o termo vem sendo utilizado para definir qualquer método, ecossistema ou ambiente que facilite ou realize a transferência de informações entre *blockchain*. Nesse trabalho tratamos como protocolo de interoperabilidade os mecanismos e técnicas que podem ser usadas para alcançar a interoperabilidade entre *blockchain*. Desses protocolos, os mais referenciados são: *Sidechains, Hash Time Locks* (HTLCs) e Esquemas Notariais. No trabalho de (REN et al., 2023), definiram por destacar mais dois protocolos, o *Relays* e Protocolos Agnósticos *blockchain*.

2.3.1 Protocolo Chainlink - CCIP

Chainlink (LINK) é uma plataforma de *blockchain* que busca facilitar o uso dos contratos inteligentes entre diferentes plataformas. Criado por Sergey Nazarov em 2017, o sistema tem uma arquitetura composta por dois elementos principais: a infraestrutura *on-chain*, representada pelos contratos inteligentes implantados no *blockchain*, e a infraestrutura *off-chain*, formada por nós de oráculos que operam fora da cadeia. Os contratos *on-chain* funcionam como coordenadores, recebendo solicitações de dados externos e agregando as respostas dos oráculos, garantindo a transparência e a verificabilidade do processo. Já os nós *off-chain* conectam-se a diferentes fontes de informação do mundo real, como APIs financeiras, serviços web, sensores e até mesmo sistemas legados, coletando e transmitindo esses dados para o ambiente *on-chain*. Nesse contexto, os oráculos desempenham papel central, atuando como intermediários descentralizados que fornecem informações seguras, auditáveis e resistentes a manipulações (JUELS; NAZAROV; ELLIS, 2017). Diferentemente de um oráculo centralizado, cuja falha ou comprometimento poderia colocar em risco a confiabilidade dos contratos inteligentes, a rede *Chainlink* distribui essa função entre múltiplos nós, utilizando mecanismos de consenso e incentivos econômicos para assegurar a integridade das informações. Dessa forma, os oráculos ampliam significativamente as possibilidades de aplicação dos contratos inteligentes, permitindo que interajam de maneira confiável com eventos e dados do mundo real (CONG; HE, 2019).

A Figura 3 ilustra a arquitetura e o funcionamento do *Chainlink*, mostrando como ele se conecta a diversas fontes de dados externas para oferecer uma solução de

interoperabilidade. O mecanismo de interoperabilidade do *Chainlink*, ou seja, o Protocolo de Interoperabilidade entre Cadeias (CCIP), adota uma arquitetura multicamadas. Ele se baseia em dois componentes principais fora da cadeia: 1) um DON de Confirmação (Redes Oracle Descentralizadas), que observa e atesta eventos na *blockchain* de origem; e 2) um DON de Execução, que verifica os dados e executa a entrega à *blockchain* de destino. Além disso, há uma Rede de Gerenciamento de Riscos (RMN - *Risk Management Network*), que supervisiona as operações em ambas as cadeias, garantindo a conformidade com os comportamentos esperados do sistema. Embora a separação entre os componentes aumente a segurança, ela também contribui para uma maior latência no processamento de transações.

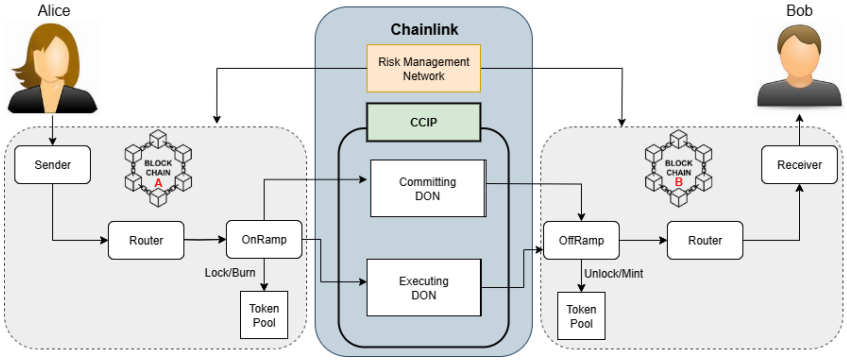

Figura 3 – Arquitetura e funcionamento do Chainlink.

A Figura 3 mostra a arquitetura do protocolo CCIP para o cenário em que Ana, na *blockchain* A, transfere seus *tokens* para Bob, na *blockchain* B. Observe que cada *blockchain* possui seu próprio Roteador CCIP (um contrato inteligente), que atua como uma interface entre a aplicação local e o protocolo. Nesta etapa, os dados são preparados e enviados para os componentes do oráculo *off-chain* do CCIP. Logo após o Roteador está o componente *OnRamp*, que bloqueia ou queima *tokens*, atuando como uma ponte de entrada para o sistema. Os *tokens* são armazenados no *Token Pool*, onde permanecem até que a transação seja processada. Em seguida, a rede Commiting DON verifica e confirma a validade da mensagem e gera uma mensagem de commit assinada. Essa mensagem aciona o DON Executing, que é responsável por entregar a mensagem e/ou *tokens* à *blockchain* de destino. Todas essas etapas são supervisionadas pela Rede de Gerenciamento de Risco, que pode pausar o protocolo se detectar falhas ou comportamento suspeito. Na *blockchain* de destino, o componente *OffRamp* atua como uma ponte de saída, por meio da qual os *tokens* armazenados no *Token Pool* são desbloqueados ou cunhados. Finalmente, o Roteador local entrega a mensagem ou *token* ao contrato da aplicação final.

2.3.2 Hash Time Lock

O bloqueio de *hash* é um mecanismo que aproveita a natureza unidirecional e de baixa colisão das funções *hash* e as combina com atraso na execução de transação na

blockchain, também conhecidos como acordos de bloqueio de tempo de *hash* (HTLAs). Um lado da transmissão entre cadeias gera um quebra-cabeça através de uma função *hash*, a publica na cadeia e define um horário a trancar. Qualquer um que consiga resolver o quebra-cabeça dentro do prazo obtém a promessa de transação, caso contrário, ela falha. HTLAs, Implementam a troca de ativos bloqueando ativos e definindo condições de tempo e desbloqueio correspondentes para garantir a atomicidade. No modelo *cross-chain hash-lock*, assumimos que o mecanismo pode ser projetado e implementado adequadamente ao mesmo tempo que é seguro e confiável o suficiente para permitir a transferência e troca de ativos durante interações entre cadeias, bem como para garantir a proteção eficaz de dados e ativos durante interações *cross-chain*. O bloqueio *hash* tem a vantagem de alta segurança, mas seus cenários de uso são limitados, suportando apenas troca de ativos ou informações, mas não transferência de ativos ou informações, e vulnerável a um grande número de mensagens de transação de spam bloqueando a comunicação do nó, levando à falha de transação de tempo limite (LI; WU; CUI, 2023).

Na arquitetura do protocolo de bloqueio de *hash*, é necessário o uso de contratos inteligentes, ou seja, o contrato é responsável pela troca segura dos ativos. Para isso acontecer, o contrato é implantado nas duas *blockchains* e possui a tarefa de conectá-las. O contrato inteligente atua sincronizando as redes no que diz respeito a verificação das transações, da palavra secreta e a devolução dos valores, caso necessário. Vale ressaltar que neste tipo de protocolo não se usa um terceiro confiável, o contrato HTLC possui as funcionalidades de bloquear os fundos que serão transferidos, registrar o horário da transação e exigir uma palavra secreta no momento da retirada dos fundos para o destinatário da segunda rede. Se por algum motivo o tempo de bloqueio expire, o contrato é capaz de reverter todo o processo, conforme a definição do mecanismo.

O uso dos HTLCs, no entanto, não é isento de limitações. Sua aplicação em transações *off-blockchain* pode enfrentar problemas de escalabilidade e latência, especialmente em redes com um grande volume de operações simultâneas, como na *Lightning Network do Bitcoin*. Além disso, a necessidade de um prazo específico para a conclusão da transação pode ser desafiadora em ambientes com alta volatilidade, pois o valor dos ativos pode mudar significativamente dentro da janela de tempo imposta. Estudos recentes exploram formas de aprimorar a eficiência e a segurança dos HTLCs, investigando alternativas e extensões que possam reduzir esses desafios enquanto mantêm a confiança descentralizada e a segurança criptográfica. (INTEROPERABILITY. . . , 2023).

A Figura 4 ilustra o processo do HTCL, demonstrando como os dois mecanismos funcionam juntos para garantirem a segurança e a atomicidade da transação.

No contexto do mecanismo de bloqueio de *hash*, conforme a Figura 4, o *Usuário A* deseja fazer a transferir seu *token* para uma conta do *Usuário B* em outra rede. Para fazer essa transferência, ele escolhe uma “palavra secreta”, e utiliza o *Hash* juntamente com o

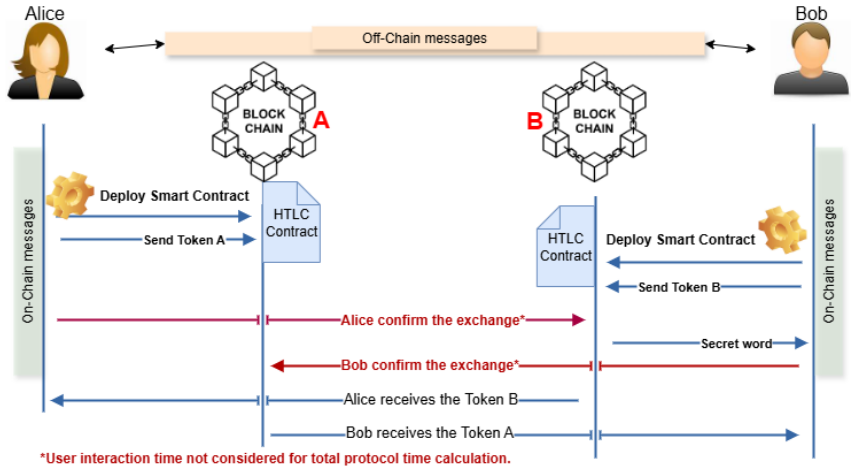

Figura 4 – Arquitetura implementada do Mecanismo Hash-Time Lock.

endereço de B para criar o contrato HTLC. Por meio do contrato criado na *Blockchain A*, ele bloqueia o *Token A* para a transferência ser realizada. De maneira similar, o *Usuário B* implanta o HTLC na *Blockchain B* com o endereço de A e a palavra secreta em *Hash*. Sendo assim, o *Usuário A* faz a retirada (*withdraw*) do *Token B* na *Blockchain B* com sua palavra secreta. Ao fazer isso, a palavra secreta pode ser usada pelo *Usuário B* para retirar o *Token A* da *Blockchain A*.

2.3.3 Esquema notarial

O mecanismo notarial é considerado a maneira mais simples de realizar operações entre cadeias, pois um terceiro confiável ou um grupo de partes é responsável por testemunhar eventos em uma cadeia (por exemplo, Cadeia A) e afirmar que o evento é válido para outra cadeia (por exemplo, Cadeia B). O sistema notarial pode fornecer infraestrutura (por exemplo, nós de mineração) e serviços (por exemplo, monitoramento de eventos) para facilitar a transferência de ativos e a troca de dados. No caso de transferência de ativos, um notário pode emitir um ativo na *blockchain* "A", após verificar uma transação de bloqueio ou queima que ocorreu na *blockchain* "B". Um esquema notarial pode servir como um único notário (esquema notarial centralizado) ou um consórcio de notários (regime notarial descentralizado) (REN et al., 2023) Os esquemas notariais estão mais próximos de plataformas confiáveis de terceiros que permitem a troca de ativos ou de dados entre várias *blockchain*, em contraste com as cadeias laterais indexadas federadas (**federated pegged sidechains**). Na arquitetura deste mecanismo, os usuários envolvidos na transferência de *tokens* devem interagir com o notário. Essa interação pode ocorrer por meio de dApps (aplicativos descentralizados executados em *blockchain*) ou contratos inteligentes, com o domínio de um terceiro confiável. O notário desempenha o papel de receptor do *token* do usuário A (remetente) na *blockchain* A, transferindo-o para o usuário B (destinatário) na *blockchain* B e registrando informações sobre as transações realizadas. O notário deve

garantir a entrega segura dos recursos ao destinatário designado.

A simplicidade e facilidade de implementação tornam os esquemas notariais atrativos, especialmente em soluções centralizadas e *exchanges* de criptomoedas, onde são amplamente utilizados para garantir a interoperabilidade entre redes como Bitcoin e Ethereum (WU et al., 2023). No entanto, essa abordagem tem desvantagens significativas, principalmente porque a confiança é centralizada em uma única entidade. Se o notário falhar, agir de maneira desonesta ou for comprometido, todo o processo pode se tornar inseguro, introduzindo um "ponto único de falha", um dos maiores problemas para esse tipo de sistema (HAUGUM et al., 2022).

Para mitigar os riscos associados à centralização, avanços recentes propuseram o uso de múltiplas assinaturas e assinaturas em grupo. Isso permite que vários notários participem da validação de uma transação, distribuindo a responsabilidade e reduzindo o risco de comprometimento de um único agente (WU et al., 2023). Alguns estudos apontam, inclusive, para o desenvolvimento de esquemas notariais resistentes a ataques quânticos, utilizando assinaturas criptográficas pós-quânticas. (YI, 2023) Propõe o uso de assinaturas multivariadas para assegurar a segurança em cenários onde computadores quânticos possam comprometer sistemas criptográficos tradicionais.

Na prática, os esquemas notariais têm uma vasta aplicação, desde a facilitação de transferências de criptomoedas entre *blockchaisn*, até sistemas de *supply chain*, onde a verificação de dados entre redes é necessária para garantir a autenticidade e integridade de informações (HAUGUM et al., 2022). Eles também são utilizados em contratos inteligentes e sistemas de votação eletrônica, onde a interoperabilidade entre diferentes redes pode ser crucial para assegurar que os dados sejam processados corretamente em ambientes distribuídos.

Embora os esquemas notariais ainda enfrentem desafios relacionados à centralização e confiança, eles continuam a desempenhar um papel fundamental no avanço da interoperabilidade *cross-chain*, permitindo que diferentes *blockchains* se comuniquem de forma mais eficiente e segura (YI, 2023) (WU et al., 2023). As melhorias tecnológicas em andamento visam equilibrar esses desafios, buscando uma maior descentralização e segurança no processo (HAUGUM et al., 2022).

A Figura 5 evidencia a estrutura do esquema notarial onde a mesma é dividida em camadas, a foto foi retirada do trabalho feito por (MENDONçA et al., 2024).

Na arquitetura deste mecanismo, os usuários envolvidos na transferência de *tokens* devem interagir com o notário. Essa interação pode ocorrer por meio de *dApps* (aplicativos descentralizados executados em *blockchain*) ou contratos inteligentes, com o domínio de um terceiro confiável. O notário desempenha o papel de receptor do *token* do usuário A (remetente) na *blockchain* A, transferindo-o para o usuário B (destinatário) na *blockchain*

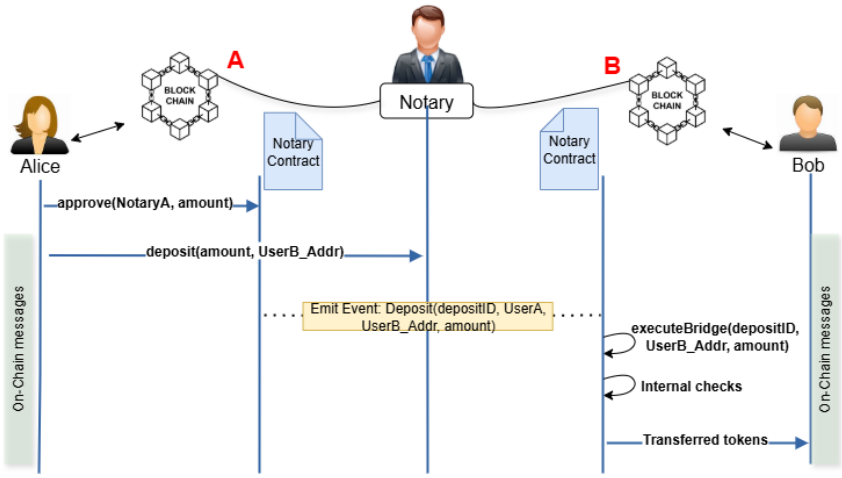

Figura 5 – Estrutura do Esquema Notarial.

B e registrando informações sobre as transações realizadas. O notário deve garantir a entrega segura dos recursos ao destinatário designado.

2.4 Estado da Arte

A interoperabilidade de redes *blockchain* é um tópico de pesquisa recente com oportunidades de contribuições novas tanto para a academia quanto para a indústria. Atingir um avanço prático e significativo de usabilidade de *blockchain* depende de técnicas e soluções bem distintas. Seja interoperabilidade baseada em cadeia, ponte ou dApp, muitas interrogações estão pendentes.

No trabalho de Wang (2021), uma revisão sistemática sobre os avanços e desafios na interoperabilidade entre *blockchains* foi apresentado. Os autores também abordam questões como diferenças estruturais entre transações e os desafios de manter propriedades de consistência e isolamento (ACID - Atomicidade, Consistência, Isolamento e Durabilidade) em operações entre redes distintas. Nesse artigo, são discutidas ainda, soluções práticas, como *atomic swaps* e protocolos de comunicação *cross-chain*.

O trabalho de Mendonça et al. (2024), faz um comparativo entre os métodos e custo de interoperar *tokens* ERC-20 dos protocolos (mecanismos) de interoperabilidade Notarial e o Bloqueio de *hash*. Nos experimentos, os autores monitoraram duas métricas de rede de ambos os mecanismos (Gas - necessário para realizar as transações e o tempo gasto para efetivá-las), nas redes *blockchains* de origem e destino em cada uma das fases dos mecanismos. A avaliação está focada em comparar o desempenho dos métodos Notarial e Bloqueio de *hash*.

Já o trabalho de (BELLAVISTA et al., 2021) propõe mais uma solução de interoperabilidade através de um esquema de retransmissão baseado em *Trusted Execution Environment - TEE* para fornecer melhores garantias de segurança. Os autores presentam

também um protótipo que mede a latência e avalia o impacto de interações entre redes *blockchains*. Atualmente já existem várias soluções de interoperabilidade em uso, e isso não quer dizer que outras propostas não são bem-vindas, mas os testes do trabalho só consideraram a latência da solução de interoperabilidade entre as plataformas, Hyperledger Fabric e Sawtooth.

O trabalho de Cao et al. (2024), propõem o protocolo MAP (sigla não especificada pelos autores), que usa o mecanismo *Relay chains* para interoperabilidade entre redes *blockchain*, destacando soluções baseadas em *zk-proofs* para melhorar a eficiência e reduzir custos. O trabalho justifica a criação do protocolo MAP, devido aos altos custos de transações *on-chain e off-chains* e problemas de escalabilidade dos protocolos existentes, mas não mostra dados que fundamentem tais deficiências.

Em Zhu, Chi e Liu (2023), são abordados os desafios de interoperabilidade e propõe frameworks baseados em sidechains e pontes cross-chain. Para isso, uma análise das técnicas dos principais projetos de interoperabilidade de *blockchain* foi concluído e consideraram que uma solução de interoperabilidade de *blockchain* bem-sucedida precisa resolver cinco problemas. a) Atomicidade e consistência de transações entre cadeias; b) mecanismo de confiança entre cadeias; c) protocolo de comunicação entre cadeias; d) segurança entre cadeias; e) gerenciamento de identidade entre cadeias. Os autores mostram também uma tabela comparativa de soluções de interoperabilidade (Cosmos, Polkadot, Aion, dentre outras), destacando características, como: Mecanismo usado para interoperabilidade (HTLC, Sidichains, etc.), Protocolo usado, Mecanismo cross-chain de gerenciamento de segurança e qual suporte a *blockchain* usado (pública, privada, Consórcio). Apesar da contribuição, não foi trabalhado nada a respeito de custos e desempenho dos mecanismos de interoperabilidade destacados nos trabalho.

O estudo feito por Alhussayen et al. (2024), propõe uma técnica de interoperabilidade de oráculo de *blockchain* projetada especificamente para plataformas de redes *blockchain* permissionada. Apresentam uma arquitetura da técnica de interoperabilidade de oráculo de *blockchain* e uma implementação em protótipo para demonstrar a praticidade da técnica proposta, além de medir a latência de transação entre redes. Todo o projeto se deu através da conexão do *Hyperledger Fabric* e a *blockchain* Corda. Além da avaliação ter sido feita apenas para redes permissionadas, ter medido a latência entre as transações, mantém abertas, várias questões, como o custo de processamento e a forma como o valor é cobrado durante as transações.

O trabalho de (GHAEMI et al., 2021), consiste em uma solução de interoperabilidade *blockchain* baseada na arquitetura publicar/assinar, onde uma *blockchain* de corretor mantém um registro dos dados que estão sendo transferidos entre redes *blockchain*. As *blockchains* que visam participar da interoperabilidade podem se conectar à rede de corretores como publicadores ou assinantes, dependendo de sua função. Os autores criaram

também um protótipo do *blockchain* de corretores implementado no Hyperledger Fabric. Além disso, um publicador de exemplo e dois assinantes de exemplo foram implementados usando o *Hyperledger Besu* e duas versões do *Hyperledger Fabric*. O desempenho da rede foi analisado usando uma ferramenta de *benchmark* para identificar os limites e gargalos da plataforma.

O protocolo IBC (*Inter-Blockchain Communication*) do ecossistema Cosmos tem sido alvo de estudos experimentais que medem seu desempenho em ambientes reais. Autores como Kwon et al. (2019) e trabalhos posteriores Developers (2023), Group (2023) demonstram que a latência de transações cross-chain depende fortemente do desempenho dos *relayers*, evidenciando que a eficiência do protocolo está vinculada à frequência de atualização e ao tempo de confirmação entre cadeias.

No ecossistema Polkadot, o protocolo XCMP (*Cross-Consensus Message Passing*) foi desenvolvido para permitir comunicação entre parachains. Estudos recentes Polkadot Developers (2023) avaliam o tempo de entrega das mensagens no HRMP (*Horizontal Relay-routed Message Passing*), ressaltando que a latência de confirmação é afetada pela congestão da rede e que o custo de operação pode aumentar quando múltiplos canais de mensagens são utilizados.

Entre as soluções de interoperabilidade generalistas, destaca-se o LayerZero, que propõe um modelo de comunicação *omnichain* com verificações independentes via oráculo e *relayer*. Conforme LayerZero Labs (2023), embora ofereça flexibilidade para o envio de mensagens arbitrárias, o custo de operação cresce de acordo com a complexidade da transação, e a latência aumenta em cenários com múltiplas confirmações de segurança.

De forma semelhante, a rede Axelar Axelar Network (2022) adota um mecanismo de *General Message Passing*, onde mensagens cross-chain podem ser propagadas entre diferentes blockchains públicas. Avaliações preliminares indicam que, embora apresente desempenho satisfatório em termos de escalabilidade, o custo de execução das operações pode variar significativamente em função da quantidade de mensagens encaminhadas.

Por fim, a solução Wormhole Wormhole Foundation (2022), baseada em uma rede de *guardians*, vem sendo utilizada em larga escala por protocolos DeFi. Estudos empíricos mostram que o tempo necessário para validação coletiva das transações pode introduzir latência adicional, ao mesmo tempo em que a cobrança de tarifas entre cadeias pode se tornar um fator relevante para a escalabilidade do sistema.

No intuito de facilitar o entendimento dos trabalhos relacionados, a Tabela 1 apresenta um resumo comparativo das principais abordagens encontradas na literatura sobre interoperabilidade entre blockchains. A coluna *Ref.* identifica as referências dos autores de cada trabalho. As colunas *Custo* e *Desempenho* indicam, respectivamente, se o estudo realiza avaliação das tarifas ou custos de transação e se analisa o desempenho ou a

latência das operações de interoperabilidade. Em seguida, a coluna *Observação* descreve de forma breve o foco, o escopo e os resultados principais de cada pesquisa. Por fim, a coluna *Comparativo* destaca os aspectos específicos ou contribuições particulares de cada trabalho, permitindo identificar as distinções entre as abordagens analisadas e evidenciar o diferencial do nosso trabalho. Em suma, o nosso trabalho avalia custo e desempenho de interoperabilidade de *tokens* via CCIP, analisa também os custos por etapa de transação (rede A $\rightarrow$ CCIP $\rightarrow$ rede B) e compara com o desempenho dos protocolos Notarial e HTLC.

Tabela 1 – Trabalhos relacionados com breves observações e comparativos.

Ref.	**Custo**	**Desempenho**	**Observação**	**Comparativo**
(WANG, 2021)	Não	Não	Revisão sistemática sobre avanços e desafios na interoperabilidade entre blockchains.	Sem avaliação prática de custo ou desempenho.
(MENDONçA et al., 2024)	Sim	Sim	Compara o desempenho dos métodos Notarial e Bloqueio de Hash.	Análise comparativa, mas sem detalhar custos por etapa.
(BELLAVISTA et al., 2021)	Não	Sim	Testes entre Hyperledger Fabric e Sawtooth.	Foco em blockchains permissionadas distintas.
(CAO et al., 2024)	Não	Não	Propõe o protocolo MAP usando arquitetura de relay.	Sem experimentos quantitativos.
(ZHU; CHI; LIU, 2023)	Não	Não	Discute desafios e frameworks baseados em sidechains e pontes cross-chain.	Abordagem teórica, sem avaliação empírica.
(ALHUSSAYEN et al., 2024)	Não	Sim	Técnica de interoperabilidade de oráculo para blockchains permissionadas.	Analisa desempenho, mas não custos.
(GHAEMI et al., 2021)	Não	Sim	Desempenho medido com ferramenta de benchmark para identificar gargalos.	Foco em throughput e latência, sem interoperabilidade cross-chain.
(KWON et al., 2019)	Não	Sim	Avalia o IBC no ecossistema Cosmos; latência depende dos relayers.	Custo não analisado; foco em tempo de confirmação.
(Polkadot Developers, 2023)	Não	Sim	Analisa o protocolo XCMP; latência e custo variam com a congestão da rede.	Sem detalhamento de custo ou comparação com outros modelos.
(LayerZero Labs, 2023)	Sim	Sim	Propõe comunicação *omnichain*; custo cresce com a complexidade da mensagem.	Foco na escalabilidade, sem custo por estágio.
(Axelar Network, 2022)	Sim	Sim	Rede de *General Message Passing*; custo varia com o volume de mensagens.	Avalia desempenho agregado, sem decomposição de custo.
(Wormhole Foundation, 2022)	Sim	Sim	Mensageria via rede de guardians; latência associada à validação coletiva.	Apresenta custos agregados; sem detalhamento por etapa.

3 Metodologia

Neste capítulo é descrito a metodologia para analisar desempenho e custo de protocolos para interoperabilidade de redes *blockchain*, em especial o protocolo CCIP que é o foco desse trabalho. Primeiramente, descrevemos o ambiente experimental baseado em redes de testes para desenvolvimento de aplicações descentralizadas em *blockchain* Seção 3.1. A seguir, detalhamos a Seção 3.2 as medições que são realizadas com os protocolos nessas redes para a referida análise de desempenho.

3.1 Ambiente Experimental

A maioria das plataformas *blockchains* públicas possuem redes de testes que são ambientes para desenvolver, experimentar e validar aplicativos, contratos inteligentes e funcionalidades antes de uma implantação real na rede *blockchain* principal. Exemplos de redes de teste populares são a Sepolia[1] da plataforma blockchain Ethereum, a *Fuji*[2] da plataforma *blockchain Avalanche*, a *Amoy*[3] da plataforma blockchain *Polygon* e etc. Importante mencionar o Bitcoin e outras *blockchains* assim como essa, consideradas de 1ª geração, não possuem *Testnets* por não suportarem execução de aplicações, ou seja, contratos inteligentes.

As redes de testes conseguem replicar o comportamento da rede principal, com algumas diferenças: Os *tokens*, ou seja, a moeda da rede *blockchain*, não têm valor financeiro (não tem validade fora da rede de teste); Possibilita o desenvolvimento de contratos inteligentes sem utilização de *tokens*, contas de usuários e contratos inteligentes reais da rede principal. Os desenvolvedores podem obter gratuitamente *tokens* das redes de testes via requisições em serviços web mantidos pelos patrocinadores das redes de teste, tais serviços são conhecidos como *faucets*.

Por sua vez, as redes de testes possuem algumas diferenças das redes principais que precisam ser consideradas durante o desenvolvimento de aplicações e análises de desempenho. Em especial, as medidas de tempo das redes de testes podem não ser semelhantes às redes principais, Isso porque o número de transações nas redes principais podem ser maiores do que nas redes de testes. Contudo, as redes de testes e principais utilizam os mesmos mecanismos para escalonar a fila de transações pendentes, isso é, são priorizadas a inclusão de transações no bloco pelo valor da sua tarifa. Já a tarifa reflete o volume de operações da transação, e o preço do GAS (unidade computacional) oferecido

[1] https://sepolia.etherscan.io/
[2] https://build.avax.network/docs/quick-start/networks/fuji-testnet
[3] https://polygon.technology/blog/introducing-the-amoy-testnet-for-polygon-pos

pelo emissor da transação para executar as operações. Portanto, os tempos e custo de execução de transações em redes de teste são representativos da rede principal para fins de avaliação de aplicações e protocolos. Em outras palavras, considerando o objetivo de avaliar custo e desempenho de protocolos, a diferença dos valores de medições obtidas entre os protocolos deve ter a mesma proporção se compararmos os resultados das redes de testes com as redes principais. Em suma, o uso de redes de teste é o procedimento padrão em redes *blockchain* para o desenvolvimento e avaliação de novos protocolos e aplicações[4].

Para os nossos experimentos, optamos pelas redes principais *Polygon* e *Avalanche* e suas redes de testes *Amoy* e *Fuji*, respectivamente. A rede *Amoy* é uma rede de testes desenvolvida para a *blockchain Polygon*, servindo como um ambiente de baixo risco para desenvolvedores construírem, testarem e aperfeiçoarem suas aplicações antes de implantá-las na rede principal. Criada em janeiro de 2024, utiliza a *Sepolia* (uma rede de teste do Ethereum) como sua rede *blockchain* base, garantindo uma infraestrutura sustentável[5]. Essa configuração permite que desenvolvedores continuem contando com validadores essenciais, ferramentas de infraestrutura, *faucets* e outros recursos necessários para o desenvolvimento de aplicações e protocolos para a rede principal. (Polygon, 2024). A rede *Amoy* utiliza o mesmo *token* da rede *Polygon*, denominado POL. Para fins de avaliação, todas aplicações em desenvolvimento dentro da *Amoy* consideram o valor real do POL, que no momento da escrita desse trabalho é de USD 0,29.

É importante observar que variações na cotação real do POL em relação ao dólar, torna difícil a obtenção de POLs gratuitos (*faucets*) junto aos mantenedores da rede teste para a condução de experimentos. Isso é um fenômeno comum em todas as redes de testes. Por esse motivo optamos em utilizar a rede de teste *Amoy* da *Polygon* ao invés da rede de teste Sepolia da Ethereum. Essa última, por se tratar de uma rede mais antiga e tradicional, há uma maior dificuldade na obtenção de *faucets* o que poderia atrasar a condução dos experimentos. Contudo, os procedimentos descritos na metodologia desse trabalho são gerais e aplicáveis a todas as redes de testes *blockchain*.

A *Avalanche Fuji*, rede de testes oficial da *Avalanche*, possibilita que desenvolvedores testem aplicações e contratos inteligentes sem custos financeiros associados às transações para a rede *blockchain Avalanche*. Essa rede é uma plataforma *blockchain* de alto desempenho que utiliza o protocolo de consenso (baseado em *proof of stake*, conhecido por sua baixa latência e capacidade de processar milhares de transações por segundo (TPS). Lançada em setembro de 2020, desenvolvida pela startup Ava Labs, chega com o objetivo de oferecer uma solução de consenso rápida e altamente escalável, capaz de operar de forma resiliente mesmo em redes não confiáveis (Avalanche, 2024). O *token* nativo da *Avalanche* é o AVAX (utilizado para pagamento de taxas de transação) e no momento

[4] https://swapped.com/blog/everything-you-need-to-know-about-testnets

[5] A rede *Polygon* é considerada uma rede *blockchain* de 2ª camada porque ela é construída sob outra rede *blockchain*, nesse caso o Ethereum, que é a sua rede de 1ª camada.

da escrita deste trabalho, seu valor é de USD 24,39 por unidade. Para experimentação e desenvolvimento, a *Avalanche* mantém a rede de teste *Fuji*, que utiliza igualmente o *token* AVAX (obtido gratuitamente por meio de *faucets*), permitindo simulações realistas de uso sem riscos financeiros (Avalanche, 2024).

Escolhemos a rede *Avalanche Fuji* para nossos experimentos, pois além de ser de primeira camada é relativamente nova em comparação ao Ethereum. Essa característica se reflete em *faucets* mais acessíveis e rápidos, o que reduz o tempo necessário para a obtenção de *tokens* de teste e agiliza significativamente a condução dos experimentos. Ressaltamos que os procedimentos descritos nesta metodologia são aplicáveis a outras redes de teste, sejam de primeira ou segunda camada — como no caso da rede *Amoy* para *Polygon* —, bastando adaptar-se às especificidades de cada *blockchain*.

Além das duas redes supracitadas, utilizamos a rede de testes da *Chainlink* e seu protocolo CCIP como ponte responsável pela interoperabilidade das redes *Amoy* e *Fuji*. A rede de testes da *Chainlink*, na prática, corresponde a várias redes de testes, cada uma definida para propósitos e ecossistemas *blockchains* distintos. Através dessas redes é possível testar e integrar os oráculos descentralizados da *Chainlink*. Consequentemente, os dados externos são transmitidos com segurança e confiabilidade para contratos inteligentes antes do lançamento na rede principal (CHAINLINK, 2023). Assim como as outras redes de testes de *blockchain*, as redes *Chainlink* utilizam o *token Link* como moeda da plataforma. Assim como os demais tokens, o token *Link* também pode ser obtido para testes de interoperabilidade entre redes de teste de forma gratuita via serviços de *faucets* da *Chainlink*. Através da *Chainlink* é possível testar aplicações de vários ecossistemas, pois ela suporta várias plataformas *blockchains*, como *Ethereum*, *Polygon*, *Avalanche* e etc.. Em especial, a plataforma *Chainlink* é compatível com as redes de testes *Amoy* e *Fuji* utilizadas como redes de testes dos experimentos nesse trabalho.

Considerando as redes de teste *Amoy* e *Fuji* acima descritas, conduzimos experimentos em uma instância virtual da AWS (t3.micro: 2 vCPUs, 1 GiB RAM, 10% CPU baseline, 12 créditos/h, rede 5 Gbps, EBS até 2.085 Mbps), utilizando a ferramenta nativa do Linux, Crontab, para agendamento automático de transações. A partir dessa configuração, agendamos execuções periódicas de uma transação variando as redes de origem e destino da transação. Dessa forma conduzimos uma transação na direção de ida (*Amoy* para *Fuji*) e a mesma transação na direção de volta (*Fuji* para *Amoy*).

A transação conduzida consiste em uma *transferência cross-chain* de *tokens* ERC-20 utilizando CCIP. Nos contratos, o ativo movimentado é o *CCIP-BnM token*, disponibilizado oficialmente pela *Chainlink* nas redes de teste *Polygon Amoy* e *Avalanche Fuji* (LABS, 2024a). Esse *token* segue o modelo *burn/mint*: ao ser transferido, ele é destruído (*burn*) na rede de origem e um novo *token* equivalente é criado (*mint*) na rede de destino (LABS, 2024b; RAKIC, 2023).

Com o intuito de viabilizar o processo, cada contrato foi configurado com os endereços do roteador CCIP e do *token BnM* correspondentes a cada rede de teste. O roteador é o responsável por encaminhar a mensagem contendo os parâmetros da transação para a rede de destino, onde o contrato correspondente executa a operação de cunhagem (*mint*). Os códigos fontes dos contratos utilizados estão disponibilizados no repositório do grupo de pesquisa[6] por questão de praticidade.

3.2 Escalonamento de experimentos e métricas

O foco dos experimentos é medir o **tempo** e o **custo das transações** entre as redes *blockchain*. Para isso, adotamos que **uma transação seria enviada a cada 8 minutos**. Em cada ciclo, realizamos dois envios em sentidos opostos, com **defasagem de 1 minuto**: primeiro de *Amoy* → *Fuji* e, em seguida (após 1 minuto), de *Fuji* → *Amoy*. O padrão se repetiu a cada 8 minutos ao longo de toda a coleta.

O intervalo de 8 minutos foi definido após verificarmos, em testes preliminares, que intervalos maiores não alteravam significativamente o desempenho (tempo e custo). Por outro lado, a adoção de intervalos menores geraria uma base de dados mais volumosa, mas aumentaria substancialmente o consumo de *faucets*, o que não era desejável para execuções prolongadas. Com essa configuração, obtivemos **1.739 transações** de *Fuji* → *Amoy* e **1.739 transações** de *Amoy* → *Fuji*, totalizando **3.478 transações**.

Medimos o custo de interoperabilidade através dos valores das tarifas pagas pelos usuários interessados em emitir transações entre redes *blockchain* diferentes. Os valores dessas tarifas são um meio adequado de mensurar esse custo porque representam tanto o incentivo (isto é, o lucro) quanto o custo operacional dos mantenedores da rede *blockchain*. As tarifas cobradas para transações de interoperabilidade de *blockchains* estão diretamente ligadas às redes que usarão o serviço, *Amoy* e *Fuji* em nossos experimentos, e aos Oráculos da rede *Chainlink*. A soma das tarifas dessas redes resulta no valor total a ser cobrado pelo serviço de interoperabilidade.

Nas transações realizadas via *Chainlink CCIP*, o usuário arca com diferentes tipos de tarifas. Por exemplo, em uma transação da rede *Amoy* para a rede *Fuji*, o usuário de origem paga: (i) uma taxa em *POL* referente ao gás da transação de origem, (ii) uma taxa de serviço do *Chainlink CCIP* em *LINK*, e (iii) uma taxa em *AVAX* pela execução da transação na *Fuji*. Embora a transação envolva diferentes *tokens* de gás em cada etapa, o custo final é sempre de responsabilidade do usuário de origem. Especificamente, as taxas em *POL*, *LINK* são pagas temporariamente pelo protocolo CCIP, mas seu valor é repassado ao usuário de origem como parte do custo total da operação. Logo, o usuário

[6] <https://github.com/LABPAAD/blockchain_interchain/tree/search/contracts>

na origem paga esse custo total de tarifação com o *token* de origem, que no exemplo em questão é POL.

Por sua vez, medimos os tempos de execução de cada transação de interoperabilidade como forma de avaliar o desempenho dessa operação. Para isso, coletamos os tempos de execução das transações realizadas a partir dos contratos inteligentes implementados para a interoperabilidade entre as redes (*Fuji* e *Amoy*) por meio do protocolo CCIP. Para cada transação, registramos o instante em que a operação foi submetida e confirmada na rede de origem, bem como o instante em que a transação correspondente foi finalizada na rede de destino. Esses valores foram obtidos a partir dos *timestamps* dos blocos que incluíram cada transação, consultados através de serviços *Web* exploradores de redes *blockchain*..

As medições de custo e tempo de transações de interoperabilidade acima descritas foram realizadas a partir dos registros em rede *blockchain* em cada uma das redes envolvidas. Para isso, registramos o identificador *hash* de cada transação emitida na VM, a seguir recuperamos informações de tarifa e tempo de cada transação pesquisando com os *hashes* em exploradores de redes *blockchain*, que disponibilizam gratuitamente esses registros nas respectivas redes de teste via requisições com APIs. Para este estudo, foram utilizados os seguintes exploradores: *Polygonscan (Amoy Testnet)*[7], *Snowtrace (Fuji Testnet)*[8] e *Chainlink CCIP Explorer*[9]. Estes exploradores permitem a obtenção de dados detalhados de cada transação, como o tempo de confirmação e o valor das taxas, de forma automatizada utilizando suas `APIs` públicas.

Finalmente, os valores de tarifas e tempos de execução de cada operação foram processados e organizados em bases de dados no formato CSV. A partir dessas bases de dados utilizamos os recursos da linguagem *Python* 3, i.e., as bibliotecas *Pandas, PyPlot, Matplotlib* e *Numpy*, para a análise quantitativa de custos e desempenho de interoperabilidade via rede *Chainlink* em comparação com outros protocolos de interoperabilidade descritos na literatura, a ser discutido no próximo capítulo.

[7] <https://amoy.polygonscan.com/>
[8] <https://testnet.snowtrace.io/>
[9] <https://ccip.chain.link/>

4 Resultados e Discussão

Neste capítulo, discutimos os resultados da análise de custo e desempenho do protocolo de interoperabilidade da *Chainlink* (CCIP), disponibilizado por meio da infraestrutura da empresa via seu serviço de Oráculos. Primeiramente, a análise considera exclusivamente o protocolo da *Chainlink* e adota as métricas previamente definidas: o desempenho é avaliado em termos do tempo de execução das operações de interoperabilidade na Seção 4.1, enquanto na Seção 4.2 o custo é medido pelo valor das tarifas associadas a essas operações . A seguir, comparamos o protocolo *Chainlink* com implementações próprias de outros protocolos de interoperabilidade que podem se despontar como futuros concorrentes da *Chainlink* na Seção 4.3. São eles o protocolo Notarial, que é uma abordagem mais centralizada para interoperabilidade, e o protocolo HTLC, que é uma abordagem mais descentralizada.

4.1 Desempenho em tempo de operação

A Figura 6 apresenta a distribuição de tempos de operação para as duas direções de redes origem e destino, i.e., da rede *Amoy* para *Fuji*, assim como *Fuji* para *Amoy* no protocolo *Chainlink*. O gráfico nessa figura apresenta *boxplots* que sumarizam a distribuição da seguinte forma: o retângulo central se expande entre o primeiro e terceiro quartil, o segmento interior é a mediana, enquanto os indicadores abaixo e acima do retângulo representam o 10^{o} e 90^{o} percentis. Adicionalmente, pontos acima e abaixo dos indicadores representam valores atípicos (*outliers*). Nota-se grande dispersão em ambas as direções, ou seja, *outliers*, indicando que em certas execuções o tempo foi anormalmente maior. Isso pode refletir atrasos de rede, congestionamento ou características específicas do protocolo.

Observa-se na Figura 6, a assimetria entre as direções: os tempos *Amoy* $\rightarrow$ *Fuji* não tem a mesma distribuição de *Fuji* $\rightarrow$ *Amoy*, sugerindo que a latência ou o processo de confirmação depende da rede de origem. Em nossos experimentos especificamente, 80% das medições (valores entre os percentis 10^{o} e 90^{o}) estão 350 e 4404 segundos na direção *Amoy* $\rightarrow$ *Fuji* e entre entre 64 e 2405 segundos na direção *Fuji* $\rightarrow$ *Amoy*.

Adicionalmente, há uma possibilidade não desprezível (até 10% em nossas medições) de atrasos anormais, i.e., operações que duram mais que 4404 segundos (*Amoy* $\rightarrow$ *Fuji*) ou 2405 segundos (*Fuji* $\rightarrow$ *Amoy*), alcançando operações ainda mais longas de até 5921 segundos e 3934 segundos respectivamente, na cauda da distribuição medida.

A Figura 6 mostra assimetria entre os tempos de operação nas direções *Amoy* $\rightarrow$ *Fuji* e *Fuji* $\rightarrow$ *Amoy*. Adicionalmente, verificamos essa diferença em termos de valor

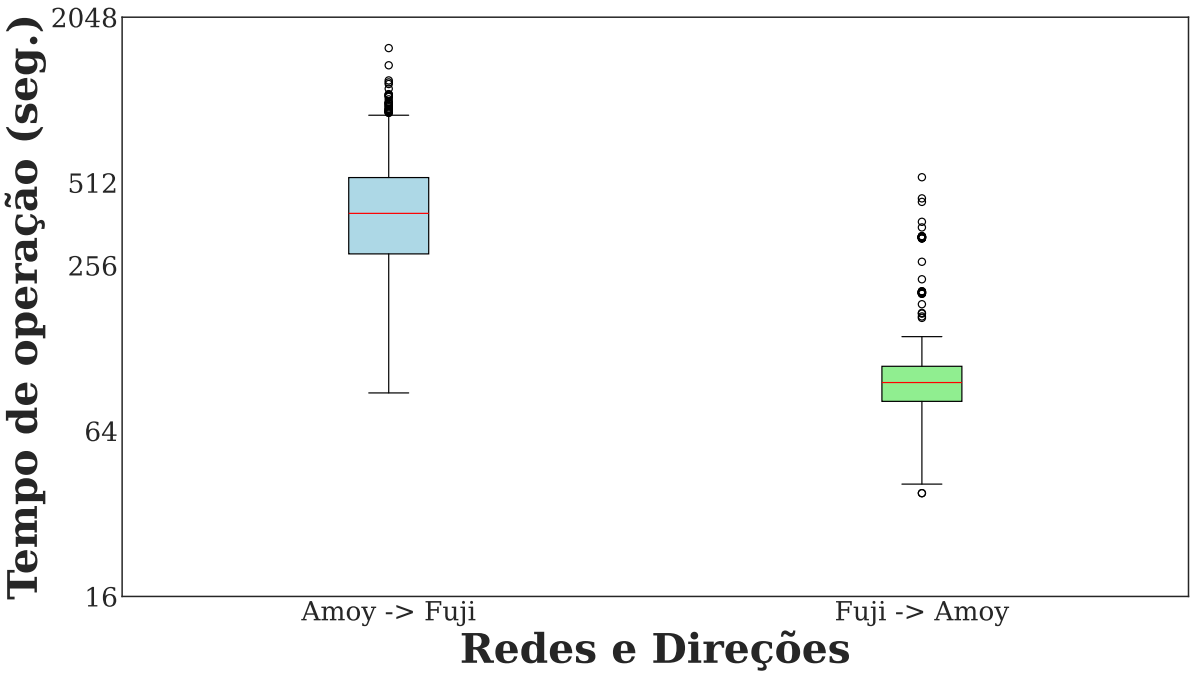

Figura 6 – Distribuição do tempo de operação no protocolo Chainlink (CCIP)

médio do tempo de operação em cada direção via o teste t de *Student* para analisar quão significativa é a diferença entre essas médias estatisticamente. Especificamente, utilizamos o teste t de *Student* para amostras independentes, na variante de Welch, apropriada para cenários em que não se assume igualdade de variâncias. As amostras foram compostas pelos tempos de operação obtidos a partir das transações realizadas via CCIP, considerando a diferença entre os instantes de origem e destino de cada transação. O teste resultou em um valor $t = 7{,}806$ com $p < 0{,}001$, levando à rejeição da hipótese nula ao nível de significância de 5%. Assim, o resultado confirma de forma estatística a assimetria já evidenciada Figura 6, indicando que o desempenho do CCIP difere entre as direções de comunicação analisadas.

Cabe ressaltar que os resultados foram obtidos em redes de teste, de modo que os valores absolutos podem diferir dos de uma rede principal. Ainda assim, esses ambientes refletem qualitativamente o mesmo comportamento, evidenciando padrões de variação de custo e possíveis atrasos que também podem ocorrer em redes reais.

Analisamos também o tempo de operações, distribuído ao longo das horas do dia (horário GMT), para maior detalhamento no desempenho dos protocolos . A Figura 7 mostra esses tempos via médias e seus respectivos erros com intervalo de confiança em 95%. onde o Eixo X representa o horário do dia (0h até 23h), ou seja, a medição do desempenho é visualizada via médias das operações em seus respectivos horários acompanhada ao longo de um dia inteiro. Já o Eixo Y, mostra o tempo médio em segundos, considerando todos os valores de médias observados, ou seja, valores de 0 até 550s no sentido *Amoy* $\rightarrow$ *Fujy* e de 0 160s no sentido *Fujy* $\rightarrow$ *Amoy*.

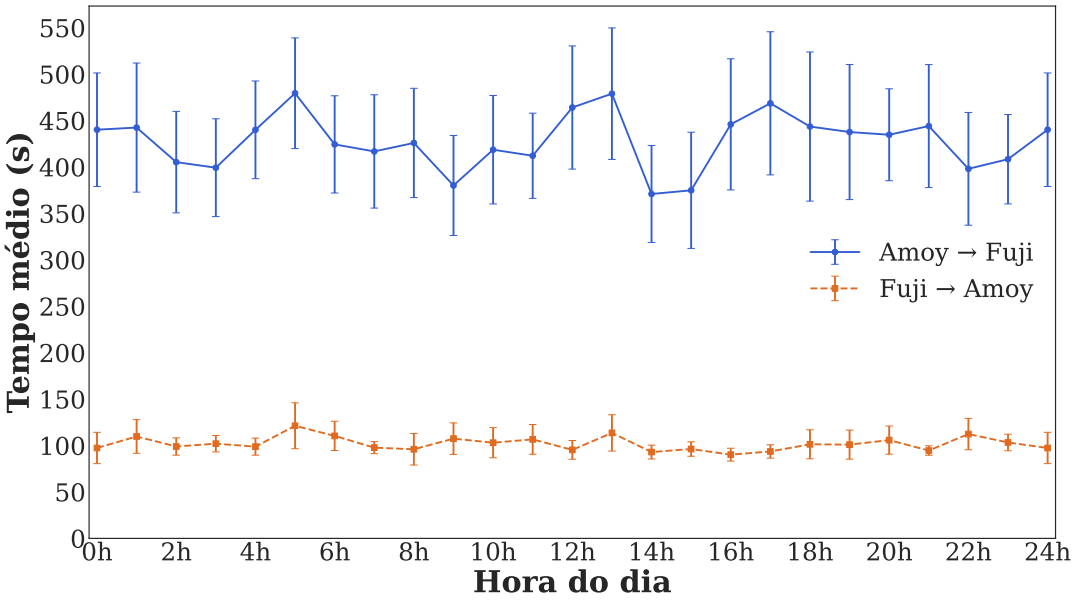

Figura 7 – Tempo médio de operação com intervalo de confiança de 95%.

A Figura 7 mostra instabilidade no desempenho de operações ao longo do dia, em especial no sentido *Amoy* → *Fujy*, é possível observar maior instabilidade ao longo do dia, onde o tempo médio das operações varia entre 110 e 150 segundos.

No sentido *Fuji* → *Amoy*, o tempo médio(s) das operações pelo *Chainlink* ao longo do dia ficaram em torno de 50–120s (bem mais baixos do que no sentido *Amoy* → *Fuji*). Observa-se ainda que os tempos médios ao longo do dia não se sobrepõem considerando os intervalos de confiança (barras de erro) mostrado em ambas as direções. Nota-se que o menor valor alcançado pelas barras no sentido *Amoy* → *Fuji* é de 300 segundos, ao passo que o maior valor alcançado pelas barras no sentido *Fuji* → *Amoy*, é 550 segundos. Isso indica que o desempenho *Chainlink* é assimétrico, i.e., tempos de operação da rede A para B e B para A diferentes significativamente, mesmo considerando valores médios.

4.2 Custo em tarifas da operação

A Figura 8 apresenta a distribuição de custos de operação, onde o eixo Y representa o custo em USD das operações (variando aproximadamente de 0 a 0,80 dólares) e o eixo X mostra o protocolo *Chainlink* e a direção da operação (*Amoy* → *Fuji* e *Fuji* → *Amoy*). Os *Boxplots* em questão sumarizam a distribuição dos valores medidos no experimento com mediana, quartis e *outliers* assim como na seção anterior.

As distribuições de custos apresentam-se relativamente próximas entre as direções analisadas. Por exemplo, em 50% das medições situadas entre o 1º e o 3º quartis (corpo do *boxplot*), o custo varia entre USD 0,30 e USD 0,45 na direção *Amoy* → *Fuji* e entre USD 0,28 e USD 0,50 na direção *Fuji* → *Amoy*. Assim, os resultados sugerem que o

ponto de origem e destino da operação exerce influência limitada sobre o custo, apesar da presença de *outliers* apenas na direção *Amoy* → *Fuji*, isto é, operações acima de USD 0,50 em menos de 10% dos casos.

É importante destacar que cada rede envolvida na operação de interoperabilidade aplica tarifas distintas, expressas no valor de seu *token* nativo (i.e., POL na *Amoy*, AVAX na *Fuji* e LINK na *Chainlink*). Por esse motivo, os valores de todas as tarifas foram convertidos para USD conforme a cotação vigente no momento de cada operação, de modo a permitir uma comparação homogênea dos custos de interoperabilidade.

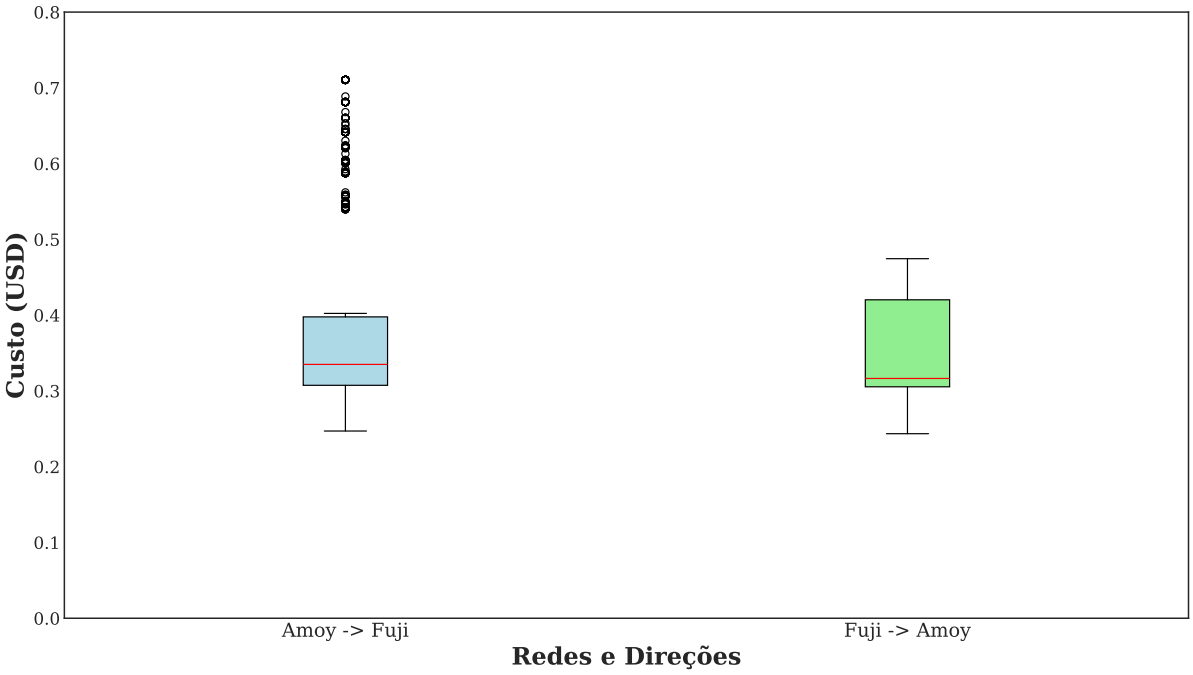

Figura 8 – Distribuição do custo de operação.

Detalhamos o custo de operação do protocolo *Chainlink* distribuído ao longo das horas dia (horário GMT), assim como na análise de desempenho. A Figura 9 mostra esses custos em dólar (USD) via médias e seus respectivos erros com intervalo de confiança em 95%. Nota-se pouca variabilidade nos custos médios do protocolo ao longo do dia em ambas as direções, contudo, tem valores médios maiores na direção *Amoy* → *Fuji* variando de 0,32 a 0,46 USD. Por sua vez, o custo médio na direção *Fuji* → *Amoy* é ligeiramente menor, variando de 0,29 a 0,42 USD. É notável, no entanto, que os intervalos de confiança indicados pelas barras de erro das médias em ambos os sentidos estão muito próximos. Logo, não é possível evidenciar em nossas medições que os custos na duas direções são diferentes significativamente. Esse resultado nos mostra que o ponto de partida da operação tem pouco impacto em seu custo, diferentemente do desempenho observado na seção anterior.

Para uma maior compreensão do custo do protocolo *Chainlink*, analisamos o custo por rede que compõe a operação em nossos experimentos. Essa análise consiste em valores médios ao longo das horas do dia, assim como na figura anterior. As medições são mostradas

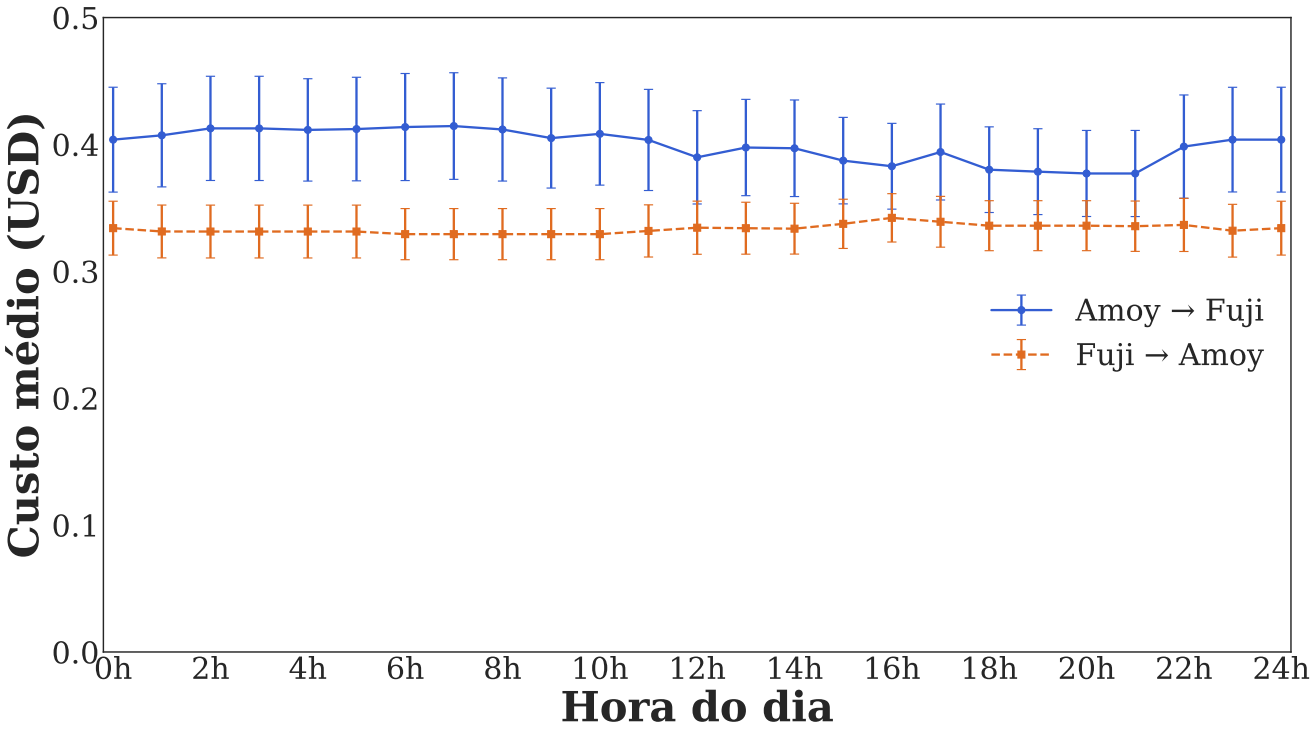

Figura 9 – Custo médio das operações com intervalo de confiança de 95%.

na Figura 10, para operações na direção *Amoy* → *Fuji* e na Figura 11 para a direção entre *Fuji* e *Amoy*.

O custo médio das transações no sentido *Amoy* → *Fuji*, apresentada na Figura 10, evidencia que a maior parcela do custo concentra-se na rede *Chainlink*, com valores estáveis em torno de 0,25–0,35 USD, representando mais de 80% do custo total. Os custos nas redes de origem (*Amoy*, ≈0,005–0,01 USD) e de destino (*Fuji*, ≈0,01–0,05 USD) mostraram-se significativamente inferiores, variando de forma marginal ao longo do dia. Este comportamento sugere que, independentemente do horário da transação, o fator determinante do custo é o serviço intermediário de roteamento, não as taxas intrínsecas das redes. Ressalta-se, contudo, que a avaliação em dólares pode mascarar a influência da volatilidade cambial das moedas nativas (*POL, LINK e AVAX*), cuja valorização ou desvalorização relativa impacta diretamente na representatividade dos custos em diferentes contextos econômicos. Até fechamento deste trabalho as cotações estavam da seguinte forma: POL em 0,28 USD, AVAX em 29,63, LINK em 24,42 USD

No sentido inverso, *Fuji* → *Amoy*, observa-se padrão semelhante ao identificado anteriormente, conforme ilustrado na Figura 11. O custo associado ao *Chainlink* permanece como principal componente, com valores médios próximos a 0,30–0,32 USD, confirmando sua predominância na estrutura de gastos da comunicação entre cadeias. A rede de origem (*Fuji*) apresenta custos de *gas* levemente superiores aos da *Amoy*, em torno de 0,01–0,015 USD, enquanto a rede de destino (*Amoy*) mantém custos praticamente residuais (≈0,003 USD). Assim como no fluxo contrário, não foram identificadas variações significativas ao

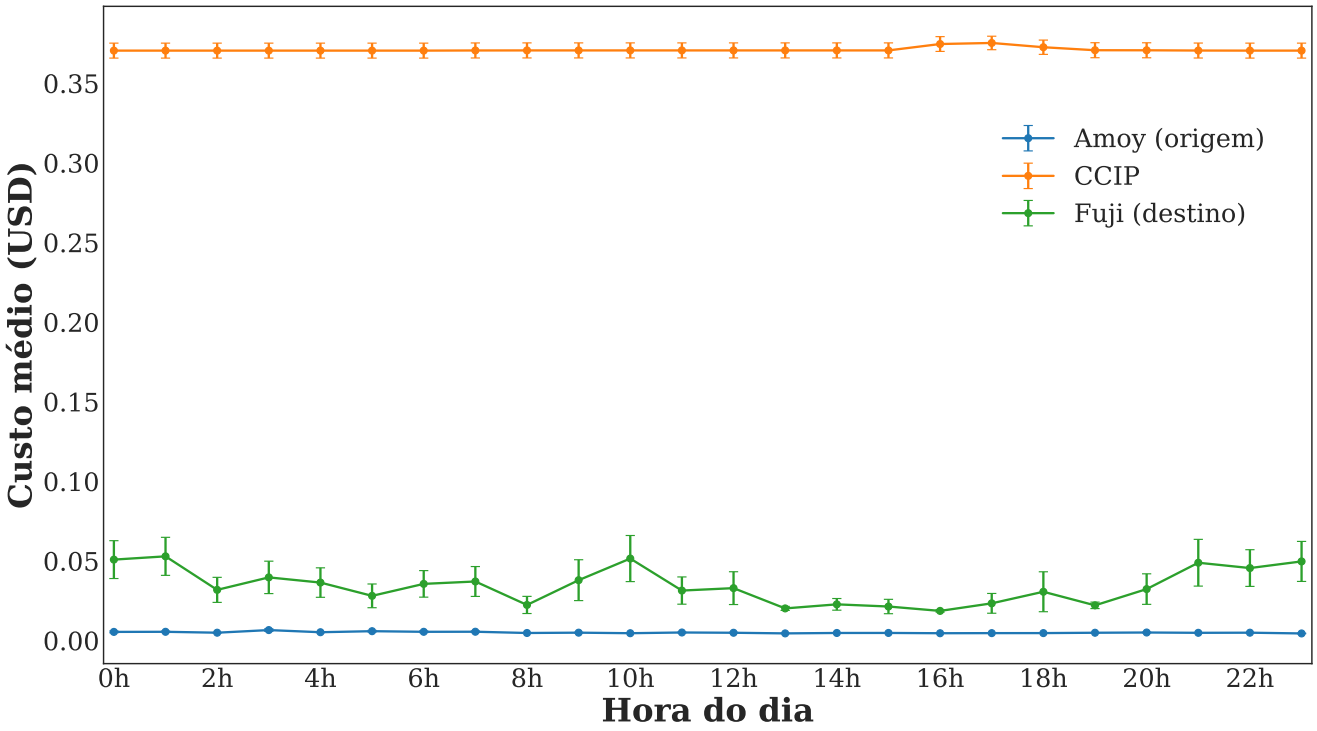

Figura 10 – Custo por etapa de transação da rede Amoy para Fuji.

longo do dia, reforçando a estabilidade do *Chainlink*.

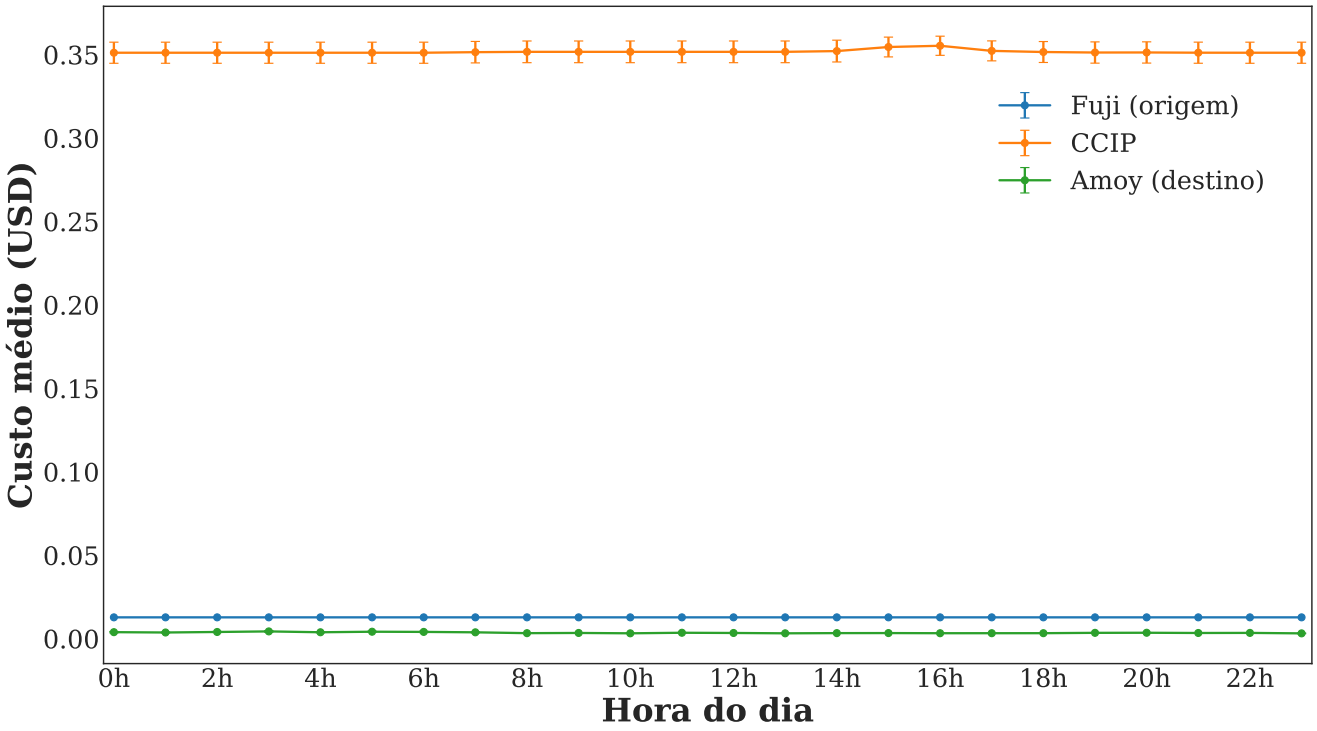

Figura 11 – Custo por etapa de transação da rede Fuji para Amoy.

4.3 Comparação com outros métodos

Nesta seção, comparamos o desempenho e o custo do protocolo *Chainlink* com outras duas abordagens de interoperabilidade descritas na literatura. Especificamente, consideramos implementações representativas dos protocolos Notarial e HTLC, conforme apresentados na Seção 2.3. Para tanto, utilizamos os códigos dessas implementações disponibilizados publicamente pelos respectivos autores[1]

Os resultados discutidos nesta seção foram previamente publicados em (MUNIZ et al., 2025), no contexto de uma colaboração em projeto de pesquisa interinstitucional que envolve tanto o proponente desta dissertação quanto os autores responsáveis pelas implementações dos protocolos mencionados.

A Figura 12 apresenta a distribuição dos tempos de operação para os três mecanismos nas direções da rede de origem e de destino, ou seja, da rede *Amoy* para a rede *Fuji*, bem como da rede *Fuji* para *Amoy*. O gráfico apresenta boxplots que resumem a distribuição da seguinte forma: o retângulo central abrange o primeiro e o terceiro quartis, e o segmento interno é a mediana. Em contraste, os indicadores abaixo e acima do retângulo representam os percentis 10º e 90º. Além disso, os pontos acima e abaixo dos indicadores representam valores discrepantes.

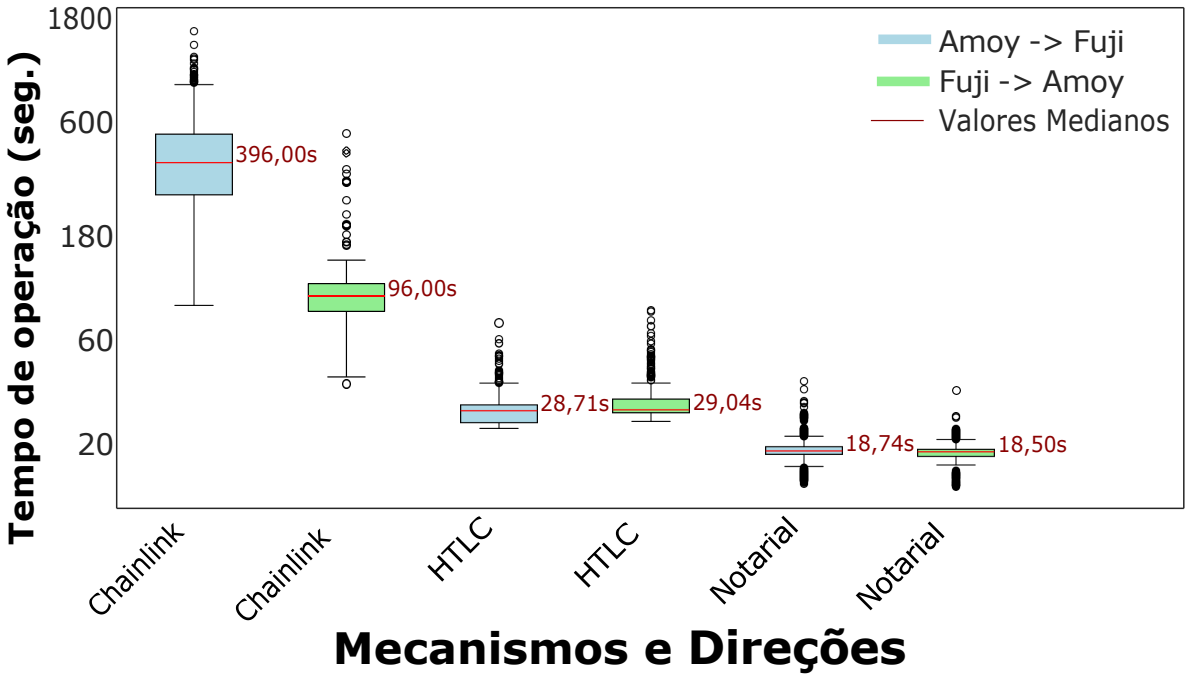

Figura 12 – Distribuição do tempo de operação.

A Figura 12 ilustra que o protocolo Notarial apresenta uma distribuição de tempos de operação com valores mais baixos, enquanto o protocolo *Chainlink* apresenta valores

[1] Implementação do protocolo Notarial disponível em: <https://github.com/RafaelPCoelho/Hash-Time-Lock-Contract> e implementação do protocolo HTLC disponível em: <https://github.com/italloferreira27/Notary-Mechanism>

mais altos, e o HTLC ocupa a posição intermediária. Portanto, o protocolo Notarial apresenta melhor desempenho em termos de tempo de operação, o que se explica pela sua simplicidade, ou seja, por envolver apenas uma entidade central, o Notário, para interoperar *tokens* entre duas redes. Em contrapartida, o protocolo *Chainlink* pode ser até sete vezes mais lento que o Notarial em termos de valores medianos, ou seja, tempos de 133 segundos na direção *Fuji* → *Amoy* contra 18 segundos para o Notarial na mesma direção, conforme mostrado na Figura 12. Na direção oposta, de *Amoy* → *Fuji*, os tempos medianos são de 35 segundos para o *Chainlink* e 18 segundos para o Notarial.

Por sua vez, o protocolo HTLC apresenta um desempenho intermediário, com tempos medianos de operação de 29 segundos nas direções *Fuji* → *Amoy* e *Amoy* → *Fuji*. Esse tempo é próximo ao do Notarial, mas, diferentemente deste último, o HTLC é totalmente descentralizado, conforme descrito na Seção 2.3.2. O desempenho inferior do protocolo *Chainlink* em comparação aos demais se deve principalmente à sobrecarga que a rede de validadores *Chainlink* exerce para interoperar *tokens* entre as redes de origem e destino.

Essa sobrecarga também impacta a direção da operação, visto que a origem *Fuji* → *Amoy* consome notavelmente mais tempo, enquanto nos demais protocolos não há essa lentidão. O protocolo *Chainlink* implementa uma rede de gerenciamento de risco que aprimora a segurança e o monitoramento entre redes. Portanto, essa gestão está comprometida em realizar operações mais seguras e confiáveis. Ainda assim, consome mais tempo e, consequentemente, um custo maior devido às transações extras inerentes à implementação do protocolo.

Também analisamos os tempos de operação, distribuídos ao longo das horas do dia (GMT), para detalhar ainda mais o desempenho dos protocolos. É possível observar maior instabilidade no protocolo *Chainlink* ao longo do dia, especialmente na direção *Fuji* → *Amoy*, onde o tempo médio de operação varia entre 110 e 150 segundos. Os protocolos Notarial e HTLC, por outro lado, permanecem com tempos de operação estáveis ao longo do dia, com tempos médios inferiores a 40 segundos (ou seja, menos de um minuto) por operação. Novamente, esses dois protocolos apresentam desempenhos muito semelhantes: os tempos médios do Notarial e do HTLC permanecem predominantemente em 20 e 35 segundos ao longo do dia, respectivamente, sem diferenças significativas em algumas horas, ou seja, há sobreposições entre os erros das médias.

As Figuras 13 e 14 mostram que o protocolo Notarial tem o menor custo, ou seja, a maioria das operações tem valores abaixo de 1 centavo. Por sua vez, os protocolos *Chainlink* e HTLC têm valores que variam de 10 centavos a 1 USD. Em particular, o custo do Chainlink é maior (a maioria das operações varia de 20 a 80 centavos) devido ao maior número de partes envolvidas na interoperabilidade dos *tokens*. Especificamente, a taxa do *Link* para os validadores da rede *Chainlink* é adicionada às taxas das redes de origem e

destino para a operação. Nesse caso, observamos que a rede de destino tem um impacto maior no custo do *Chainlink*, visto que a direção *Amoy* → *Fuji* tem uma distribuição de valor de custo superior, e o *token AVAX* atualmente tem um custo em dólar maior que o *POL*.

A figura 12 também mostra que a direção da operação impacta notavelmente o protocolo HTLC. Esse comportamento ocorre porque a rede de origem é responsável pela implementação do contrato na *blockchain*. Em contrapartida, a rede de destino realiza apenas a transação de resgate dos *tokens* previamente bloqueados pela rede de origem, conforme descrito na Seção 2.3. A implementação do contrato geralmente apresenta um custo computacional (gás) maior em redes *blockchain* e, portanto, uma taxa mais alta. Assim, a direção *Fuji* → *Amoy* apresenta um custo maior, visto que o custo maior do *token AVAX* na rede *Fuji* para a implementação do contrato torna o HTLC mais caro nessa direção.

Detalhamos o custo de operação dos protocolos distribuídos ao longo do horário de Brasília (GMT), bem como na análise de desempenho. A figura 13 mostra esses custos em dólares (USD) por meio de médias e seus respectivos erros com intervalo de confiança de 95%. É possível observar, desta vez, alta instabilidade ao longo do dia, não apenas no protocolo *Chainlink*, mas também no HTLC. O custo do protocolo *Chainlink* apresenta alta variação na direção *Amoy-Fuji* devido ao impacto da taxa *Fuji* na origem da rede (ou seja, o *token AVAX* tem um custo maior em dólares), fazendo com que os custos médios variem de 30 a 50 centavos de dólar. Em comparação, os outros protocolos apresentam custos estáveis abaixo de 5 centavos de dólar. Por sua vez, esse mesmo problema impacta o protocolo HTLC na direção *Fuji-Amoy*.

4.4 Sumário

Nesta seção sumarizamos os resultados apresentados neste capítulo. Nas Tabelas 2 e 3, apresentamos um resumo de nossos resultados apresentados em cada seção desse capítulo.

A análise inicial concentrou-se no desempenho do protocolo *Chainlink* no fluxo entre as redes *Amoy* e *Fuji*. Os resultados mostraram que: (i) em termos de **tempo de execução**, o sentido *Fuji* → *Amoy* foi mais eficiente, com valores em torno de 160 segundos, contra até 500 segundos no sentido inverso, que apresentou maior instabilidade; (ii) em termos de **custo total**, ambos os sentidos permaneceram na faixa de até **0,5 USD**, embora as transações no fluxo *Amoy* → *Fuji* tenham demonstrado tendência a custos ligeiramente mais elevados; (iii) quanto à **distribuição dos custos por etapa**, observou-se que a parcela mais onerosa concentrou-se no componente intermediário do *Chainlink*, enquanto origem e destino corresponderam a custos adicionais menores.

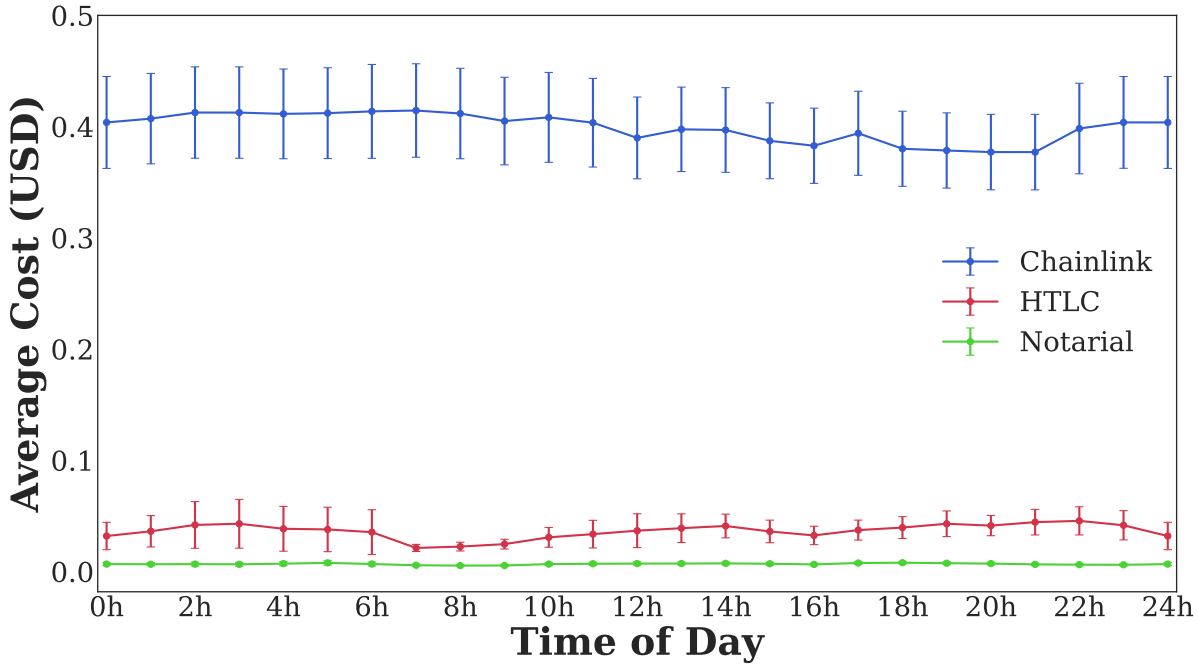

Figura 13 – Custos em dólares (USD) x Hora do dia - Direção da operação: Amoy para Fuji.

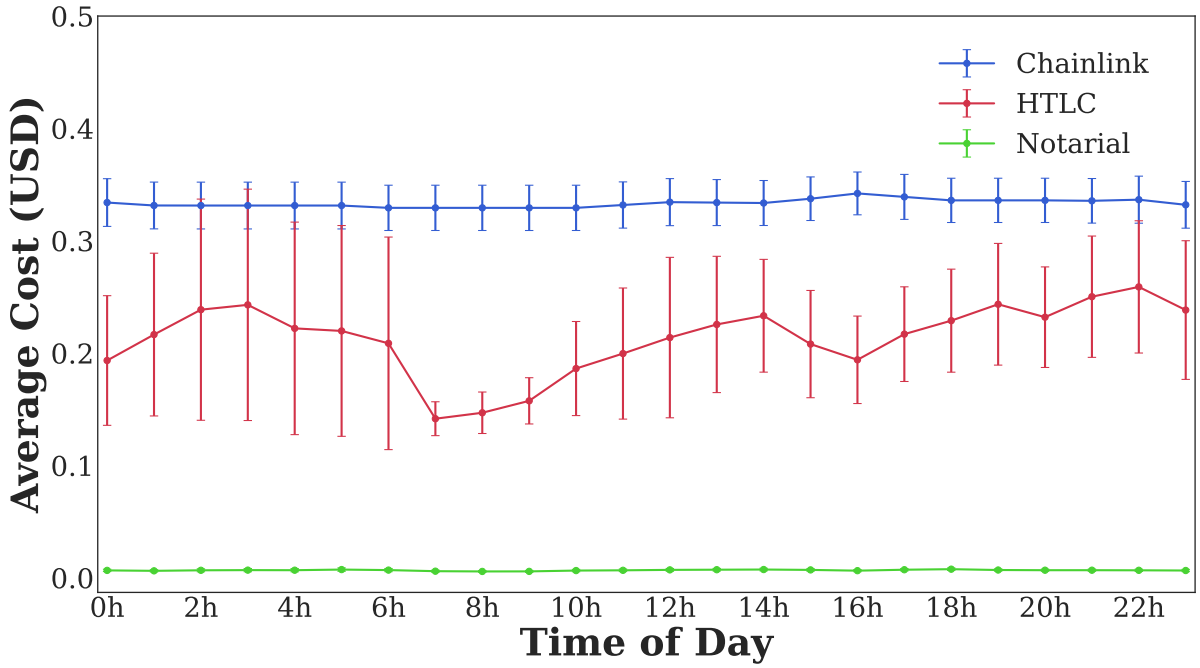

Figura 14 – Custos em dólares (USD) x Hora do dia - Direção da operação: Fuji para Amoy.

Em um segundo momento, o desempenho do *Chainlink* foi comparado com os mecanismos Notarial e HTLC. Os resultados evidenciaram diferenças expressivas: (i) no **tempo de execução**, o Notarial destacou-se como o mais eficiente (medianas em torno de 18–19 segundos), seguido pelo *HTLC* (28–29 segundos), enquanto o *Chainlink* apresentou valores muito mais elevados, alcançando 396 segundos em *Amoy* → *Fuji* e 96 segundos em

Tabela 2 – Desempenho do protocolo CCIP por sentido e etapa de custo

Critério	**Amoy → Fuji**	**Fuji → Amoy**
Tempo médio (s)	Até ∼500 (instável)	Até ∼160 (estável)
Custo médio (USD)	≤ 0,5 (ligeiramente maior)	≤ 0,5 (ligeiramente menor)
Custo por etapa	Origem + Destino (∼20–30%) CCIP (∼70–80%, mais elevado)	Origem + Destino (∼20–30%) CCIP (∼70–80%, mais elevado)

Fuji → Amoy; (ii) em relação ao **custo**, o *Chainlink* manteve-se consistentemente mais caro (até 0,5 USD), ao passo que Notarial e HTLC permaneceram em níveis inferiores a **0,2 USD**; (iii) no que se refere à **estabilidade**, tanto Notarial quanto HTLC apresentaram menor variação em comparação ao CCIP, cujo desempenho foi mais instável, principalmente no sentido *Amoy → Fuji*.

Tabela 3 – Resumo comparativo entre protocolos de interoperabilidade

Critério	**CCIP (Chainlink)**	**HTLC**	**Notarial**
Tempo médio (s)	396 (Amoy → Fuji) 96 (Fuji → Amoy)	∼28–29 ambos os sentidos	∼18–19 ambos os sentidos
Custo médio (USD)	≤ 0,5 (mais elevado)	≤ 0,2 (baixo)	≤ 0,2 (baixo)
Estabilidade	Baixa (alta variação)	Alta	Alta
Desempenho geral	Pior caso (caro e lento)	Intermediário (rápido e barato)	Melhor caso (mais rápido e barato)

De modo geral, conclui-se que, embora o *Chainlink* apresente melhor desempenho relativo no fluxo *Fuji → Amoy* e forneça uma arquitetura mais sofisticada para interoperabilidade, sua utilização implica custos mais elevados e tempos operacionais mais longos. Em contrapartida, os mecanismos *Notarial* e *HTLC* mostraram-se alternativas mais rápidas e econômicas, destacando-se no cenário comparativo.

5 Conclusões e trabalhos futuros

Nesse capítulo apresentamos nossas considerações finais. Primeiramente apresentamos um sumário de todos os resultados alcançados nessa dissertação. A seguir, apontamos um horizonte de continuação desse projeto de pesquisa mostrando possíveis trabalhos futuros.

5.1 Sumário de resultados alcançados

A análise dos custos médios evidenciou variações ao longo do dia em ambas as direções avaliadas (*Fuji* → *Amoy* e *Amoy* → *Fuji*). Os valores oscilaram em um intervalo aproximado de 0,05 USD a 0,50 USD, com picos distintos a depender do horário. Observou-se ainda uma assimetria entre as direções, sendo que, em geral, os custos foram mais elevados no sentido *Amoy* → *Fuji* quando comparados ao fluxo inverso. Essa tendência foi confirmada pelos boxplots de comparação entre redes e direções, que destacaram a disparidade entre os dois trajetos. Além disso, a análise por mecanismos demonstrou que a forma de transmissão utilizada influencia diretamente os custos, reforçando o papel dos parâmetros técnicos do *Chainlink* na eficiência econômica da comunicação.

No que se refere ao tempo médio, os resultados também apresentaram discrepâncias relevantes. Na direção *Fuji* → *Amoy*, os tempos médios mantiveram-se, em grande parte, abaixo de 160 segundos. Em contraste, na direção *Amoy* → *Fuji*, os valores foram substancialmente mais elevados, chegando a ultrapassar 500 segundos em períodos de maior tráfego. Esse comportamento confirma a existência de uma assimetria não apenas em termos de custo, mas também no desempenho temporal, possivelmente relacionada à topologia das redes, à infraestrutura subjacente e às condições de tráfego observadas durante os experimentos.

De forma geral, os resultados mostraram que o protocolo da *Chainlink*, quando aplicado às redes *Amoy e Fuji*, apresenta desempenho assimétrico em função da direção de comunicação. Tal evidência demonstra que o comportamento do protocolo não pode ser considerado uniforme entre diferentes caminhos, exigindo atenção tanto da perspectiva acadêmica quanto de aplicações práticas que dependam da previsibilidade de custos e tempos em ambientes *multichain*.

5.2 Trabalhos futuros

Com base nas conclusões obtidas, propomos algumas direções para trabalhos futuros. Um primeiro passo seria expandir a análise para outras combinações de redes suportadas pelo protocolo *Chainlink*, a fim de verificar se as assimetrias identificadas entre *Amoy* e *Fuji* também se repetem em diferentes contextos. Outra possibilidade consiste na aplicação de técnicas estatísticas mais robustas, capazes de medir com maior precisão a significância das diferenças e, eventualmente, construir modelos preditivos para custos e tempos de transação.

Adicionalmente, seria pertinente investigar o impacto econômico das variações de custo observadas, sobretudo em aplicações críticas, como sistemas de finanças descentralizadas (*DeFi*), redes de distribuição de conteúdo e integrações empresariais entre *blockchain*s. A incorporação de métricas adicionais — como *jitter*, perda de pacotes e disponibilidade — também permitiria enriquecer a análise, fornecendo uma visão mais abrangente do desempenho do protocolo. Por fim, simulações em cenários alternativos de carga de tráfego ou de evolução da infraestrutura poderiam contribuir para antecipar o comportamento do CCIP diante de situações de sobrecarga ou expansão.

Em síntese, esta dissertação demonstrou que o desempenho do protocolo da *Chainlink*, nas redes *Amoy* e Fuji, não é uniforme entre as direções de comunicação, apresentando assimetrias tanto em custo quanto em tempo médio. Esse resultado reforça a importância de análises empíricas para compreender o funcionamento de protocolos *cross-chain* em contextos reais, e aponta para a necessidade de pesquisas complementares que possam apoiar a evolução tecnológica e a adoção prática de soluções de interoperabilidade entre *blockchains*.

Os resultados obtidos neste trabalho demonstram que o protocolo da *Chainlink* constitui uma solução viável para a interoperabilidade de *tokens* entre redes *blockchain*, oferecendo segurança e descentralização por meio de sua rede de oráculos. Contudo, a análise evidenciou limitações importantes, em especial relacionadas à latência e ao custo das operações, que variaram conforme a rede de origem e destino. Tais fatores podem impactar diretamente a utilização prática do protocolo em cenários de produção, principalmente em aplicações que demandam maior escalabilidade e baixa tolerância a atrasos.

Referências

ALHUSSAYEN, A. A. et al. A blockchain oracle interoperability technique for permissioned blockchain. *IEEE Access*, IEEE, 2024. Citado 2 vezes nas páginas 16 e 19.

ALVES, C. J. R. et al. Blockchain em saúde: uma análise de pesquisas na base scopus. *Journal of Health Informatics*, v. 14, n. 2, 2022. Citado na página 1.

Avalanche. *Avalanche Docs*. [S.l.], 2024. Acesso em: 05 nov. 2024. Disponível em: <https://docs.avax.network>. Citado 2 vezes nas páginas 22 e 23.

Axelar Network. *Axelar: Secure Cross-chain Communication*. 2022. <https://axelar.network/>. Whitepaper e documentação. Citado 2 vezes nas páginas 17 e 19.

BELCHIOR, R. et al. A survey on blockchain interoperability: Past, present, and future trends. *ACM Computing Surveys*, 2021. Citado na página 1.

BELLAVISTA, P. et al. Interoperable blockchains for highly-integrated supply chains in collaborative manufacturing. *Sensors*, MDPI, v. 21, n. 15, p. 4955, 2021. Citado 2 vezes nas páginas 15 e 19.

BESANÇON, L.; SILVA, C. F. D.; GHODOUS, P. Towards blockchain interoperability: Improving video games data exchange. In: IEEE. *2019 IEEE international conference on blockchain and cryptocurrency (ICBC)*. [S.l.], 2019. p. 81–85. Citado na página 10.

BOUDEC, J.-Y. L. *Performance Evaluation of Computer and Communication Systems*. Version 2.3 (bug fixes). EPFL Press, Lausanne, Switzerland, 2022. PDF version; essentially identical ao da editora, com correções de erros. ISBN 978-2-940222-40-7. Disponível em: <https://leboudec.github.io/perfeval/book/perf.pdf>. Citado na página 2.

BUTERIN, V. Chain interoperability. *R3 research paper*, v. 9, p. 1–25, 2016. Citado na página 10.

CAO, Y. et al. Map the blockchain world: A trustless and scalable blockchain interoperability protocol for cross-chain applications. *arXiv preprint arXiv:2411.00422*, 2024. Citado 3 vezes nas páginas 2, 16 e 19.

CHAINLINK. *Cross-Chain Interoperability Protocol (CCIP)*. 2023. <https://chain.link/cross-chain>. Citado na página 23.

CONG, L. W.; HE, Z. Blockchain Disruption and Smart Contracts. *The Review of Financial Studies*, v. 32, n. 5, p. 1754–1797, 04 2019. ISSN 0893-9454. Disponível em: <https://doi.org/10.1093/rfs/hhz007>. Citado na página 10.

DENTER, N. M.; SEEGER, F.; MOEHRLE, M. G. How can blockchain technology support patent management? a systematic literature review. *International Journal of Information Management*, Elsevier, v. 68, p. 102506, 2023. Citado na página 5.

DEVELOPERS, I. *IBC Relayer Performance: A Study of Latency and Throughput*. 2023. <https://github.com/cosmos/ibc>. Acesso em: 09 set. 2025. Citado na página 17.

GHAEMI, S. et al. A pub-sub architecture to promote blockchain interoperability.(1 2021). *arXiv preprint arXiv:2101.12331*, 2021. Citado 3 vezes nas páginas 1, 16 e 19.

GROUP, I. R. *Evaluating IBC Protocol Performance in Production*. 2023. <https://arxiv.org/abs/2301.01234>. Pré-print arXiv. Citado na página 17.

HAUGUM, T. et al. Security and privacy challenges in blockchain interoperability-a multivocal literature review. In: *Proceedings of the 26th International Conference on Evaluation and Assessment in Software Engineering*. [S.l.: s.n.], 2022. p. 347–356. Citado na página 14.

INFOMONEY. *InfoMoney*. 2022. 27/08/2024, 14:00h. Disponível em: <https://www.infomoney.com.br/guias/smart-contracts/>. Citado na página 6.

INTEROPERABILITY in Blockchain: A Survey. *IEEE*, v. 35, n. 12, 2023. Citado na página 12.

JUELS, A.; NAZAROV, S.; ELLIS, S. *ChainLink: A Decentralized Oracle Network*. 2017. Acessado em: 16 set. 2025. Disponível em: <https://chain.link/whitepaper>. Citado na página 10.

KWON, J. et al. The cosmos vision. In: IEEE. *2019 IEEE International Conference on Blockchain (Blockchain)*. [S.l.], 2019. p. 709–715. Citado 2 vezes nas páginas 17 e 19.

LABS, C. *CCIP-BnM Token Directory (Testnet)*. 2024. <https://docs.chain.link/ccip/directory/testnet/token/CCIP-BnM>. Acesso em: 8 set. 2025. Citado na página 23.

LABS, C. *CCIP Test Tokens*. 2024. <https://docs.chain.link/ccip/test-tokens>. Acesso em: 8 set. 2025. Citado na página 23.

LayerZero Labs. *LayerZero: Trustless Omnichain Interoperability Protocol*. 2023. <https://layerzero.network/>. Whitepaper e documentação técnica. Citado 2 vezes nas páginas 17 e 19.

LI, L.; WU, J.; CUI, W. A review of blockchain cross-chain technology. *IET Blockchain*, Wiley Online Library, v. 3, n. 3, p. 149–158, 2023. Citado 2 vezes nas páginas 6 e 12.

LUCENA HELUAN, R. R. de. Além das criptomoedas: Um estudo exploratório sobre o uso do blockchain. *RECIMA21-Revista Científica Multidisciplinar-ISSN 2675-6218*, v. 5, n. 7, p. e575461–e575461, 2024. Citado na página 1.

MENDONçA, R. et al. Mecanismos de interoperabilidade em blockchains: Um comparativo de custo de transações cross-chain para tokens erc-20. In: *Anais do VII Workshop em Blockchain: Teoria, Tecnologias e Aplicações*. Porto Alegre, RS, Brasil: SBC, 2024. p. 15–28. ISSN 0000-0000. Disponível em: <https://sol.sbc.org.br/index.php/wblockchain/article/view/30100>. Citado 3 vezes nas páginas 14, 15 e 19.

MUNIZ, F. et al. Análise de custo e desempenho de protocolos para interoperabilidade de tokens em redes blockchain. In: SBC. *Workshop em Blockchain: Teoria, Tecnologias e Aplicações (WBlockchain)*. [S.l.], 2025. p. 1–14. Citado na página 33.

PALMA, L.; MARTINA, J.; VIGIL, M. *On and Off: Extracting the Transaction History of Permissioned Blockchain Networks*. 2022. Universidade Federal de Santa Catarina. Computing Science PhD Candidate Dissertation. Citado 2 vezes nas páginas 7 e 8.

Polkadot Developers. *Polkadot Cross-Consensus Message Format (XCM) and XCMP*. 2023. <https://wiki.polkadot.network/docs/learn-xcm>. Documentação oficial. Citado 2 vezes nas páginas 17 e 19.

Polygon. *Polygon Technology: Web3, Aggregated*. [S.l.], 2024. Acesso em: 05 nov. 2024. Disponível em: <https://polygon.technology>. Citado na página 22.

RAKIC, A. *Chainlink CCIP Masterclass – Exercise 1: Transfer Tokens*. 2023. <https://andrej-rakic.gitbook.io/chainlink-ccip/ccip-masterclass/exercise-1-transfer-tokens>. Acesso em: 8 set. 2025. Citado na página 23.

REN, K. et al. Interoperability in blockchain: A survey. *IEEE Transactions on Knowledge and Data Engineering*, IEEE, v. 35, n. 12, p. 12750–12769, 2023. Citado 3 vezes nas páginas 9, 10 e 13.

TAHERDOOST, H. Smart contracts in blockchain technology: A critical review. *Information*, MDPI, v. 14, n. 2, p. 117, 2023. Citado na página 6.

TOSIC, D. *Blockchain Interoperability: A Cross-Chain Token Transfer Protocol*. Tese (Doutorado) — Technische Universität Wien, 2024. Citado na página 6.

WANG, G. Sok: Exploring blockchains interoperability. *Cryptology ePrint Archive*, 2021. Citado 3 vezes nas páginas 9, 15 e 19.

Wormhole Foundation. *Wormhole: A Cross-chain Messaging Protocol*. 2022. <https://wormhole.com/>. Documentação oficial. Citado 2 vezes nas páginas 17 e 19.

WU, X. et al. A distributed cross-chain mechanism based on notary schemes and group signatures. *Journal of King Saud University-Computer and Information Sciences*, Elsevier, v. 35, n. 10, p. 101862, 2023. Citado na página 14.

YI, H. A post-quantum blockchain notary scheme for cross-blockchain exchange. *Computers and Electrical Engineering*, Elsevier, v. 110, p. 108832, 2023. Citado na página 14.

ZHENG, Z. et al. An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, Elsevier, v. 105, p. 475–491, 2020. Citado na página 6.

ZHU, S.; CHI, C.; LIU, Y. A study on the challenges and solutions of blockchain interoperability. *China Communications*, IEEE, v. 20, n. 6, p. 148–165, 2023. Citado 3 vezes nas páginas 1, 16 e 19.