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

Fredison Muniz[1], **Ronan D. Mendonça**[2]
Emanuel F. de Miranda[1], **Ítallo W. F. Cardoso**[2], **Rafael Coelho**[3]
Alex B. Vieira[3], **José A. M. Nacif**[2], **Glauber D. Gonçalves**[1]

[1] Departamento de Ciência da Computação - UFPI
[2] Departamento de Informática - UFV
[3]Departamento de Ciência da Computação - UFJF

{fredisonmuniz, emanuelmiranda.si, ggoncalves}@ufpi.edu.br

{ronan.dutra,itallo.cardoso,jnacif}@ufv.br

{alex.borges,rafael.coelho}@ufjf.edu.br

Abstract. *Blockchain is a disruptive technology with potential applications in several sectors, such as agriculture, industry, and services. However, interoperability between different blockchains, which allows communication and data exchange between them, is still a challenge. Some protocols have been proposed to address this issue, but performance analyses in real scenarios are lacking. This work proposes a comparison between state-of-the-art interoperability protocols: Chainlink, which is provided via proprietary infrastructure and is currently the most popular, and the Notarial and Hash Block protocols implemented in this work. We conducted experiments with several transactions between different blockchain networks and showed that the Chainlink protocol, despite its popularity, can be up to seven times slower than other protocols and with higher fees reaching up to 78 cents per transaction, highlighting the wide room for innovation in blockchain network interoperability.*

Resumo. *Blockchain é uma tecnologia disruptiva, com potencial de aplicações em diversos setores, como agricultura, indústria e serviços. No entanto, a interoperabilidade entre diferentes blockchains, que permite a comunicação e troca de dados entre elas, ainda é um desafio. Alguns protocolos vem sendo propostos para tratar essa questão, mas faltam análises de desempenho deles em cenários reais. Este trabalho propõe uma comparação entre protocolos de interoperabilidade estado da arte: Chainlink, que é provido via infraestrutura proprietária, sendo o mais popular atualmente, e os protocolos Notarial e Bloqueio de Hash, implementados neste trabalho. Conduzimos experimentos com várias operações entre redes blockchain distintas e mostramos que o protocolo Chainlink, a despeito de sua popularidade, pode ser até sete vezes mais lento que os outros protocolos e com tarifas maiores, alcançando até 78 centavos de dólar por operação, evidenciando o amplo espaço para inovação em interoperabilidade de redes blockchain.*

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. [de Lucena 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 et al. 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.

Neste trabalho buscamos preencher essa lacuna com as seguintes contribuições:

1. Metodologia para comparar protocolos de interoperabilidade baseado em ambiente realista para aplicações descentralizadas;
2. Analise 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, aplicamos o uso desse três mecanismo de interoperabilidade em um am-

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

biente realista, baseado em redes de testes *blockchains*. Em seguida, implantamos o protocolo da *Chainlink* e os protocolos Bloqueio de Hash e o Esquema Notarial 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 próximas seções têm a seguinte organização. Na Seção 2, apresentamos os trabalhos relacionados. Na Seção 3 descrevemos os protocolos que são o foco da análise nesse artigo. A metodologia utilizada para a análise é apresentada na Seção 4, ao passo que os resultados são apresentados na Seção 5. Finalmente, a Seção 6 expõe as considerações finais e trabalhos futuros.

2. Trabalhos Relacionados

A interoperabilidade entre redes *blockchain* é um campo de pesquisa recente, repleto de oportunidades para contribuições tanto na academia quanto na indústria. O avanço prático e significativo da usabilidade das *blockchains* depende do desenvolvimento de técnicas e soluções distintas. Seja por meio de abordagens baseadas em Cadeias, Pontes ou Aplicações Descentralizadas (DApp), ainda há diversas questões em aberto que precisam ser exploradas.

No trabalho de [Wang 2021], uma revisão sistemática sobre os avanços e desafios da 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 trabalho, são discutidas ainda, soluções práticas, como *atomic swaps* e protocolos de comunicação *cross-chain*. Assim, os autores não trazem uma metodologia concreta sobre o funcionamento dos protocolos.

O estudo de [Mendonça et al. 2024] compara os métodos e custos de interoperabilidade de *tokens* ERC-20 nos protocolos Notarial e Bloqueio de Hash. Nos experimentos, os autores monitoraram duas métricas de rede em ambos os protocolos, tanto na *blockchain* de origem quanto na de destino, em todas as fases do processo (o consumo de GAS necessário para as transações e o tempo gasto para sua efetivação). A avaliação foca na análise de desempenho dos métodos Notarial e Bloqueio de Hash, ambos teóricos, mas não inclui comparações com protocolos amplamente utilizados na prática, como o CCIP.

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 apresentam também um protótipo que mede a latência e avalia o impacto de interações entre redes *blockchains*, contudo 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 denominado MAP, para interoperabilidade entre redes *blockchain*, destacando soluções baseadas em prova de conhecimento zero (*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 há avaliações de desempenho para a análise desses problemas.

Em [Zhu et al. 2023], são discutidos os desafios da interoperabilidade em *blockchain* e proposto um *frameworks* baseados em *side-chains* e pontes *cross-chain*. Os autores mostram também uma tabela comparativa de soluções de interoperabilidade (Cosmos, Polkadot, Aion, dentre outras), destacando características como: protocolo utilizado (e.g., HTLC, *sidechains*, etc.); Mecanismo *cross-chain* de gerenciamento de segurança e tipo de *blockchain* usada (pública, privada, Consórcio). Apesar da contribuição, não foram discutidas metodologias para a avaliação de custos e desempenho dos protocolos de interoperabilidade mencionados nesse trabalho.

Em [Alhussayen et al. 2024] propõe uma técnica de interoperabilidade baseada em oráculos, projetada especificamente para plataformas *blockchains* permissionadas. Os autores apresentam a arquitetura da técnica e implementam um protótipo para demonstrar sua viabilidade, além de medir a latência das transações entre redes. O projeto conecta as plataformas *Hyperledger Fabric* e *Corda*. No entanto, embora a avaliação tenha focado em redes permissionadas e na latência das transações, várias questões permanecem em aberto, como o custo de processamento e a forma de cobrança durante as transações

O trabalho de [Ghaemi et al. 2021], consiste em uma solução de interoperabilidade entre *blockchains* permissionadas baseada na arquitetura publicar/assinar. Essa abordagem visa facilitar a transferência de ativos e dados entre diferentes redes, que frequentemente operam de forma isolada, criando silos de informações e ativos. Os autores dessa solução implementaram um protótipo que integra diferentes redes *blockchain*, como o *Hyperledger Besu* (um cliente Ethereum) e duas versões distintas da plataforma *Hyperledger Fabric*. O desempenho da rede foi analisado usando uma ferramenta de *benchmark* para identificar os limites e gargalos da solução proposta, entretanto na análise de desempenho dos autores, não há comparativos com as soluções de interoperabilidade já em uso.

3. Protocolos de Interoperabilidade

Neste trabalho definimos como protocolo de interoperabilidade, mecanismos ou técnicas que podem ser utilizadas com o objetivo de transferir ou trocar *tokens* entre redes *blockchain* distintas. Nesse sentido, focamos em três protocolos cujas eficiências acerca desse objetivo vem sendo alvo de pesquisas e discussões recentes: *Hash Time Lock* (HTLC), Mecanismo Notarial *(*Notary) e o protocolo CCIP da Chainlink.

3.1. Hash Time Lock Contract(HTLC)

O mecanismo de bloqueio de *hash* ou *Hash Time Lock Contract* (HTLC) representa um marco significativo na evolução dos protocolos de troca entre *blockchains*, proporcionando uma solução inovadora para realizar transações entre redes sem depender de intermediários confiáveis [Ou et al. 2022]. Ao implementar contratos nas *blockchains* envolvidas na negociação, o processo de troca de ativos via HTLC se torna seguro e confiável. Esses contratos atuam como uma garantia, bloqueando os ativos envolvidos até que as condições acordadas sejam atendidas. A utilização do conceito de *hash* criptográfico, que transforma dados de qualquer tamanho em uma sequência fixa de caracteres, insere uma camada adicional de segurança, criando uma trava com uma palavra secreta que deve ser correspondente em ambas as extremidades da transação. Além disso, a imposição de um limite de tempo para a conclusão da troca aumenta a eficiência e a segurança do processo. Em caso de não cumprimento dentro do prazo estipulado, o contrato automaticamente

cancela a transação, revertendo os *tokens* para suas respectivas carteiras de origem. Esse protocolo desempenha um papel fundamental na facilitação de trocas descentralizadas, promovendo a confiança e a segurança nas transações *blockchain* [Belchior et al. 2021].

A Figura 1 ilustra o processo do HTCL, demonstrando como os dois contratos funcionam juntos para garantirem a segurança e a atomicidade da transação.

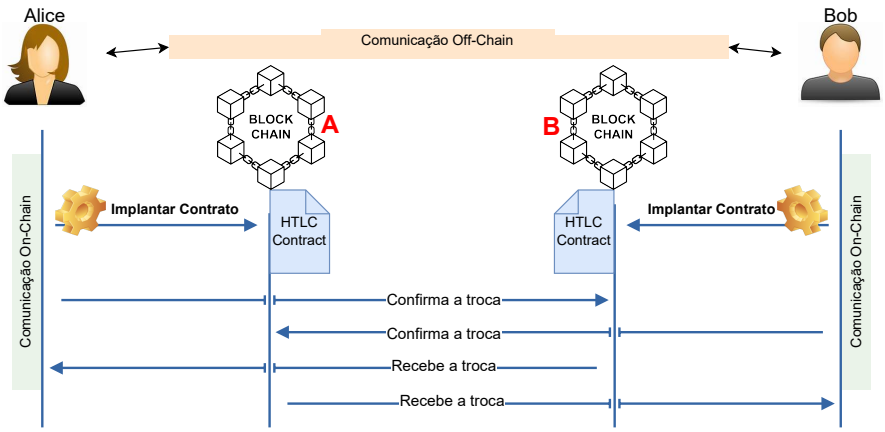


Figura 1. Arquitetura implementada para o protocolo *Hash-Time Lock*.

No contexto do protocolo de bloqueio de *hash*, conforme a Figura 1, o usuário Alice deseja transferir em troca de seu *token* para uma conta do usuário Bob em outra rede. Para fazer essa transferência, ela escolhe uma ”palavra secreta”, e utiliza o *Hash* juntamente ao endereço de Bob para criar o contrato HTLC. Por meio do contrato criado na *blockchain* A, o contrato bloqueia o *token* A para a transferência ser realizada. De maneira similar, o Usuário Bob implanta o contrato de HTLC na *blockchain* B com o endereço de Alice e a palavra secreta em *Hash*. Sendo assim, o Usuário Alice faz a retirada do *token* B na *blockchain* B com sua palavra secreta, isto é, a etapa de (*withdraw*) do contrato HTLC. Ao fazer isso, a palavra secreta pode ser usada por Bob para retirar o *token* A da *blockchain* A.

3.2. Notarial

O mecanismo notarial é uma forma de implementar a interoperabilidade entre cadeias de forma relativamente simples. Ele consiste em verificar e encaminhar mensagens entre cadeias por meio de uma entidade confiável intermediária chamada de Notário. Quando há troca e/ou transferência de ativos entre diferentes *blockchains*, uma ou mais organizações são designadas como notários para monitorar eventos entre as cadeias, e alcançar um consenso sobre a ocorrência do evento por meio de um algoritmo de consenso específico, e, por fim, responder de forma tempestiva [Belchior et al. 2021]. O mecanismo notarial se divide em mecanismo notarial de assinatura única e de múltiplas assinaturas [Ou et al. 2022].

O mecanismo notarial de assinatura única, também denominado mecanismo notarial centralizado, consiste em designar um único nó ou instituição independente para atuar como notário, e o notário assume as tarefas de coleta de dados, verificação e confirmação de transações no processo de interação entre cadeias. O notário é composto por, pelo

menos, uma conta nas cadeias de origem e de destino. Este mecanismo consegue ter um processamento rápido de transações e é bastante adaptável, apesar do escopo restrito, limitando-se a troca de ativos.

No mecanismo notarial de múltiplas assinaturas o notário é geralmente composto por vários nós, onde cada nó possui uma chave e somente quando uma determinada porcentagem destes nós assinam em conjunto é que há um consenso e as transações entre cadeias podem ser confirmadas. Durante a verificação da transação, uma parte dos notários é selecionada aleatoriamente do grupo notarial, diminuindo o grau de dependência da confiabilidade dos notários [Yang et al. 2019]. A Figura 2 ilustra esse mecanismo.

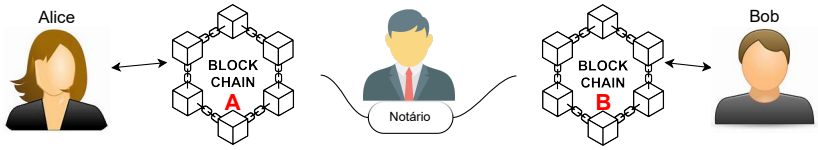


Figura 2. Arquitetura do mecanismo notarial.

Na arquitetura do mecanismo notarial da Figura 2, 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 Alice (remetente) na *blockchain* A, transferindo-o para o usuário Bob (destinatário) na *blockchain* B e registrando informações sobre as transações realizadas. O Notário deve garantir a entrega segura dos recursos ao destinatário designado.

3.3. Chainlink

O protocolo CCIP é usualmente categorizado como um protocolo *relay* agnóstico, mas com suporte adicional fornecido por uma rede descentralizada de oráculos (semelhante ao esquema notarial) para garantir a segurança, verificabilidade e execução confiável das mensagens entre redes *blockchain* [Chainlink 2024]. Esse protocolo visa atender à crescente demanda por interações complexas entre cadeias, estabelecendo uma conexão universal entre redes *blockchains* por meio de uma única interface. Ele foi desenvolvido para ser altamente compatível, permitindo integração com uma variedade de serviços de oráculo dentro de uma estrutura de ponte de *tokens* programável para oferecer suporte a interações e aplicações entre cadeias.

A Figura 3 mostra a arquitetura do protocolo CCIP, onde roteadores são contratos inteligentes que fornecem uma interface para usuários. A partir dessa interface os usuários podem chamar funções de contrato inteligente ou transferir *tokens* para um contrato inteligente ou conta EOA (*Externally Owned Account*) em uma *blockchain* diferente, além de enviar mensagens e *tokens* arbitrários dentro da mesma transação.

O componente "Rede de Gerenciamento de Risco" na Figura 3 oferece um sistema robusto de segurança em profundidade com camadas adicionais de proteção como limites de taxa de transferência. Esse componente ainda facilita transferências de *tokens* simplificados e seguros entre *blockchains*, permitindo que empresas escalem suas bases de usuários de forma ágil, sem a necessidade de desenvolver soluções personalizadas.

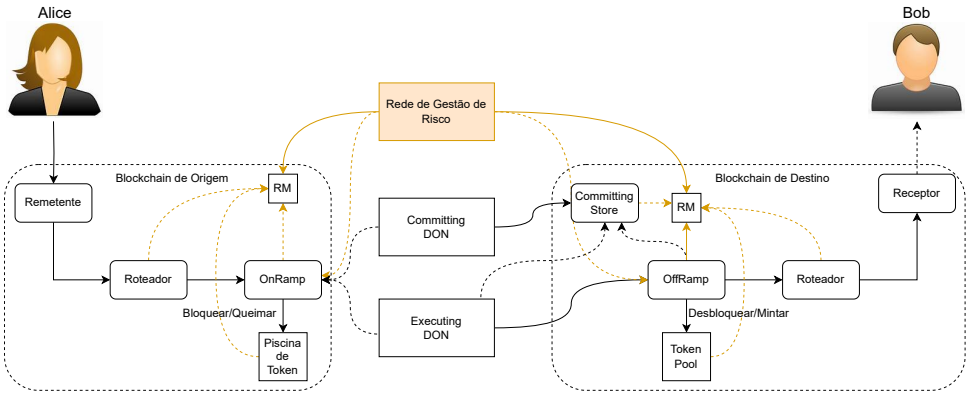


Figura 3. Arquitetura básica do CCIP, adaptado de [Campos et al. 2024].

Além disso, há o suporte a transferências programáveis, em que *tokens* e instruções de uso podem ser enviados a contratos inteligentes em outras *blockchains* para execução de operações como troca ou *staking* ao chegarem à cadeia de destino.

Por sua vez, o mecanismo de pagamento com taxa bloqueada do protocolo garante a execução confiável de transações, mesmo em condições de picos de congestionamento. Com uma interface de fácil integração, os proponentes do CCIP visam proporcionar uma experiência unificada de desenvolvimento entre cadeias, permitindo que desenvolvedores criem aplicações seguras e inovadoras. Aplicações baseadas no protocolo CCIP podem começar a transferir *tokens* entre cadeias rapidamente, utilizando o componente *Pool de Tokens* onde contratos auditados gerenciam a complexidade de queima ou bloqueio de *tokens* entre *blockchains*. Além disso, os patrocinadores de *tokens* mantêm controle total sobre seus contratos de pool ao utilizar o CCIP.

Em suma, o protocolo CCIP visa oferecer transferências de *tokens* altamente seguras, contando com contratos inteligentes auditados e recursos de segurança adicionais, como limites de taxa configuráveis para limitar o valor transferido em um intervalo de tempo específico, definidos em colaboração com o emissor do *token*. Isso proporciona uma camada extra de segurança para transferências de *tokens* sem permitir mensagens arbitrárias. A composição aprimorada do CCIP aumenta a utilidade dos *tokens*, facilitando a expansão de sua base de usuários e permitindo que parceiros do ecossistema transfiram e desenvolvam novas funcionalidades para seus *tokens* por meio de uma única interface.

4. Metodologia

Nesta seção é descrita a metodologia para analisar desempenho e custo dos três protocolos de interoperabilidade foco deste artigo. Primeiramente, descrevemos o ambiente experimental utilizado que consistem em redes de testes de duas *blockchains* públicas populares para desenvolvedores de aplicações descentralizadas. A seguir, detalhamos o ambiente experimental desenvolvido nessas redes e as métricas utilizadas para a análise.

4.1. Ambiente Experimental

Algumas plataformas *blockchains* possuem redes de testes, as (*Testnets*), que são ambientes de testes que possibilitam desenvolver, experimentar e validar aplicativos, contratos

inteligentes e funcionalidades antes de uma implementação real na rede *blockchain* principal, (a *mainnet*). As redes de testes conseguem replicar o comportamento da rede principal, com algumas diferenças importantes: Os *tokens* não têm valor financeiro (não se aplica ou retira moeda financeira); Possibilita o uso de contratos inteligentes sem colocar em risco os softwares, fundos e usuários reais da rede; A acessibilidade aos ambientes, pois os desenvolvedores podem obter gratuitamente *tokens* das redes de testes gratuitamente através de ”faucets”; As medidas de tempo das redes de testes dificilmente serão iguais às redes de produção, logo o número de transações nas redes principais são bem maiores do que nas redes de testes e isso pode alterar consideravelmente o valor das taxas de transações cobradas, como também o valor do GAS, mas as redes de testes e principais utilizam os mesmos métodos na hora de realizar e taxar as operações. Como o objetivo é avaliar custo e desempenho dos três protocolos citados, a diferença de valores avaliadas entre os protocolos terá a mesma proporção se compararmos os resultados das redes de testes com as redes principais.

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* (*Proof-of-Stake*), 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 *testnet* do Ethereum) como sua cadeia raiz (L1), garantindo uma infraestrutura sustentável. Essa configuração permite que desenvolvedores continuem contando com validadores essenciais, ferramentas de infraestrutura, ”*faucets*”e outros recursos necessários para o desenvolvimento eficiente. [Polygon 2024]

A Avalanche Fuji, rede de testes oficial da Avalanche, possibilita que desenvolvedores testem aplicações descentralizadas (dApps) e contratos inteligentes sem custos financeiros associados às transações. A Avalanche é uma plataforma *blockchain* de alto desempenho que utiliza o protocolo de consenso Avalanche (baseado em *proof of stake*, conhecido por sua baixa latência e capacidade de processar milhares de transações por segundo (TPS).

Apesar das redes de testes não consumirem valores financeiros reais, e sim ”faucets”que são fornecidos gratuitamente, vale ressaltar que, cada rede *blockchain* tem seu próprio *token* para transações. A Polygon utiliza o *token* chamado POL como sua moeda, enquanto a Avalanche utiliza o AVAX com *token* da sua moeda. 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 [Labs 2025]. Assim como as outras redes de testes de *blockchain*, as redes Chainlink utilizam o *token Link* como moeda da plataforma. Esses *tokens* de testes podem ser obtidos gratuitamente por meio de ”faucets”específicos para cada *testnet*. Através da Chainlink é possível testar aplicações de vários ecossistemas, pois ela suporta várias plataformas *blockchains*, como *Ethereum*, Polygon, Avalanche e etc.. Por fim, a plataforma Chainlink é compatível com as redes de

testes Amoy e Fuji utilizadas como redes de testes dos experimentos nesse trabalho.

O mecanismo Notarial necessita de um terceiro confiável para gerenciar as transações entre a *blockchain* de origem e destino. Dessa maneira, abstraímos o terceiro confiável por meio de um contrato inteligente. Esse contrato atua como o Notário do mecanismo recebendo o *token* do remetente da rede "A", e o transferindo para o destinatário na rede "B". Esse mecanismo possui limitações de segurança, atuando de maneira centralizada, sendo assim a transação depende da integridade do Notário. Se o Notário for comprometido, pode ocasionar perdas financeiras aos usuários das redes.

O mecanismo HTLC necessita de implementação de contratos inteligentes responsáveis pela troca segura dos ativos. Esses contratos são implantados nas duas redes e possuem métodos de conectá-las. Como nesse mecanismo não há um terceiro confiável, o contrato atua sincronizando as redes com as funções de verificação das transações, da palavra secreta e a devolução dos valores, caso seja necessário abortar a transação. Sendo assim, o contrato para o 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. Caso o tempo tenha ultrapassado o período de bloqueio, o contrato é capaz de devolver a quantia para o remetente.

4.2. Configurações e Métricas

A preparação do ambiente para a execução dos experimentos se deu por meio de scripts implementados na linguagem *Javascript* e contratos inteligentes na linguagem *Solidity*. Os experimentos foram executados à partir da configuração da ferramenta nativa do Linux "Crontab"em uma máquina virtual da AWS-EC2[2]. Crontab é utilizado para agendamento e execução de comandos e scripts de maneira recorrente. Desse ponto em diante, configuramos as execuções por agendamentos via Crontab para que a cada 30 minutos fosse enviada uma transação para a rede Amoy e outra para a rede Fuji. Também foram agendadas, a cada 30 minutos, envio de uma transação da rede Fuji para a rede Amoy, mas com uma diferença de 5 minutos entre o envio Amoy/Fuji e Fuji/Amoy. As transações em questão são transferências de *tokens* ERC-20 entre contas distintas em cada uma dessas redes testadas.

O tempo de operação para a interoperabilidade entre redes *blockchain*, no caso, utilizando a Chainlink, depende de vários fatores que podem ser determinantes no tempo de execução total da transação. Nas redes *blockchains*, uma transação para ser confirmada, antes é necessário um processo de verificação e depois de validação. Os Oráculos da Chainlink estão sendo usados para que a interoperabilidade entre as redes Amoy e Fuji aconteçam, sendo assim, os Oráculos precisam de tempo para obter dados da rede de origem, em seguida processar e validar tais dados e por fim, publicar os dados na rede de destino. Outro ponto importante é que o tempo necessário para a obtenção desses dados depende da rede que está sendo utilizada. Congestionamento de rede, prioridade de taxa de GAS ou até mesmo a complexidade dos contratos podem influenciar no tempo total da transação. Em nossos experimentos as transações foram feitas de duas formas paralelamente: Amoy como rede de origem, Fuji como rede de destino e vice-versa. Para um estudo e avaliação do tempo e tarifa aplicadas nessas transações, optamos por

[2]Amazon Web Services - Elastic Compute Cloud - https://docs.aws.amazon.com/ec2

configurar o envio de uma transação a cada 30 minutos com intervalo de 5 minutos entre o envio da Amoy para Fuji e Fuji para Amoy.

As tarifas cobradas para transações de interoperabilidade de *blockchains* são definidas com base em uma combinação de fatores e estão diretamente ligadas às redes que usarão o serviço, nesse caso a Amoy e Fuji, e aos Oráculos da Chainlink. A junção desses fatores resulta no valor tarifário total a ser cobrado pelo serviço de interoperabilidade. De modo geral, quem paga a tarifa é a rede de origem, ou seja, na transação da rede Amoy para a rede Fuji, a Amoy paga uma taxa para envio da transação e paga outra taxa pelo uso do Oráculo da Chainlink. A rede de destino também paga uma taxa pela transação feita na Chainlink. Como cada rede tem sua própria moeda, baseando-se no exemplo citado, ficaria da seguinte forma: Amoy sendo rede de origem, paga duas taxas na moeda AVAX para a Chainlink e a Fuji como destino paga uma taxa em POL para a Chainlink.

5. Resultados

Discutimos nessa seção os resultados da análise comparativa entre o protocolo de interoperabilidade da *Chainlink*, que é provido via infraestrutura dessa empresa com o seu serviço de Oráculo, e os protocolos Notarial e HTLC, que foram implementados nesse trabalho de acordo com propostas recentes da literatura. Portanto, a análise visa comparar o protocolo proprietário a dois protocolos abertos com as métricas definidas e apresentadas. Onde, o aspecto desempenho é medido em termos de tempo da operação de interoperabilidade e o aspecto custo é medido em termos de valores da tarifa dessa operação.

5.1. Desempenho em tempo de operação

A Figura 4 apresenta a distribuição de tempos de operação para os três mecanismos nas duas direções de redes origem e destino, i.e., da rede Amoy para Fuji, assim como Fuji para Amoy. O gráfico 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*).

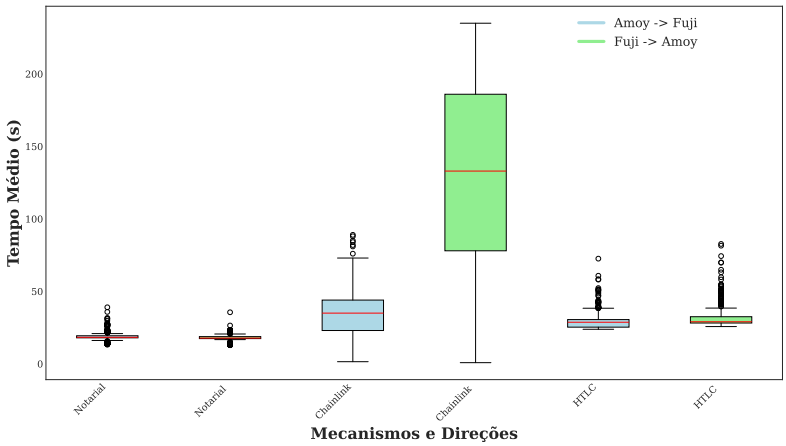
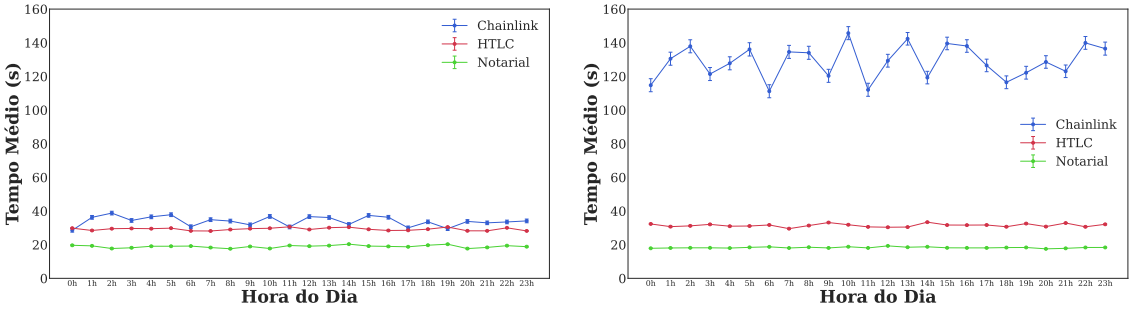


Figura 4. Distribuição do tempo de operação.

Observa-se na Figura 4 que o protocolo Notarial apresenta distribuição de tempos de operação com valores menores, ao passo que o protocolo Chainlink tem valores maiores, e o HTLC ocupa a posição intermediária. Portanto, o protocolo Notarial tem melhor desempenho em termos de tempo de operação, o que é explicado devido à sua simplicidade, i.e., envolver apenas uma entidade central, o Notário, para interoperar *tokens* entre duas redes. Em contraste, o protocolo Chainlink pode ser até sete vezes mais lento que o Notarial em termos de valores medianos, i.e., tempos de 133 segundos no sentido Fuji para Amoy contra 18 segundos para o Notarial na mesma direção, como mostra a Figura 4. No sentido oposto, Amoy para Fuji, os tempos medianos são 35 segundos para o Chainlink e 18 segundos para o Notarial. Por sua vez, o protocolo HTLC tem desempenho intermediário, com tempos medianos de operação de 29 segundos no sentido Fuji-Amoy e Amoy-Fuji [3]. Esse tempo é próximo ao Notarial, mas diferentemente deste, o HTLC é totalmente descentralizado, como descrevemos na Seção 3.1.

O menor desempenho do protocolo Chainlink em comparação aos demais se deve principalmente à sobrecarga que a rede de validadores da Chainlink exerce para interoperar *tokens* entre as redes de origem e destino (ver Seção 3.3). Tal sobrecarga impacta também na direção da operação, visto que a origem Fuji para Amoy é notavelmente mais lenta, enquanto nos demais protocolos esse impacto não é observado. O protocolo CCIP da Chainlink implementa uma rede de gerenciamento de riscos que aprimora a segurança e o monitoramento entre as redes. Sendo assim, esse gerenciamento compromete-se em realizar operações mais seguras e confiáveis, porém despende de um maior tempo e consequentemente um maior custo devido as transações extras inerentes à implementação do protocolo.



(a) Amoy para Fuji **(b) Fuji para Amoy**

Figura 5. Tempo médio de operação ao longo do dia com erro da média em confiança de 95%.

Analisamos também o tempo de operações, distribuído ao longo das horas dia (horário GMT), para maior detalhamento no desempenho dos protocolos . A Figura 5 mostra esses tempos via médias e seus respectivos erros com intervalo de confiança em 95%. É possível observar maior instabilidade no protocolo Chainlink ao longo do dia, especialmente na direção Fuji-Amoy onde o tempo médio das operações variam entre 110 e 150 segundos. Os protocolos Notarial e HTLC, ao contrário, permanecem com tempos de operações estáveis ao longo do dia com tempos médios inferiores a 40 segundos (i.e., menos de um minuto) por operação. Novamente, nota-se que esses dois protocolos

[3]Os tempos de interação de usuários humanos na operação são desconsiderados

tem desempenhos muito similares: os tempos médios de Notarial e HTLC se mantém majoritariamente em 20 e 35 segundos ao longo do dia respectivamente, sem diferenças significativas em algumas horas, i.e., há sobreposições entre erros das médias.

5.2. Custo em tarifas da operação

A Figura 6 apresenta a distribuição de custos de operação para os três mecanismos nas duas direções de redes origem e destino. *Boxplots* são utilizados assim como na Figura 4, mas aqui representando o custo total de tarifas por operação em cada mecanismo, convertidos em dólar americano (USD). É importante observar que cada rede envolvida na operação de interoperabilidade tem tarifa distinta expressa no valor do *token* nativo da rede (i.e., POL na Amoy, Avax na Fuji e Link na Chainlink). Logo, convertemos os valores de cada tarifa em USD de acordo com a cotação no momento da operação para fins de análise do custo de interoperabilidade.

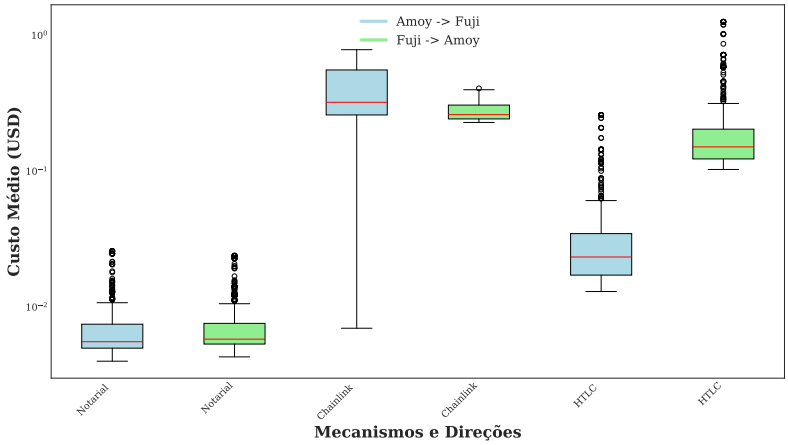
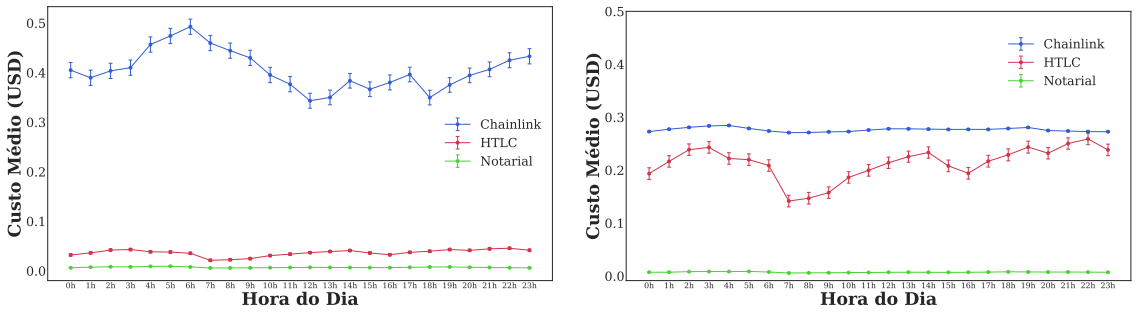


Figura 6. Distribuição do custo de operação.

Observa-se na Figura 6 que o protocolo Notarial tem o menor custo, i.e., cerca de 90% das operações (indicador do percentil 90^o.) tem valores abaixo de 1 centavo de dólar. Por sua vez, os protocolos Chainlink e HTLC tem valores entre 10 centavos e 1 dólar. Em particular, o custo da Chainlink é maior (90% das operações entre 20 e 80 centavos de dólar) devido ao maior número de partes envolvidas para interoperar *tokens*, i.e., acrescenta-se a tarifa em Link para os validadores da rede Chainlink e as tarifas das redes de origem e destino da operação. Nesse caso, observamos que a rede de destino tem maior impacto no custo Chainlink, dado que a direção Amoy-Fuji tem distribuição de valores de custos superior e o *token* Avax tem custo em dólar superior ao POL atualmente.

A Figura 6 mostra também que o protocolo HTLC é, notavelmente, impactado pela direção da operação. Isso ocorre porque a rede de origem é responsável pela implementação do contrato na *blockchain*, ao passo que a rede de destino realiza apenas a transação de resgate dos *tokens* bloqueados pela origem previamente, como foi descrito na Seção 3.1. Usualmente, implementação de contratos tem custo computacional (gas) maior em redes *blockchain*, e por conseguinte tarifa maior. Logo, a direção Fuji-Amoy tem custo maior, pois o custo mais elevado do *token* Avax na rede Fuji para a implementação do contrato torna o HTLC mais oneroso nessa direção.

Detalhamos o custo de operação dos protocolos distribuído ao longo das horas dia (horário GMT), assim como na análise de desempenho. A Figura 7 mostra esses custos em dólar (USD) via médias e seus respectivos erros com intervalo de confiança em 95%. É possível observar, dessa vez, alta instabilidade ao longo do dia não apenas no protocolo Chainlink, mas também HTLC. O custo do protocolo Chainlink tem alta variação na direção Amoy-Fuji devido o impacto da tarifa Fuji na origem da rede (i.e., *token* Avax tem maior custo em dólar), fazendo que os custos médios variem de 30 a 50 centavos USD, enquanto os demais protocolos tem custos estáveis abaixo de USD 5 centavos. Por sua vez, essa mesma questão impacta o protocolo HTLC na direção Fuji-Amoy.



(a) Amoy para Fuji **(b) Fuji para Amoy**

Figura 7. Custo médio de operação ao longo do dia com erro da média em confiança de 95%.

6. Considerações Finais

A interoperabilidade de *blockchains* possibilita uma gama de soluções antes fragmentadas no universo *blockchain*. Avaliamos o desempenho das transações em redes *blockchains* utilizando a *Chainlink* com o seu protocolo CCIP, o protocolo Notarial e o HTLC, levando em consideração métricas de tempo de processamento e custo operacional de transação. Os resultados evidenciam que cada abordagem possui vantagens e desafios distintos, dependendo do cenário da aplicação. Para trabalhos futuros, pretendemos analisar a escalabilidade e mitigação a ataques específicos, além de avaliar outros modelos híbridos que combinem a eficiência de cada um dos protocolos de interoperabilidade.

Referências

Alhussayen, A. A., Jambi, K., Khemakhem, M., and Eassa, F. E. (2024). A blockchain oracle interoperability technique for permissioned blockchain. *IEEE Access*.

Alves, C. J. R., dos Reis, L. T. P., Neto, L. R., da Silva, D. O., and da Costa, C. A. (2022). Blockchain em saúde: uma análise de pesquisas na base scopus. *Journal of Health Informatics*, 14(2).

Belchior, R., Vasconcelos, A., Guerreiro, S., and Correia, M. (2021). A survey on blockchain interoperability: Past, present, and future trends. *Acm Computing Surveys (CSUR)*, 54(8):1–41.

Bellavista, P., Esposito, C., Foschini, L., Giannelli, C., Mazzocca, N., and Montanari, R. (2021). Interoperable blockchains for highly-integrated supply chains in collaborative manufacturing. *Sensors*, 21(15):4955.

Campos, J. N., Mendonça, R. D., Fontinele, A., de Carvalho, L. H. S., Oliveira, I. R., Ítallo W. F. Cardoso, Coelho, R., Freitas, A. E. S., Gonçalves, G. D., Nacif, J. A. M., and Vieira, A. B. (2024). Finanças descentralizadas em redes blockchain: Perspectivas sobre pesquisa e inovação em aplicações, interoperabilidade e segurança. In *Jornada de Atualização em Informática (JAI) - CSBC 2024*. Sociedade Brasileira de Computação.

Cao, Y., Cao, J., Bai, D., Wen, L., Liu, Y., and Li, R. (2024). Map the blockchain world: A trustless and scalable blockchain interoperability protocol for cross-chain applications. *arXiv preprint arXiv:2411.00422*.

Chainlink (2024). Blockchain Agnostic: What, Why, and How? `https://chain.link/education-hub/blockchain-agnostic`. Acesso em: 04 de novembro de 2024.

de Lucena, Heluan, R. R. (2024). Além das criptomoedas: Um estudo exploratório sobre o uso do blockchain. *RECIMA21-Revista Científica Multidisciplinar-ISSN 2675-6218*, 5(7):e575461–e575461.

Ghaemi, S., Rouhani, S., Belchior, R., Cruz, R. S., Khazaei, H., and Musilek, P. (2021). A pub-sub architecture to promote blockchain interoperability.(1 2021). *arXiv preprint arXiv:2101.12331*.

Labs, C. (2025). Using testnet oracles - chainlink documentation. Acessado em: 24 jan. 2025.

Mendonça, R., Ítallo Cardoso, Coelho, R., Campos, J., Gonçalves, G., Vieira, A., and Nacif, J. (2024). Mecanismos de interoperabilidade em blockchains: Um comparativo de custo de transações cross-chain para tokens erc-20. In *Anais do WBlockchain*, pages 15–28.

Ou, W., Huang, S., Zheng, J., Zhang, Q., Zeng, G., and Han, W. (2022). An overview on cross-chain: Mechanism, platforms, challenges and advances. *Computer Networks*.

Polygon (2024). *Polygon Technology: Web3, Aggregated*. Acesso em: 05 nov. 2024.

Wang, G. (2021). Sok: Exploring blockchains interoperability. *Cryptology ePrint Archive*.

Yang, W., Aghasian, E., Garg, S., Herbert, D., Disiuta, L., and Kang, B. (2019). A survey on blockchain-based internet service architecture: requirements, challenges, trends, and future. *IEEE access*, 7:75845–75872.

Zhu, S., Chi, C., and Liu, Y. (2023). A study on the challenges and solutions of blockchain interoperability. *China Communications*, 20(6):148–165.