Universidade Federal de Juiz de Fora
Instituto de Ciências Exatas
Bacharelado em Ciência da Computação

Mecanismos de Interoperabilidade em *Blockchains*: Um Comparativo de Custo de Transações Cross-chain para Tokens ERC-20

Rafael Fialho Pinto Coelho

JUIZ DE FORA
03, 2025

Mecanismos de Interoperabilidade em *Blockchains*: Um Comparativo de Custo de Transações Cross-chain para Tokens ERC-20

Rafael Fialho Pinto Coelho

Universidade Federal de Juiz de Fora

Instituto de Ciências Exatas

Departamento de Ciência da Computação

Bacharelado em Ciência da Computação

Orientador: Alex Borges Vieira

Coorientador: Ronan Dutra Mendonça

JUIZ DE FORA

03, 2025

Mecanismos de Interoperabilidade em *Blockchains*: Um Comparativo de Custo de Transações Cross-chain para Tokens ERC-20

Rafael Fialho Pinto Coelho

MONOGRAFIA SUBMETIDA AO CORPO DOCENTE DO INSTITUTO DE CIÊNCIAS EXATAS DA UNIVERSIDADE FEDERAL DE JUIZ DE FORA, COMO PARTE INTEGRANTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE BACHAREL EM CIÊNCIA DA COMPUTAÇÃO.

Aprovada por:

Alex Borges Vieira
Pós-Doutorando

Ronan Dutra Mendonça
Doutorando

Glauber Dias Gonçalves
Doutor

JUIZ DE FORA

13 DE 03, 2025

Aos meus amigos, namorada e pet.

Aos pais, pelo apoio e sustento.

Resumo

A interoperabilidade de dados refere-se à capacidade de diferentes sistemas, redes ou plataformas se comunicarem e funcionarem de maneira eficiente, compartilhando informações e recursos sem restrições. No contexto das blockchains, a interoperabilidade representa um desafio significativo, especialmente para aplicações que dependem dessa característica. A diversidade de plataformas e as distintas implementações de protocolos aumentam a complexidade desse processo. Este trabalho explora a importância da interoperabilidade no ecossistema blockchain e detalha os mecanismos utilizados para viabilizar a comunicação entre diferentes redes. Foram estruturados, implementados e testados dois mecanismos de interoperabilidade, o Mecanismo Notarial e o Bloqueio por Hash, com o objetivo de avaliar os custos e tempo envolvidos na interoperabilidade de tokens ERC-20. Os resultados obtidos revelam que, embora o Mecanismo Notarial apresente maior complexidade, ele possui um custo muito menor do valor total do Bloqueio por Hash.

Palavras-chave: Blockchain, Interoperabilidade, ERC-20.

Abstract

Data interoperability refers to the ability of different systems, networks, or platforms to communicate and operate efficiently by sharing information and resources without restrictions. In the context of blockchains, interoperability represents a significant challenge, especially for applications that rely on this feature. The diversity of platforms and distinct protocol implementations increase the complexity of this process. This work explores the importance of interoperability in the blockchain ecosystem and details the mechanisms used to enable communication between different networks. Two interoperability mechanisms, the Notary Mechanism and Hash Lock, were structured, implemented, and tested to evaluate the costs and time involved in ERC-20 token interoperability. The results reveal that while the Notary Mechanism exhibits higher complexity, it incurs a significantly lower cost compared to the total value of Hash Lock.

Keywords: Blockchain, Interoperability, ERC-20.

Agradecimentos

A todos os meus parentes, pelo encorajamento e apoio durante minha trajetória dentro da UFJF, cada carinho, apoio financeiro ou emocional me ajudou a chegar aqui. Aos meus amigos que me ajudaram nas disciplinas e fora delas, cada ato de carinho será guardado para sempre junto comigo.

Ao professor Alex pela orientação, amizade e principalmente, pela paciência, sem a qual este trabalho não se realizaria. Me mostrou principalmente a beleza de ser um bom profissional e um amigo para aqueles que precisam, com leveza e comprometimento.

Aos professores do Departamento de Ciência da Computação pelos seus ensinamentos e aos funcionários do curso, que durante esses anos, contribuíram de algum modo para o nosso enriquecimento pessoal e profissional.

Conteúdo

Lista de Figuras

Lista de Tabelas

Lista de Abreviações

DCC	Departamento de Ciência da Computução
UFJF	Universidade Federal de Juiz de Fora
BTC	Bitcoin
HTLC	Hash Time Lock Contract
EVM	Ethereum Virtual Machine
ERC20	Ethereum Request for Comment 20

1 Introdução

1.1 Apresentação do tema

Em um mundo onde a tecnologia, em alguns aspectos, avança para a centralização em nuvem, existe outra vertente que busca a descentralização e menos dependência de terceiros. A *blockchain* vem se tornando uma tecnologia promissora para registros de informações de forma distribuída. O trabalho de (NAKAMOTO; BITCOIN, 2008) mostra como essa tecnologia pode ser aplicada para criar um sistema de registro de transações descentralizado, como é o caso da moeda digital da rede *Bitcoin*.

O início da moeda digital *Bitcoin* trouxe discussões para os desenvolvedores e investidores que queriam expandir a funcionalidade da *blockchain*. Dessa forma, (BUTERIN, 2016) criou os contratos inteligentes, que permitiram aprimorar a implantação de códigos dentro da rede da *Ethereum*, permitindo executar transações muito mais complexas, buscando atender outras necessidades e aplicações diversas (MENDONçA et al., 2024). Apesar da evolução que as *blockchains* alcançaram, abrangendo diversas áreas do desenvolvimento tecnológico, cada uma delas cresceu de forma heterogênea, impulsionada por diferentes tecnologias. Isso resultou em uma difícil comunicação entre as redes e um desafio para a interoperabilidade de dados e informações.

1.2 Contextualização

Com o grande potencial e crescimento da *blockchain*, empresas e desenvolvedores começaram a criar diferentes tecnologias para resolver diversos problemas e construir aplicações para as redes descentralizadas. No entanto, mesmo solucionando a demanda de problemas dentro daquela rede, surgia a necessidade de permitir que os usuários interagissem entre os diversos sistemas *blockchain* criados. Mesmo após a implementação de contratos inteligentes, outros desafios mais complexos começaram a aparecer. A criação de novos tipos de redes tornou-se inevitável, porém, poucas *blockchains* se preocuparam em interagir

diretamente com outra. A falta de interoperabilidade para transações e dados ficou em falta, mostrando assim uma falta de preparo para o futuro.

Dentro das redes públicas de *blockchain*, especialmente em Máquinas Virtuais da Ethereum (EVM), existe um padrão para criptomoedas chamado token ERC20 ou $EthereumRequestforComment20$. Esse token é usado para as moedas nativas da rede, que são utilizadas para pagar transações de contratos inteligentes. Contudo, existem moedas que não são nativas de uma determinada *blockchain* e estão presentes em várias outras redes, como, por exemplo, as stablecoins $USDT$ ou $USDC$, que, embora diferentes, possuem o mesmo valor de 1 dólar, independentemente da rede. Entretanto, não existe uma maneira direta para o usuário interoperar essas moedas entre diferentes redes devido à falta de consenso entre as tecnologias, sendo necessário utilizar corretoras para garantir essa interoperabilidade.

1.3 Descrição do Problema

Apesar de existirem soluções como corretoras, que centralizam e intermedeiam transações entre *blockchains* diferentes, essa solução nem sempre é um caminho barato ou confiável. Há contratos maliciosos e com falhas, assim como uma corretora pode sofrer uma quebra de segurança. Taxas altas também podem ser um problema, pois, para trocas entre redes diferentes, não apenas haverá a taxa da rede para uma transação, mas também a taxa de câmbio entre as redes. Além disso, existem diversas formas de interoperabilidade, e cada uma depende da tecnologia aplicada na rede e do protocolo utilizado.

Dessa forma, é de extrema importância que o usuário saiba qual protocolo de interoperabilidade utilizar, para evitar taxas desnecessárias e falhas catastróficas. Alguns mecanismos são usados apenas em redes homogêneas, onde as tecnologias são parecidas ou idênticas, facilitando as transações. Por outro lado, existem redes heterogêneas, nas quais até mesmo a linguagem de programação se difere significativamente. Por exemplo, redes EVM apresentam compatibilidade com o Solidity, sendo consideradas redes homogêneas, enquanto redes que utilizam tecnologia baseada em RUST, como a *Solana*, não aceitam contratos ERC20.

Cada mecanismo de interoperabilidade possui um custo que varia de acordo com o

tamanho e a complexidade dos dados envolvidos na transação. Alguns são mais custosos, porém mais seguros. Tudo isso deve ser analisado antes de tomar uma decisão.

1.4 Justificativa e motivação

Transações de Tokens ERC20 ou criptomoedas ocorrem constantemente nas *blockchains*, com altos valores e grandes volumes de dinheiro sendo movimentados pelas redes. Diante disso, conhecer as taxas de transações em ativos é fundamental para o cálculo de um investidor ou até mesmo para um trabalhador que recebe em cripto. Nas *blockchains* que utilizam a Máquina Virtual da Ethereum (EVM), as taxas funcionam através de um cálculo de "feeGas", que é convertido para a moeda padrão da rede. Embora o cálculo seja o mesmo para todas as redes EVM, o valor pode variar, pois depende da demanda da rede e da complexidade das transações. Redes sobrecarregadas, com grande volume de transações concorrentes, tendem a ter taxas mais altas, já que os mineradores ou validadores priorizam transações com maiores incentivos.

Este trabalho tem como objetivo calcular os custos envolvidos de diferentes mecanismos de interoperabilidade para fazer um comparativo de custo, gerando dados valiosos para usuários que buscam realizar transações entre *blockchains*. Como essa questão é frequentemente negligenciada pelas redes, as transações cross-chain (como são chamadas transações entre *blockchains* de mesma tecnologia) são difíceis de prever, visto que é necessário calcular tanto a taxa de uma rede quanto da outra, e essas redes podem ter volumes de transações diferentes e complexidades desiguais.

1.5 Objetivos

O objetivo deste trabalho é realizar testes com mecanismos de interoperabilidade existentes para criar um comparativo de custo entre diferentes soluções. Com a ampla gama de transações proporcionadas pelas inúmeras possibilidades dos contratos inteligentes, o foco será nas transações de tokens ERC20, analisando métodos e taxas comumente adotados.

Para isso, será necessário definir um escopo claro de testes, que inclua a análise das variáveis que impactam o custo das transações, como o tipo de contrato inteligente

utilizado, a demanda da rede e a complexidade das operações.

O objetivo final é fornecer um panorama comparativo que auxilie na compreensão das melhores práticas e soluções mais eficientes para a interoperabilidade entre blockchains no contexto de tokens ERC20. Será realizada uma revisão bibliográfica dos mecanismos, adaptando-os de forma consistente e padronizada para o ambiente de testes. Aspectos como velocidade, custo e segurança das transações entre diferentes redes serão verificados, com foco na viabilidade prática de cada solução. Além disso, será analisada a compatibilidade dos mecanismos com as principais plataformas que utilizam tokens ERC20, visando identificar oportunidades de otimização e redução de custos para os usuários e desenvolvedores que utilizam essas soluções.

1.6 Metodologia

Para atingir os objetivos propostos, o trabalho será dividido em etapas claras, iniciando com uma revisão bibliográfica aprofundada. Esta revisão terá como foco a identificação de diferentes mecanismos de interoperabilidade entre blockchains, com ênfase nos métodos aplicáveis a tokens ERC20. Isso permitirá uma compreensão detalhada das soluções disponíveis e a seleção dos mecanismos mais adequados para os testes comparativos.

Paralelamente à revisão bibliográfica, será estabelecido um ambiente de testes controlado. Esse ambiente será configurado utilizando plataformas compatíveis com a Máquina Virtual da Ethereum (EVM), onde serão realizadas as transações de tokens ERC20. Será necessário configurar as redes envolvidas, garantindo que os mecanismos de interoperabilidade selecionados possam ser testados de forma padronizada e repetível.

Os testes incluirão a simulação de transações entre redes, utilizando mecanismos de interoperabilidade como Notário e Hash Time Lock Contracts (HTLC). Cada teste será avaliado com base em dois critérios principais: custo da transação e tempo de execução. Para a coleta desses dados, será utilizado um conjunto de ferramentas de monitoramento e medição de performance adequadas ao ambiente EVM.

Após a realização dos testes, os resultados obtidos serão analisados quantitativamente, comparando o desempenho de cada mecanismo em diferentes cenários. Com base nesses resultados, será possível avaliar a viabilidade prática das soluções e identificar

quais mecanismos são mais eficientes, tanto em termos de custo quanto de desempenho.

2 Fundamentação Teórica

Neste capítulo, serão abordados os conceitos fundamentais para a compreensão e desenvolvimento deste trabalho. O objetivo é fornecer uma base teórica sólida que sustente as discussões e implementações realizadas ao longo do projeto. A Seção 2.1 introduz os conceitos essenciais de Blockchain, explorando seu funcionamento, características e importância. A Seção 2.2 discute os Tokens ERC-20, um padrão amplamente utilizado para a criação de tokens no ecossistema Ethereum. Na Seção 2.3, é apresentada a Interoperabilidade entre blockchains, abordando os desafios e as soluções para a comunicação entre redes diferentes. A Seção 2.4 detalha o conceito de Hash Time Lock Contract (HTLC), um mecanismo de segurança que permite transações condicionais entre partes. Por fim, a Seção 2.5 discute o Mecanismo Notarial, explorando sua aplicação prática em sistemas blockchain e sua relevância para interoperabilidade.

2.1 Blockchain

O conceito de Blockchain tem suas raízes na necessidade de sistemas descentralizados e seguros para o armazenamento de dados. Apresentado inicialmente por Satoshi Nakamoto em 2008 como a base para o Bitcoin (NAKAMOTO; BITCOIN, 2008), a Blockchain se destaca por sua capacidade de armazenar registros de transações de forma distribuída, mantendo a segurança e integridade dos dados sem a necessidade de intermediários.

A Blockchain é composta por blocos, que são estruturas de dados que contêm informações sobre um conjunto de transações. Cada transação representa uma operação registrada na rede, como a transferência de ativos digitais entre participantes. Além disso, os blocos incluem um identificador único chamado hash, que é gerado a partir das informações contidas no bloco e do hash do bloco anterior. Isso cria um encadeamento criptográfico entre os blocos, formando uma cadeia linear onde cada bloco está conectado ao anterior. Essa estrutura garante a segurança dos dados, pois qualquer tentativa de alteração em um bloco exigiria a modificação de todos os blocos subsequentes, algo inviável

em uma rede descentralizada.

A tecnologia é amplamente adotada em diversas áreas, desde transações financeiras até gerenciamento de identidades. Sua principal característica é a imutabilidade dos dados, uma vez que qualquer alteração requer o consenso de todos os participantes da rede. Além disso, a descentralização garante que o sistema não seja controlado por uma única entidade, aumentando a transparência e a resistência a fraudes.

2.2 Tokens ERC20

Os Tokens ERC20 são um padrão de contrato inteligente utilizado na blockchain Ethereum para a criação de tokens fungíveis. Introduzido em 2015, o padrão ERC20 define um conjunto de regras que os tokens devem seguir, o que facilita sua interoperabilidade com outros contratos e plataformas descentralizadas (BUTERIN, 2016). Entre as funções básicas desse padrão estão a transferência de tokens entre endereços, a verificação do saldo de uma conta e a aprovação para que outro endereço gaste tokens em nome do proprietário.

A popularidade dos tokens ERC20 deve-se, em grande parte, à facilidade de criação de novos ativos digitais sem a necessidade de desenvolver uma blockchain separada. Isso abriu portas para uma ampla gama de aplicações, como o uso de tokens em plataformas de finanças descentralizadas (DeFi) permitindo a criação de pools de liquidez, empréstimos, staking e até governança descentralizada. Além disso, esses tokens têm sido amplamente adotados em projetos de crowdfunding por meio de ofertas iniciais de moedas (ICOs), tornando-se uma ferramenta essencial para startups que desejam levantar capital e criar incentivos em seus ecossistemas digitais.

2.3 Interoperabilidade

Interoperabilidade é a capacidade de diferentes sistemas, redes ou plataformas se comunicarem e trocarem informações entre si de maneira eficaz. No contexto da blockchain, a interoperabilidade refere-se à capacidade de diferentes redes blockchain trabalharem juntas, permitindo a troca de informações e ativos sem a necessidade de intermediários

centralizados. Essa característica é fundamental para o crescimento e adoção em larga escala da tecnologia, pois permite a conexão de ecossistemas distintos, cada um com suas próprias funcionalidades e vantagens.

As redes blockchain geralmente operam de forma isolada, o que cria sistemas heterogêneos, dificultando a troca de informações, principalmente em aplicações DeFi e seus tokens, que não podem funcionar em redes distintas das que foram criadas. Isso evidenciou a necessidade de interoperabilidade entre essas redes. Recentemente, diversas organizações começaram a desenvolver soluções para aumentar a capacidade de cooperação entre as redes, mesmo com diferentes tecnologias (WEGNER, 1996).

Os tipos de interoperabilidade mais comuns incluem: entre redes blockchain homogêneas, entre dApps de diferentes redes e entre redes heterogêneas. Cada tipo apresenta diferentes formas de transação, como as transações cross-chain (CC-Tx) e cross-blockchain (CB-Tx), que permitem transferências seguras de ativos entre redes (BELCHIOR et al., 2021).

Essas transações são facilitadas por "pontes", que nesse trabalho serão os mecanismos que conectam as redes blockchain, garantindo a validação e a segurança das transações em ambas as cadeias. No contexto dos tokens, a interoperabilidade é essencial, pois viabiliza a transferência de ativos entre redes distintas, mantendo o histórico e consistência das transações.

2.4 Bloqueio de Hash

O Hash Time Lock Contract (HTLC) é uma técnica utilizada em blockchains para garantir a execução de transações entre partes que não confiam totalmente umas nas outras. O conceito foi introduzido para possibilitar a realização de transações cross-chain, em que ativos de diferentes blockchains são trocados de forma segura sem a necessidade de uma entidade centralizadora.

O HTLC funciona com base em dois mecanismos principais: hashlocks e timelocks. O hashlock garante que a transação só será confirmada se a contraparte fornecer uma prova criptográfica. Já o timelock determina um limite de tempo para que essa prova seja fornecida, ou a transação é revertida, protegendo ambas as partes contra possíveis

perdas. São feitos 2 contratos inteligentes para ambas as redes, o destinatário, a quantia e o hashlock é feito direto no código do contrato, assim dando segurança que a troca não será modificada.A Figura 2.1 mostra dois usuários usando dois contratos HTLC para fazer uma troca entre si,no exemplo cada um implementa o contrato em uma *blockchain* e o outro retira os fundos depositados naquele contrato por meio de funções.

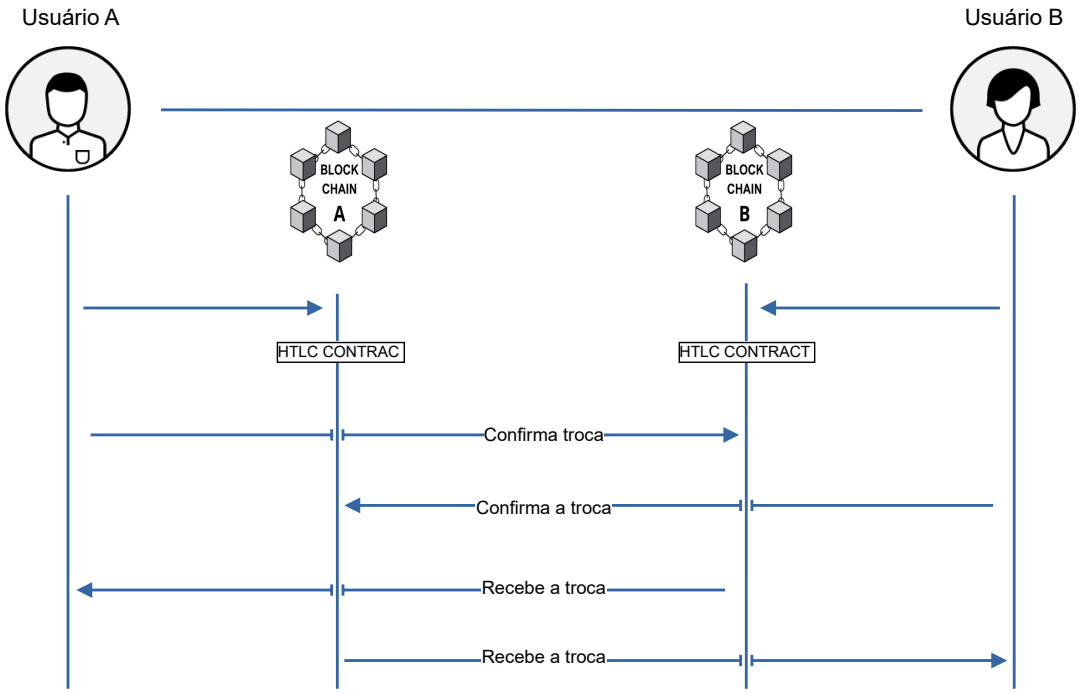

Figura 2.1: Mecanismo Bloqueio de Hash

2.5 Mecanismo Notorial

O mecanismo notarial é uma abordagem relativamente simples para implementar a interoperabilidade entre blockchains. Ele funciona através de uma entidade confiável chamada notário, que verifica e encaminha mensagens entre as cadeias. Quando há a necessidade de transferir ativos ou informações entre diferentes blockchains, um ou mais notários são designados para monitorar os eventos e alcançar um consenso por meio de um algoritmo específico. Esses notários garantem a ocorrência e a validação do evento de forma tempestiva, assegurando a integridade das transações (BELCHIOR et al., 2021).

Existem dois tipos principais de mecanismos notariais: o de assinatura única e o de múltiplas assinaturas (OU et al., 2022). No mecanismo de assinatura única, também

chamado de mecanismo notarial centralizado, apenas um nó ou instituição independente atua como notário, sendo responsável pela coleta de dados e verificação das transações entre as blockchains. Embora seja rápido e adaptável, esse modelo tem um escopo mais restrito, limitando-se a transações simples de troca de ativos.

Por outro lado, o mecanismo de múltiplas assinaturas envolve vários nós atuando como notários. Nesse sistema, cada nó possui uma chave e as transações só são confirmadas quando uma porcentagem mínima dos nós assina em conjunto. Isso reduz a dependência de um único notário e garante maior segurança e confiança no processo, já que a seleção dos notários ocorre de forma aleatória. Na Figura 2.2 mostra a troca entre dois usuários que utilizam o Notário para ser o intermediador, apesar da imagem de um homem, o intermediário pode ser um outro contrato ou tecnologia semelhante.

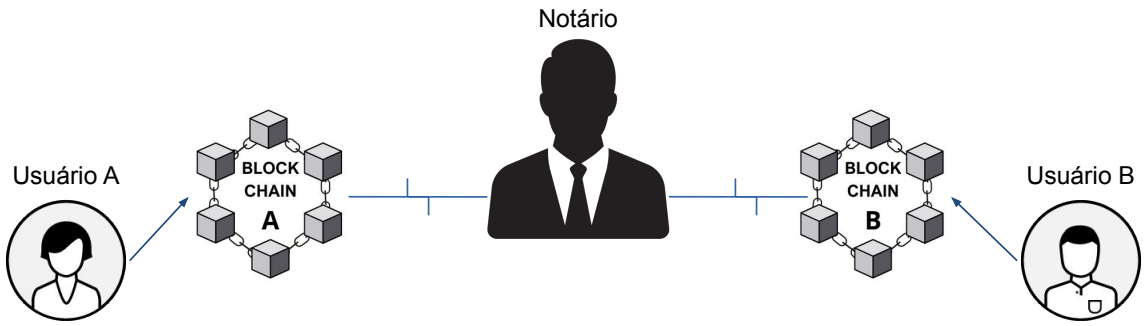

Figura 2.2: Mecanismo Notorial

3 Revisão da Literatura

Este capítulo apresenta uma revisão detalhada da literatura existente sobre interoperabilidade entre blockchains, com foco em como diferentes abordagens e tecnologias podem ser aplicadas para melhorar a integração e a comunicação entre sistemas descentralizados.

Cada trabalho revisado aborda diferentes aspectos da interoperabilidade, utilizando diversas tecnologias e metodologias. A análise inclui desde modelos baseados em contratos inteligentes e protocolos de segurança, até soluções específicas para a troca de ativos digitais e a gestão de dados entre plataformas. Esta revisão fornece uma base sólida para compreender as práticas atuais e identificar lacunas nas soluções existentes, o que é essencial para o desenvolvimento de novas abordagens e para a escolha dos mecanismos mais adequados para a comparação de custos e eficácia em transações cross-chain.

3.1 Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability

No estudo de (GORDON; CATALINI, 2018), é apresentado um modelo inovador que utiliza a tecnologia blockchain para facilitar a interoperabilidade centrada no paciente na área da saúde. O modelo aborda a crescente demanda por um sistema de troca de dados que não dependa exclusivamente de instituições, permitindo que os pacientes sejam os principais responsáveis pela gestão de suas informações de saúde. O primeiro aspecto do modelo envolve a definição de regras de acesso digital, que garantem que os pacientes tenham controle total sobre quem pode acessar seus dados. Em seguida, o modelo promove a agregação de dados, permitindo que os pacientes reúnam informações de diferentes fontes em uma única plataforma. Além disso, a liquidez dos dados é aprimorada, facilitando o compartilhamento rápido e seguro das informações. Outro ponto importante é a identificação do paciente, utilizando uma infraestrutura de chave pública que permite

a resolução de identidade de maneira eficiente. Por fim, a imutabilidade dos dados é garantida, proporcionando um registro seguro e auditável das transações. A combinação desses elementos visa não apenas aumentar a precisão na troca de dados, mas também empoderar os pacientes, transformando-os em participantes ativos na gestão de sua saúde.

Os autores concluíram que, apesar da empolgação em torno da interoperabilidade centrada no paciente, ainda existem desafios substanciais a serem superados. Os principais obstáculos incluem o volume de transações de dados clínicos, preocupações com privacidade e segurança, engajamento do paciente e incentivos. A tecnologia blockchain é vista como uma possível solução para alguns desses desafios, proporcionando uma maneira segura e eficiente de gerenciar e compartilhar dados de saúde

3.2 Towards A Novel Architecture for Enabling Interoperability Amongst Multiple Blockchains

Em (JIN; DAI; XIAO, 2018), foi proposta uma arquitetura inovadora para habilitar a interoperabilidade entre múltiplos sistemas de blockchain. O projeto busca resolver os desafios de comunicação e transferência de dados eficazes entre diferentes blockchains, reconhecendo que a diversidade desses sistemas exige uma colaboração cruzada para oferecer serviços mais ricos e valiosos. A arquitetura proposta é estruturada em cinco camadas, cada uma abordando desafios específicos, como a unificação do formato de transações, a comunicação entre blockchains, a verificação de dados, a execução de contratos inteligentes inter-chain e a criação de APIs amigáveis para desenvolvedores.

Os resultados encontrados indicam que a arquitetura proposta melhora a eficiência e a segurança na interação entre blockchains, além de oferecer um método chamado MMR (Monitor Multiplexing Reading) que reduz significativamente a sobrecarga de leitura passiva, mantendo a temporalidade da comunicação.A capacidade de integrar diversos sistemas de blockchain com segurança, a redução da complexidade na interação entre diferentes blockchains e a criação de uma interface amigável para desenvolvedores, o que pode estimular a adoção e o desenvolvimento de aplicações interconectadas. Além disso, a proposta de unificação do formato de transação e a introdução de um protocolo de verificação aju-

dam a garantir a atomicidade e a confiabilidade das operações.Porem, a dificuldade de integrar em sistemas já existentes e a complexidade de integração podem exigir adaptações significativas para integrar a nova arquitetura. Além disso, a dependência de um monitor centralizado para a comunicação entre blockchains pode levantar preocupações sobre a segurança e a privacidade dos dados, embora o projeto afirme que isso não compromete a segurança do sistema.

3.3 Towards blockchain interoperability: Improving video games data exchange

O trabalho de (BESANÇON; SILVA; GHODOUS, 2019), propõe uma arquitetura voltada para melhorar a interoperabilidade entre tecnologias descentralizadas e blockchains, com foco na indústria de videogames. A arquitetura visa integrar blockchains com tecnologias de armazenamento distribuído, como o IPFS, permitindo o uso de ativos de jogos em ambientes descentralizados. Além disso, é proposta uma nova representação de dados para esses ativos, focando na escalabilidade e na facilidade de intercâmbio de informações entre plataformas.

A arquitetura proposta mostrou-se eficaz para solucionar problemas de escalabilidade e interoperabilidade com a implementação de ativos de jogos digitais. Utilizando a representação de dados proposta, demonstrou melhorar a transferência de informações entre diferentes camadas da aplicação descentralizada. Além disso, a integração com tecnologias de armazenamento distribuído permitiu que grandes volumes de dados fossem armazenados fora da blockchain, diminuindo o custo e o tempo de processamento das transações. No entanto, a implementação ainda enfrenta desafios devido à complexidade tecnológica, especialmente para desenvolvedores menos familiarizados com blockchain. Além disso, a descentralização completa dificulta a moderação de conteúdos ilegais ou indesejados, criando um desafio adicional para a gestão da plataforma.

3.4 Interoperability in Internet of Things: Taxonomies and Open Challenges

O trabalho de (NOURA; ATIQUZZAMAN; GAEDKE, 2019) propõe uma taxonomia detalhada e aborda os desafios abertos relacionados à interoperabilidade no Internet of Things (IoT). A pesquisa foca em como diferentes dispositivos, redes, plataformas e dados podem ser integrados em um ambiente heterogêneo de IoT. O estudo revisa as abordagens existentes para facilitar a interoperabilidade e apresenta uma visão abrangente de soluções desenvolvidas nos últimos anos. O estudo identificou que a falta de interoperabilidade entre diferentes sistemas IoT impede o pleno desenvolvimento dessa tecnologia em larga escala. A pesquisa destacou a necessidade de criar padrões universais que permitam a comunicação eficiente entre plataformas, dispositivos e redes heterogêneas. Além disso, mostrou que, embora existam várias soluções, a maioria delas não aborda todas as camadas de interoperabilidade, como a semântica e a interoperabilidade entre plataformas. O estudo concluiu que a ausência de padrões amplamente aceitos e de soluções de interoperabilidade completas ainda representa um grande desafio.

Os pontos positivos incluem a identificação de soluções inovadoras para interoperabilidade, como o uso de APIs abertas e a integração de tecnologias semânticas, que facilitam a comunicação entre dispositivos heterogêneos. O trabalho também destaca os esforços da indústria e da academia para padronizar as interações entre plataformas de IoT. No entanto, os pontos negativos são a falta de um padrão universal que abranja todas as camadas de interoperabilidade, bem como a dificuldade de integrar soluções de diferentes fornecedores de IoT. Além disso, a complexidade técnica e os custos associados à implementação de soluções interoperáveis ainda são obstáculos significativos.

3.5 HyperService: Interoperability and Programmability Across Heterogeneous Blockchains

O trabalho de (LIU et al., 2019) propõe o HyperService, uma plataforma inovadora que oferece interoperabilidade e programabilidade entre diferentes blockchains heterogêneas.

O objetivo principal é permitir que desenvolvedores criem aplicações descentralizadas (dApps) que possam operar em várias blockchains de maneira eficiente e segura. O HyperService combina um framework de programação unificado, que abstrai a complexidade das interações entre blockchains, com um protocolo criptográfico (UIP) que garante a execução segura dessas operações em múltiplas blockchains.A implementação do HyperService foi bem-sucedida, demonstrando que a plataforma pode incorporar grandes blockchains e executar dApps com latência razoável, na ordem de segundos. Os testes realizados com um protótipo de aproximadamente 35.000 linhas de código mostraram que o sistema suporta dApps que realizam operações complexas entre diferentes blockchains, indo além de simples trocas de tokens.

Entre os pontos positivos, destaca-se a capacidade de programabilidade cruzada entre diferentes blockchains, facilitada pelo modelo de estado unificado (USM) e pela linguagem de programação HSL, que permite aos desenvolvedores escrever dApps sem a necessidade de lidar com a heterogeneidade das blockchains subjacentes. Além disso, o sistema oferece garantias de segurança robustas e escalabilidade contínua. No entanto, como ponto negativo, a complexidade técnica da implementação pode apresentar desafios, especialmente para desenvolvedores menos familiarizados com criptografia avançada e sistemas de execução distribuída. Além disso, a latência, embora aceitável, pode ser um fator limitante para certas aplicações em tempo real.

3.6 Atomic Cross-Chain Swaps

O trabalho de (HERLIHY, 2018) propõe um protocolo para Atomic Cross-Chain Swaps, que permite a troca de ativos entre múltiplas blockchains de forma descentralizada, sem a necessidade de confiança entre as partes envolvidas. O protocolo utiliza contratos inteligentes com hashlocks e timelocks para garantir que todos os ativos sejam trocados de forma simultânea ou nenhuma troca ocorra, evitando que qualquer parte saia prejudicada. A proposta é baseada em um modelo gráfico direcionado onde os nós representam as partes envolvidas e as arestas representam as trocas de ativos. O protocolo desenvolvido foi capaz de garantir que todos os swaps ocorram de forma simultânea e atômica, desde que todas as partes sigam o protocolo. O estudo também demonstrou que a arquitetura pode

ser aplicada a várias blockchains simultaneamente e em diferentes tipos de ativos digitais. O tempo de execução do protocolo está limitado ao diâmetro do gráfico de troca, e o espaço de armazenamento exigido pelas blockchains depende da quantidade de arestas de transferência de ativos.

Os pontos positivos incluem a garantia de segurança para todas as partes envolvidas em trocas inter-blockchain, com um sistema que evita prejuízos caso alguma parte falhe ou tente agir de maneira maliciosa. O uso de hashed timelock contracts (HTLC) elimina a necessidade de intermediários de confiança e facilita a coordenação de trocas de ativos complexas entre blockchains. No entanto, entre os pontos negativos, está a complexidade do protocolo, que exige que os participantes implementem corretamente os contratos inteligentes e lidem com aspectos de temporização e sincronização entre blockchains, o que pode aumentar a latência em cenários de redes complexas.

3.7 Exploring interoperability of Blockchain technology and the possibility

O projeto apresentado por (DIMITROV; GIGOV, 2020) investiga como a tecnologia blockchain pode ser integrada com sistemas de informação já estabelecidos nas empresas. O objetivo principal é analisar as implicações da interoperabilidade entre diferentes sistemas de informação e como a blockchain pode melhorar a eficiência e a segurança nas transações e na gestão de dados. O estudo propõe um modelo que combina as características da blockchain com as necessidades específicas das empresas, visando facilitar a comunicação e a troca de informações entre diferentes plataformas.Os resultados indicam que a implementação da tecnologia blockchain pode levar a uma melhoria significativa na transparência e na rastreabilidade das transações. O estudo demonstrou que, ao integrar a blockchain com sistemas de informação existentes, as empresas podem reduzir custos operacionais e aumentar a confiabilidade dos dados. Além disso, foram identificados casos de uso em setores como logística, finanças e saúde, onde a interoperabilidade pode trazer benefícios substanciais. A pesquisa também revelou que a adoção da blockchain pode ser gradual, permitindo que as empresas adaptem suas operações sem a necessidade de uma

reestruturação completa.

Entre os pontos positivos, destaca-se a capacidade da blockchain de proporcionar um registro imutável e seguro das transações, o que aumenta a confiança entre as partes envolvidas. A interoperabilidade proposta permite que diferentes sistemas de informação se comuniquem de forma mais eficaz, resultando em processos mais ágeis e menos propensos a erros. No entanto, os pontos negativos incluem a complexidade da integração da blockchain com sistemas legados, que pode exigir investimentos significativos em tecnologia e treinamento. Além disso, a resistência à mudança por parte das organizações e a necessidade de conformidade regulatória podem ser barreiras à adoção generalizada da tecnologia. A latência nas transações, embora geralmente aceitável, pode ser um fator limitante em aplicações que exigem respostas em tempo real.

3.8 appXchain: Application-Level Interoperability for Blockchain Networks

O trabalho de (MADINE et al., 2021) propõe o appXchain, uma solução inovadora para a interoperabilidade entre diferentes redes blockchain. O objetivo principal é permitir que sistemas blockchain heterogêneos interajam e compartilhem dados de forma eficiente e sem a necessidade de intervenção do usuário. O appXchain se baseia na adaptabilidade e atualizabilidade das Aplicações Descentralizadas (DApps) para desenvolver uma solução prática e padronizada para a comunicação entre blockchains, visando atender a uma ampla gama de aplicações e casos de uso.A implementação do appXchain demonstrou que a arquitetura proposta pode facilitar a troca de dados e interações entre diferentes sistemas blockchain, sem causar interrupções significativas nas redes existentes. Os testes realizados indicaram que a solução é capaz de suportar a interoperabilidade de forma contínua e escalável, permitindo a integração de novos sistemas de maneira fluida. O foco em aplicações no setor de saúde, como a gestão de registros médicos, mostrou resultados promissores em termos de eficiência e segurança.

Entre os pontos positivos, destaca-se a capacidade do appXchain de permitir a interoperabilidade sem exigir modificações frequentes em contratos inteligentes ou a neces-

sidade de infraestrutura off-chain confiável. A solução também minimiza a dependência de intervenções manuais, o que a torna mais acessível para usuários finais. No entanto, como ponto negativo, a complexidade da implementação e a necessidade de padronização entre diferentes tecnologias blockchain podem representar desafios significativos. Além disso, a performance e a segurança das redes blockchain podem ser impactadas dependendo da forma como a interoperabilidade é implementada, exigindo um equilíbrio cuidadoso entre funcionalidade e segurança.

3.9 Considerações finais

A revisão da literatura revela a diversidade de abordagens para a interoperabilidade entre blockchains, cada uma com suas vantagens e desafios. A tabela 3.1 mostra os principais aspectos dos trabalhos analisados, destacando a aplicação de diferentes tecnologias e o impacto na segurança, confiabilidade, desempenho e aplicabilidade prática.

Tabela 3.1: Tabela comparativa entre trabalhos relacionados

Nome do Trabalho	**Cross-chain (Redes Heterogêneas)**	**Segurança e Confiabilidade**	**Desempenho (Latência e Escalabilidade)**	**Tecnologia Utilizada**	**Aplicações Práticas**
(GORDON; CATALINI, 2018)		X		Contratos Inteligentes	Saúde
(JIN; DAI; XIAO, 2018)	X	X	X	Contratos Inteligentes e MMR	Geral
(BESANÇON; SILVA; GHODOUS, 2019)			X	IPFS, Contratos Inteligentes	Jogos
(NOURA; ATIQUZZAMAN; GAEDKE, 2019) 4		X	X	APIs Abertas	IoT
(LIU et al., 2019)	X	X	X	HSL, USM	dApps
(HERLIHY, 2018) 6	X	X	X	HTLC	Geral
(DIMITROV; GIGOV, 2020)		X	X	Blockchain Corporativa	Empresas
(MADINE et al., 2021)	X		X	dApps	Saúde
Este trabalho	X	X	X	Mecanismos de Interoperabilidade	Geral

4 Materiais e métodos

4.1 Descrição e coleta de dados

Na coleta de dados e experimentos, foi usada a biblioteca $Truffle$ e $Ethers.js$ para a criação do código em JavaScript para testes. O ambiente de coleta de dados foram redes de testes das próprias *blockchains*. Essas redes permitem a experiência real de criação de contratos inteligentes dentro de *blockchains* sem a necessidade de gastar dinheiro. São ambientes controlados usados principalmente por desenvolvedores.

A existência de redes de teste permite simular resultados reais que aconteceriam ao realizar transações em determinada rede *blockchain* aumentando a eficiência real dos resultados. Porém, para a melhor eficácia dos experimentos, foi utilizado o software *Ganache*, que cria uma rede *blockchain* local com EVM para serem realizados testes. A escolha desse método inicial foi devido à dificuldade existente de recolher criptomoedas das redes de teste que são usadas para as transações. Apesar da gratuidade, os requisitos variam de rede para rede.

Foi utilizada a IDE de desenvolvimento Visual Studio Code para escrever o código, sendo um repositório o mecanismo de Hash Time Lock Contract (HTLC) e outro para o mecanismo Notorial. Os dois scripts são feitos com looping, executando um numero determinado de ciclos de transações. Cada ciclo contem uma interoperabilidade completa dos Tokens colocados em ambas as redes, junto com as chamadas de funções, existe também o recolhimento do custos das transações. Para recolher os dados é usado uma função da biblioteca do $Ethers.js$ onde recolhe o custo de cada transação onde chamamos de *Gas*, onde a unidade é medida em *Gwei*, onde 1 gwei é igual a 0,000000001 *Ethers*

4.2 Resultados

Com os dados de 1, 10 e 100 ciclo de transações consecutivas, obtemos a quantidade de *Gas* necessária para fazer as avaliações de cada mecanismo de interoperabilidade, a

transações foram feitas na rede *ArbitrumSepolia* e na *EthereumSepolia*, ambas muito conhecidas na área de Blockchain. Os resultados dos testes pelo mecanismo HTLC, podem ser encontrados na 4.1

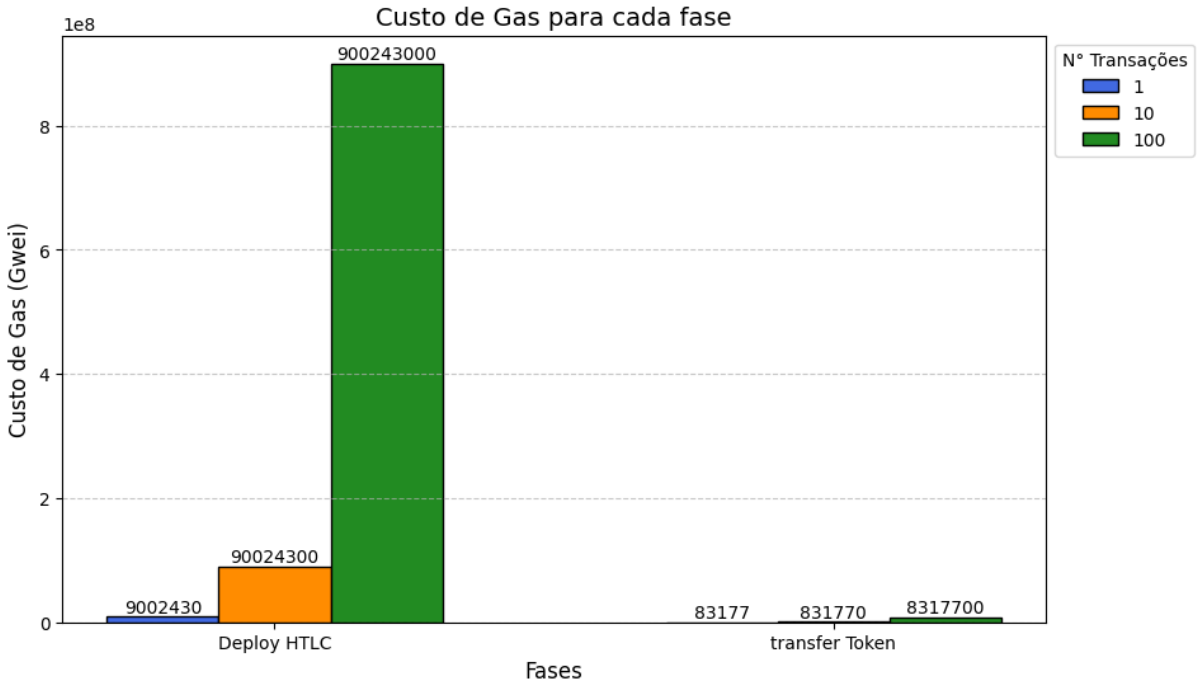

Figura 4.1: Custos do mecanismo HTLC

Como mostra no gráfico, o mecanismo de interoperabilidade Hash Time Lock Contract utiliza duas principais transações para a transferência de Tokens, a transação de $DeployHTLC$ e a $transferToken$. A primeira transação é significantemente mais custosa dentro da *blockchain*, pois se trata de uma transação de implantação de contrato dentro da rede, deixando assim uma exponencial de custos relacionados a sua complexidade exigida. Já a transação de transferência de token demonstra ser bem mais simples pelo fato de ser uma chamada de função.

Já a figura 4.2 demonstra os resultados do mecanismo Notarial, onde apresenta as transações de $deployContract$, $reciveFunds$, $transferContract$ e $sendEther$. Diferentemente do HTLC, o mecanismo Notarial apresenta uma constância na transação de *deploy* onde só é necessário implementar o contrato uma vez dentro da *blockchain* para fazer a interoperabilidade. A função de *receive* vai transferir os tokens da carteira do usuário para o contrato implementado dentro da *blockchain* e a $transafer$ fará a ponte dentre as *redes* para transferência de dados. Quando estiver tudo ok, a *send* irá mandar

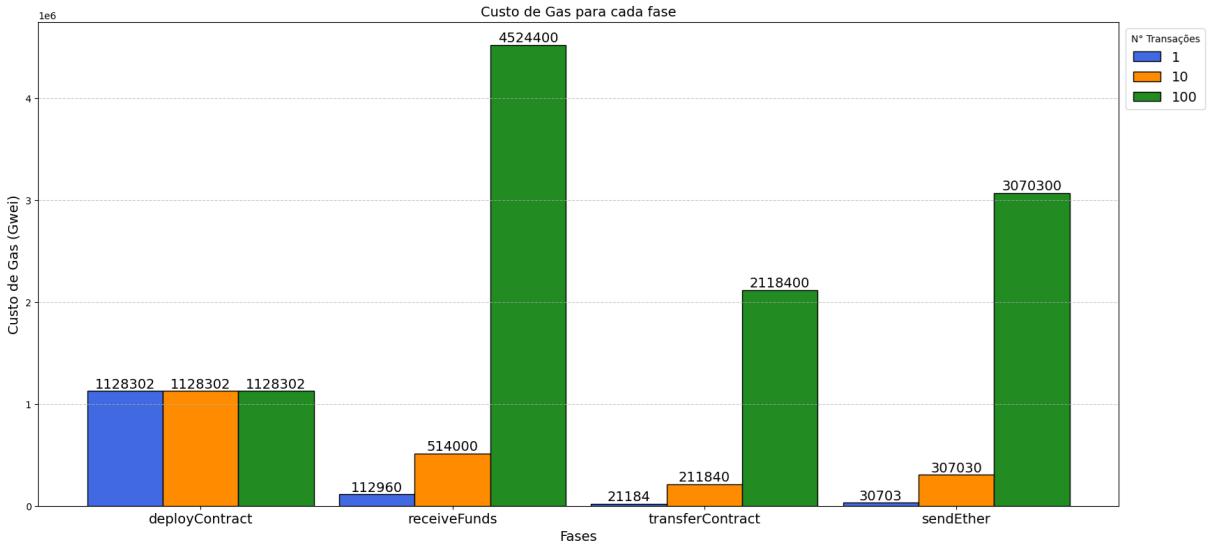

Figura 4.2: Custos do mecanismo Notarial

os tokens para a carteira de destino completando a transferência.

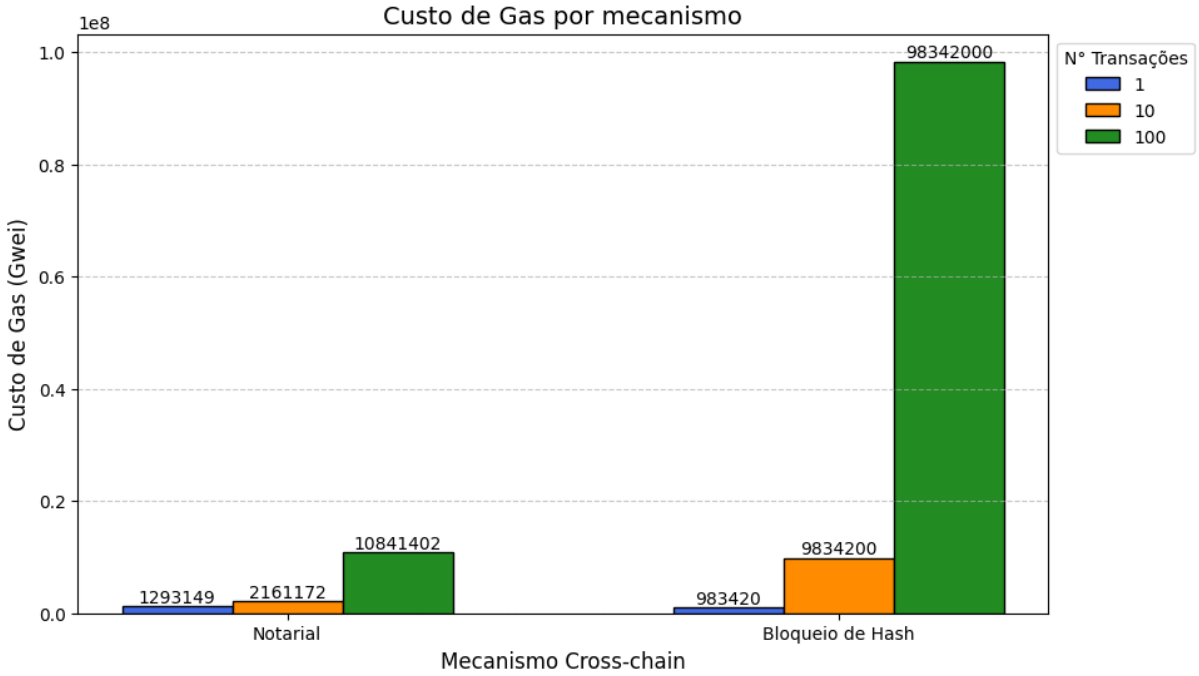

Figura 4.3: Comparação de Custos entre os dois mecanismos

Colocando no mesmo gráfico o custo total de cada mecanismo (4.3), vemos que o Mecanismo Notarial mantém um custo fixo independente do número de transações, o que o torna mais viável em cenários com um grande volume de operações. Em contrapartida, o mecanismo de Bloqueio de Hash apresenta um custo elevado por transação, o que pode torná-lo inviável para transações de baixo valor, já que cada operação incorre no custo total do método.

5 Conclusões

Este trabalho teve como objetivo analisar diferentes mecanismos de interoperabilidade entre blockchains, visando fortalecer a cooperação em aplicações descentralizadas. Para isso, implementamos arquiteturas baseadas na literatura que permitem a experimentação desses mecanismos, com o propósito de avaliar seus custos.

Esses resultados reforçam a importância de escolher o mecanismo de interoperabilidade mais adequado para cada cenário, considerando não apenas a segurança e a eficiência, mas também a viabilidade econômica. Além disso, destacam a necessidade de futuras pesquisas para otimizar esses métodos e explorar novas abordagens, especialmente em ambientes de teste reais e com diferentes padrões de tokens e protocolos cross-chain.

Bibliografia

BELCHIOR, R.; VASCONCELOS, A.; GUERREIRO, S.; CORREIA, M. A survey on blockchain interoperability: Past, present, and future trends. *Acm Computing Surveys (CSUR)*, ACM New York, NY, v. 54, n. 8, p. 1–41, 2021.

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.

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

DIMITROV, I.; GIGOV, R. Exploring interoperability of blockchain technology and the possibility of collaboration with the existing information systems of the enterprises. In: IEEE. *2020 III international conference on high technology for sustainable development (HiTech)*. [S.l.], 2020. p. 1–4.

GORDON, W. J.; CATALINI, C. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. *Computational and structural biotechnology journal*, Elsevier, v. 16, p. 224–230, 2018.

HERLIHY, M. Atomic cross-chain swaps. In: *Proceedings of the 2018 ACM symposium on principles of distributed computing*. [S.l.: s.n.], 2018. p. 245–254.

JIN, H.; DAI, X.; XIAO, J. Towards a novel architecture for enabling interoperability amongst multiple blockchains. In: IEEE. *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*. [S.l.], 2018. p. 1203–1211.

LIU, Z.; XIANG, Y.; SHI, J.; GAO, P.; WANG, H.; XIAO, X.; WEN, B.; HU, Y.-C. Hyperservice: Interoperability and programmability across heterogeneous blockchains. In: *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*. [S.l.: s.n.], 2019. p. 549–566.

MADINE, M.; SALAH, K.; JAYARAMAN, R.; AL-HAMMADI, Y.; ARSHAD, J.; YAQOOB, I. appxchain: Application-level interoperability for blockchain networks. *IEEE Access*, IEEE, v. 9, p. 87777–87791, 2021.

MENDONçA, R.; CARDOSO Ítallo; COELHO, R.; CAMPOS, J.; GONçALVES, G.; VIEIRA, A.; NACIF, J. 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⟩.

NAKAMOTO, S.; BITCOIN, A. A peer-to-peer electronic cash system. *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, v. 4, n. 2, p. 15, 2008.

NOURA, M.; ATIQUZZAMAN, M.; GAEDKE, M. Interoperability in internet of things: Taxonomies and open challenges. *Mobile networks and applications*, Springer, v. 24, p. 796–809, 2019.

OU, W.; HUANG, S.; ZHENG, J.; ZHANG, Q.; ZENG, G.; HAN, W. An overview on cross-chain: Mechanism, platforms, challenges and advances. *Computer Networks*, Elsevier, v. 218, p. 109378, 2022.

WEGNER, P. Interoperability. *ACM Computing Surveys (CSUR)*, ACM New York, NY, USA, v. 28, n. 1, p. 285–287, 1996.