

Título:

Interoperabilidade entre plataformas *Blockchain* com *Cross-chain*

Autores e Orientadores:

Gabriel Antonio Lopes de Castro¹; Daniel José Diaz²; Paulo Caetano da Silva (Dr)¹;

¹Universidade Salvador (UNIFACS), gabriel.aldc7@gmail.com:

caetano.paulo@animaeducacao.com.br

²Universidade Rosario, ddiaz@fcecon.unr.edu.ar

Resumo:

A *Blockchain* é uma rede peer-to-peer que utiliza criptografia para garantir segurança, imutabilidade e anonimato em transações distribuídas. Com a expansão de casos de uso e o surgimento de diversas plataformas, a interoperabilidade entre elas se tornou essencial para permitir inovação e novos serviços. Atualmente, a falta de integração eficiente entre *Blockchains* é uma das principais limitações, e várias soluções têm sido propostas, incluindo tecnologias *Cross-chain*, que atuam como protocolos de comunicação entre redes. No entanto, muitas dessas abordagens enfrentam desafios, como limitação a trocas simples de ativos, introdução de elementos centralizados e problemas de escalabilidade e eficiência. O futuro da interoperabilidade depende de avanços em áreas como consenso descentralizado, segurança *Cross-chain* e padronização. Este artigo apresenta uma revisão sistemática da literatura, com foco no uso de tecnologias *Cross-chain* para melhorar a interoperabilidade entre diferentes plataformas *Blockchain*.

Palavras-chave: *Blockchain*; *Cross-Chain*; *Interoperabilidade*

Introdução

A tecnologia *Blockchain* é uma inovação proposta pela primeira vez por Satoshi Nakamoto em 2008. A rede *Blockchain* é uma rede *peer-to-peer* que depende de criptografia para alcançar imutabilidade e anonimato no armazenamento e processamento de dados através de arquiteturas de sistemas distribuídos com mecanismos de consenso. O sistema *Blockchain* permite que usuários alcancem um consenso sem a intervenção de uma organização de terceiros e resolve problemas de confiança e valor dos dados na Internet com baixo custo. Com sua capacidade de armazenar dados e realizar computações de maneira descentralizada e imutável, a *Blockchain* mostra potencial em diversas áreas de aplicação, como criptomoedas, agricultura, cuidados médicos, finanças, energia e cadeias de suprimentos.

Apesar do progresso, uma das principais limitações das plataformas *Blockchain* é a falta de interoperabilidade entre diferentes redes. Redes *Blockchain*

independentes são como ilhas isoladas, enfrentam desafios significativos na troca de dados e transferência de ativos, o que resulta em fragmentação e ineficiência. A interoperabilidade entre plataformas *Blockchain* é crucial para permitir um ecossistema verdadeiramente integrado, onde ativos e dados podem fluir entre diferentes plataformas.

Várias soluções têm sido propostas para abordar a interoperabilidade das redes *Blockchain*, incluindo tecnologias de *Cross-chain*. As tecnologias de *Cross-chain*, como esquemas de notário, hash-locking e relays, têm como objetivo facilitar a comunicação entre diferentes plataformas *Blockchain*. A tecnologia *Cross-chain* pode ser entendida como um protocolo de comunicação entre *Blockchain*. No contexto de *Blockchain* e tecnologia de *Cross-chain*, um notário é uma entidade ou um grupo de entidades que atuam como intermediários confiáveis em transações entre diferentes *Blockchain*. No entanto, essas tecnologias enfrentam desafios específicos: os notários podem ser maliciosos, o hash-locking limita os cenários de aplicação à troca de ativos e os relays são difíceis de implantar em cenários reais. Além disso, muitos protocolos dependem de intermediários centralizados, o que contraria o princípio de descentralização da *Blockchain*.

Este artigo apresenta uma Revisão Sistemática da Literatura (RSL) com o objetivo de analisar o estado da arte sobre o uso de *Cross-chain* para facilitar a interoperabilidade entre diferentes plataformas *Blockchain*. Em razão do crescente uso da *Blockchain*, faz-se necessário uma avaliação sobre o estado atual da interoperabilidade entre suas plataformas, de forma a permitir a melhora de atividades realizadas nas plataformas, além de poder inovar e realizar novos serviços.

Métodos

Os objetivos da revisão da literatura foram fornecer elementos entender os estudos disponíveis relacionados à interoperabilidade entre plataformas *Blockchain*. A primeira etapa da metodologia foi a definição das questões de pesquisa. A seguir foram definidos os critérios de inclusão e exclusão dos artigos identificados na busca no repositório IEEE. Além dos critérios inclusão e exclusão, considera-se crítico avaliar a qualidade dos estudos. A partir do trabalho do guia emitido pela Keele University (Keele, 2007), foram definidas perguntas de qualidade usadas no processo de seleção.

A consulta com a string de busca retornou 1440 artigos, após uma leitura do título e do abstract para identificar aqueles que estivessem relacionados ao tema. Em seguida a string foi refinada, aplicando-se as mesmas etapas anteriores, de forma a

se restringir aos trabalhos relacionados com interoperabilidade com *Cross-chain*, sendo encontrados 128 artigos.

Após a execução desta fase, 49 artigos foram selecionados. Sendo feita uma análise sobre os artigos com a leitura completa dos artigos selecionados. Então, após aplicar os critérios de qualidade, excluir os artigos duplicados e os que não foram possíveis efetuar o Download, restaram 14 artigos.

Resultados e discussão

Com base nas respostas dos 14 artigos, observa-se que há uma diversidade de abordagens em relação ao uso de *Blockchain* permissionada. Embora alguns artigos explorem a aplicação de *Blockchain* permissionadas [1, 2, 3, 7], a maioria foca em *Blockchain* públicas ou não fornecem detalhes suficientes para determinar com clareza o tipo de *Blockchain* [8, 9, 11, 15]. Alguns artigos [4, 10, 13, 14] destacam o uso de *Blockchain* públicas e descentralizadas, como Ethereum e Bitcoin, ou mencionam redes de teste públicas como Ropsten, Kovan e Goerli [13].

Os artigos [9, 12 e 13] mencionam APIs existentes para facilitar a interação entre *Blockchains*. Porém, a maioria não menciona APIs ou sua aplicação no escopo discutido. Alguns artigos sugerem, embora não tenha menção direta [5, 7, 8, 10, 11, 2]. Outros artigos não fazem menção explícita a APIs, indicando que o foco principal está em outros aspectos da *Blockchain* [1, 4, 3, 14, 15].

A análise dos 14 artigos revela que a maioria propõe ou discute diferentes arquiteturas baseadas em *Blockchain* com foco em soluções de interoperabilidade e comunicação entre redes *Blockchain*. Essas arquiteturas variam significativamente refletindo a diversidade de abordagens nesse domínio.

A menção ao uso de *frameworks* não está presente na maioria dos artigos, apenas alguns citam ferramentas específicas para apoiar o desenvolvimento ou implementação das propostas [2, 9, 12, 13].

O uso de *Smart Contracts* para facilitar a interoperabilidade entre plataformas *Blockchain* é citado em alguns artigos [4, 5, 8, 9, 10, 11] para gerenciar transferências, comunicação entre cadeias e sincronização de estados. Os artigos [2, 13, 3, 14, 15] mencionam algum tipo ou uso de *Smart Contracts*, enquanto os artigos [1, 7, 12] não mencionam o seu uso para interoperabilidade.

Com relação ao uso de protocolos de consenso para interoperabilidade, alguns trabalhos abordam essa questão, embora a abordagem e o foco variem entre eles. Os artigos [3, 5, 8, 9] usam protocolos de consenso no contexto da interoperabilidade.

Os artigos [1, 2] mencionam não de forma explícita. Os artigos [4, 7, 10, 11, 12, 13, 14, 15] não mencionam uso para interoperabilidade.

Um dos principais obstáculos para a interoperabilidade entre plataformas *Blockchain* se trata da natureza intrinsecamente isolada dessas redes. Isso se dá devido a cada *Blockchain* possuir suas próprias regras, algoritmos de consenso e arquiteturas, que por sua vez, dificultam a comunicação direta e o compartilhamento de dados e ativos. Tecnologias como *hash-locking*, esquemas de notário, e *relays* vêm sendo propostas para abordar essa limitação, porém todas enfrentam dificuldades práticas. O *hash-locking*, por exemplo, limita-se à troca de ativos, não sendo eficaz em cenários mais complexos, como *Smart contracts interBlockchain*. Esquemas de notário, por outro lado, introduzem um elemento centralizado de confiança, o que vai contra o princípio de descentralização que define as redes *Blockchain*. Já os *relays* oferecem potencial de interconexão, mas são complexos de implementar e ainda apresentam desafios de escalabilidade e eficiência [4, 7, 9].

Além disso, outro ponto crítico é a segurança. Protocolos que conectam diferentes *Blockchain*, como as pontes *Cross-chain*, podem ser vulneráveis a ataques, que por sua vez, acabam comprometendo a confiança e a segurança das transações. Nessa mesma lógica, questões como gastos duplos e ataques de *replay* ainda representam um risco considerável. Da mesma maneira, a descentralização de soluções de interoperabilidade também é um grande desafio, pois muitas propostas ainda dependem de intermediários centralizados, o que pode criar pontos únicos de falha e comprometer a segurança e a eficiência do sistema [5, 12].

A utilização de contratos inteligentes para a comunicação entre plataformas *Blockchain* também apresenta uma oportunidade crescente. Ao implementar *Smart contracts* que garantam a integridade das transações entre diferentes redes, sem a necessidade de intermediários, torna-se possível realizar operações mais complexas, como a execução destes contratos entre plataformas heterogêneas [3, 4, 5, 9, 10, 11, 13, 14, 15].

Conclusões

A interoperabilidade entre plataformas *Blockchain* continua sendo um campo de extrema relevância para o futuro das tecnologias descentralizadas. Através desta revisão da literatura, foi possível identificar tanto os avanços quanto as barreiras que ainda precisam ser superadas para que soluções de interoperabilidade, como *Cross-chain*, se tornem plenamente funcionais, escaláveis e atinjam seu potencial máximo.

Embora tecnologias como *hash-locking*, esquemas de notário, e *relays* tenham sido desenvolvidas para facilitar a comunicação entre redes *Blockchain*, elas enfrentam desafios práticos, como a limitação na troca de ativos e a centralização em alguns mecanismos, o que vai contra o princípio fundamental da descentralização.

Soluções mais recentes, como *Polkadot* e *Cosmos*, que utilizam *Sidechains* e *Parachains*, têm demonstrado grande potencial ao oferecer maior escalabilidade e segurança nas interações entre *Blockchains*. Ao mesmo tempo, o uso de *Smart contracts* está emergindo como uma forma eficaz de facilitar transações e operações mais complexas entre redes, reduzindo a necessidade de intermediários e promovendo um ecossistema mais descentralizado [5, 9].

No entanto, o progresso até agora ainda aponta para a necessidade de mais pesquisas e inovações. Os principais desafios, como segurança, escalabilidade e a padronização de protocolos, ainda precisam ser abordados de forma abrangente. A adoção de soluções *Cross-chain* em larga escala dependerá da capacidade dos pesquisadores e desenvolvedores de superar essas limitações e criar plataformas que possam operar com eficiência e confiança em diferentes redes *Blockchain*.

Portanto, o futuro da interoperabilidade entre plataformas *Blockchain* é promissor, mas depende de novos avanços em áreas como consenso descentralizado, segurança *Cross-chain*, e mecanismos padronizados que possam garantir que as *Blockchains*, independentemente de suas diferenças estruturais, possam interagir de maneira segura, eficiente e escalável.

Referências

[1] Guan-Yan Yang; Kuo- Hui Yeh; Lin- Fa Lee (2021) Towards a Novel Interoperability Management Scheme for Cross- *Blockchain* Transactions, *IEEE 10th Global Conference on Consumer Electronics (GCCE)*.

[2] Yangyang Sun; Longyang Yi; Li Duan; Wei Wang (2022) A Decentralized Cross-chain Service Protocol based on Notary Schemes and Hash- Locking, *2022 IEEE International Conference on Services Computing (SCC)*.

[3] Zhipeng Gao; Hongli Li; Kaile Xiao; Qian Wang (2020) Cross-chain Oracle Based Data Migration Mechanism in Heterogeneous *Blockchain*, *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*.

[4] Christopher G. Harris (2023) Cross-chain Technologies: Challenges and Opportunities for *Blockchain* Interoperability, *2023 IEEE International Conference on Omni- layer Intelligent Systems (COINS)*.

[5] H. Mao, T. Nie, H. Sun, D. Shen and G. Yu, "A Survey on Cross-Chain Technology: Challenges, Development, and Prospect," in *IEEE Access*, vol. 11, pp. 45527-45546, 2023, doi: 10.1109/ACCESS.2022.3228535.

[6] Keele, S. (2007) Guidelines for Performing Systematic Literature Reviews in Software Engineering, Technical Report, Ver. 2.3 EBSE Technical Report.

[7] M. Darshan; Matthieu Amet; Gautam Srivastava; Jorge Crichigno (2023) An Architecture That Enables Cross-chain Interoperability for Next-Gen *Blockchain* Systems, *IEEE Internet of Things Journal* (Volume: 10, Issue: 20, 15 October 2023).

[8] Lu Lin; Jiayi Li; Yuzhen Wang; Qiong Wang (2023) A Survey on Cross-chain Asset Transfer Schemes: Classification, Challenges, and Prospects, 2023 International Conference on Networking and Network Applications (NaNA).

[9] Kirtirajsinh Zala; Vyom Modi; Deepakkumar Giri; Biswaranjan Acharya; Saurav Mallik; Hong Qin (2023) Unlocking *Blockchain* Interconnectivity: Smart Contract-Driven Cross-chain Communication, *IEEE Access* (Volume: 11).

[10] Yue Li; Han Liu; Yuan Tan (2022) POLYBRIDGE: A Cross chain Bridge For Heterogeneous *Blockchains*, 2022 IEEE

International Conference on *Blockchain* and Cryptocurrency (ICBC).

[11] Martin Westerkamp; Axel Küpper (2022) SmartSync: Cross-*Blockchain* Smart Contract Interaction and Synchronization, 2022 IEEE International Conference on *Blockchain* and Cryptocurrency (ICBC).

[12] Felix Härrer (2022) Towards Interoperability of Open and Permissionless *Blockchains*: A Cross-chain Query Language, 2022 IEEE International Conference on e-Business Engineering (ICEBE).

[13] Monika; Ankit Goyal; Shivam Raina; Kashish Bhatia; Rajesh Bhatia (2021) Atomic Cross-chain Asset Exchange for Ethereum Public Chains, 2021 International Conference on Computer Communication and Informatics (ICCCI).

[14] Marten Sigwart; Philipp Frauenthaler; Christof Spanring; Michael Sober; Stefan Schulte (2021) Decentralized Cross-*Blockchain* Asset Transfers, 2021 Third International Conference on *Blockchain* Computing and Applications (BCCA).

[15] Zuqiang Ke; Jongho Seol; Abhilash Kancharla; Nohpill Park (2022) Performance Modeling and Assurance for Cross Chain, 2022 Fourth International Conference on *Blockchain* Computing and Applications (BCCA).

Fomento:

O trabalho teve a concessão de Bolsa pelo PIBIC CNPQ