INTEROPERABILIDADE ENTRE PLATAFORMAS BLOCKCHAIN COM CROSS-CHAIN

Gabriel Antonio Lopes de Castro, Daniel José Diaz, Paulo Caetano da silva

Unifacs
Ciência da computação, Tancredo Neves , caetano.paulo@animaeducacao.com.br

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.

Objetivos

A revisão sistemática da literatura foi conduzida para identificar trabalhos que abordam interoperabilidade entre plataformas Blockchain, dando ênfase na tecnologia Cross-chain. Os objetivos foram fornecer elementos para a apresentação de dados de pesquisa, descobrir o sistemamais adequado para coleta e análise de dados e entender os estudos disponíveis relacionados à interoperabilidade entre plataformas Blockchain.

Metodologia

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

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 P*arachains*, 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.

Bibliografia

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