Uso de redes peer-to-peer em Blockchain

Universidade Federal de Santa Catarina

Graduação em Ciência da Computação

Setembro de 2023

Tális Breda - 22102202

Título:

Uso de redes peer-to-peer em Blockchain

Resumo:

A Blockchain é uma tecnologia que vem ganhando muita popularidade nos últimos anos, por conta de sua flexibilidade e segurança. Neste artigo, serão apresentados alguns conceitos, problemas e soluções relacionadas às redes peer-to-peer (P2P), que são a base das redes blockchain atualmente. Uma rede P2P é uma arquitetura de rede onde os dispositivos individuais, chamados de "peers," interagem diretamente uns com os outros, em vez de dependerem de um servidor central. Todos os peers têm papéis semelhantes e podem agir tanto como clientes quanto como servidores, compartilhando recursos e informações entre si. Os problemas desse tipo de rede estão relacionados com seu desempenho e, como será visto em sequência, anonimidade, no caso de redes maiores. Além da apresentação dos problemas, serão estudadas propostas de solução para alguns deles, provenientes de diversos autores.

1. Introdução

1.1. Motivação e justificativas

Nos últimos anos, a tecnologia blockchain tem desempenhado um papel significativo em diversas indústrias devido à sua capacidade de criar registros descentralizados e imutáveis. No entanto, para garantir a eficácia das blockchains, é essencial considerar a infraestrutura base, e as redes peer-to-peer (P2P) desempenham um papel crucial nesse contexto. Este artigo explora a interseção entre blockchains e redes P2P, examinando como a adoção estratégica dessas redes pode otimizar a comunicação entre os nós participantes. A motivação reside na necessidade de compreender as complexidades das redes P2P em blockchains, impulsionar a escalabilidade, eficiência energética e segurança, e promover a descentralização e inclusão na tecnologia blockchain. A pesquisa oferece insights valiosos para a comunidade blockchain, contribuindo para o avanço contínuo dessa inovação disruptiva.

Em resumo, este estudo investiga como as redes P2P podem aprimorar o desempenho e a segurança das blockchains, oferecendo uma infraestrutura de comunicação robusta entre os participantes. Isso se torna cada vez mais relevante à medida que a blockchain se expande para diversas aplicações, e o conhecimento gerado pela pesquisa pode beneficiar desenvolvedores e pesquisadores na melhoria contínua da tecnologia blockchain, alinhando-a com as demandas crescentes por escalabilidade, eficiência e descentralização.

1.2. Objetivos

1.2.1. Objetivo geral

Este artigo tem como objetivo investigar a integração estratégica das redes peer-to-peer (P2P) em blockchains, destacando seu potencial para solucionar problemas críticos associados às P2P e, assim, otimizar o desempenho e a segurança das blockchains.

1.2.2. Objetivos específicos

- Identificar os problemas e desafios enfrentados pelas redes P2P quando utilizadas em blockchains e explorar soluções potenciais para essas questões.
- Apresentar casos em que a integração estratégica de redes P2P foi bem-sucedida em resolver problemas específicos de blockchains, destacando as lições aprendidas e as melhores práticas.

1.3. Organização do artigo

O presente artigo está organizado da seguinte forma:

- **Seção 2 - Conceitos básicos:** serão abordados e explicados alguns conceitos básicos, necessários para a compreensão do assunto de forma geral
- **Seção 3 - Trabalhos correlatos:** aqui serão citados e resumidos alguns trabalhos que foram utilizados como referência para este artigo
- **Seção 4 - Aspectos relevantes:** serão levantados alguns pontos importantes, tanto relacionados aos trabalhos correlatos, quanto ao assunto no geral
- **Seção 5 - Problemas existentes:** aqui serão apresentados alguns problemas relacionados ao assunto
- **Seção 6 - Possíveis soluções:** aqui serão mostradas algumas propostas feitas por outros autores para resolver alguns dos problemas citados
- **Seção 7 - Projeto e desenvolvimento de uma proposta:** aqui será apresentada uma proposta para lidar com os problemas citados
- **Seção 8 - Conclusão e trabalhos futuros:** aqui será apresentada a conclusão do que foi estudado no artigo, além de coisas que podem ser feitas no futuro sobre o assunto.
- **Referências bibliográficas:** Referências de outros artigos

2. Conceitos básicos

2.1. Rede Peer-to-Peer (P2P)

Em uma rede P2P, não há uma autoridade central ou servidor dominante. Em vez disso, todos os dispositivos são iguais e colaboram para compartilhar recursos, como arquivos, poder de processamento ou largura de banda. Essa arquitetura descentralizada oferece vantagens, como resistência a falhas, escalabilidade e redução da carga em servidores centrais. No contexto das blockchains, as redes P2P são usadas para conectar os nós participantes e facilitar a comunicação e a transferência de informações, tornando-se uma parte essencial da infraestrutura blockchain.

Exemplos de redes P2P incluem o BitTorrent, onde usuários compartilham arquivos diretamente uns com os outros, e o Bitcoin, uma criptomoeda que opera em uma rede P2P descentralizada.

2.2. Blockchain

Uma blockchain é um registro digital público e imutável que armazena transações ou informações em blocos interconectados. Cada bloco contém um conjunto de registros e um hash (uma impressão digital única) do bloco anterior. Uma vez adicionada, uma transação não pode ser alterada, tornando a blockchain resistente a adulterações.

A blockchain é o cerne da tecnologia que sustenta criptomoedas, como o Bitcoin, mas também é aplicada em muitos outros setores. Ela oferece transparência, segurança e confiabilidade por meio de uma rede descentralizada. A adição de novos blocos é feita através de um processo de consenso, como o Proof of Work (PoW) ou o Proof of Stake (PoS), que garante a integridade das transações. As redes P2P são usadas para disseminar e validar as transações entre os nós da blockchain, tornando-a acessível a todos os participantes da rede e garantindo a segurança e a descentralização que são características essenciais das blockchains.

3. Trabalhos correlatos

3.1. Revisão bibliográfica sistemática

Palavra-chave	**Resultados**
“Peer-to-peer”	1.360.000
“Peer-to-peer networks”	1.060.000
“Blockchain”	519.000
“Blockchain” AND “peer-to-peer”	163.000
“Blockchain” AND “peer-to-peer networks”	70.500

3.2. Strategic Latency Reduction in Blockchain Peer-to-Peer Networks

Blockchains são comumente construídas com base em redes peer-to-peer, que proporcionam segurança e flexibilidade essenciais para seu funcionamento apropriado. Porém, a desvantagem desse tipo de rede é a performance, que é baixa por conta da alta latência da rede. Em grande parte das aplicações, isso não é um problema, porém recentemente começaram a surgir aplicações em que a baixa latência é crucial para a integridade da aplicação.

O trabalho de Tang et al. (2023) divide essa latência em dois tipos:

- **Latência Direta:** Latência direta refere-se ao atraso entre o envio de uma transação por um nó específico (a vítima) e seu recebimento por um nó pertencente a um agente, calculado como uma média para todas as transações da vítima. Também pode ser uma média para todos os nós de origem na rede em vez de uma vítima específica.

- **Latência Triangular:** Latência triangular diz respeito à capacidade de um nó de agente "atalhar" caminhos entre um remetente e um receptor, medindo a diferença entre o atraso total no caminho envolvendo o nó do agente e o menor atraso em caminhos que não o incluem. A latência triangular global é a média dessa latência relativa entre todos os pares de origem e destino na rede.

Os autores propõem o Peri, que é uma variação do Perigee, um protocolo usado para reduzir a latência da comunicação em redes peer-to-peer, influenciando as ações dos diversos agentes da rede para atingir essa redução. O Peri modifica as técnicas usadas pelo Perigee, adaptando-as para agentes individuais. Os autores mostram vantagem de latência direta e triangular nos agentes que usam Peri, comparado aos que não usam.

3.3. Efficient topology control of blockchain peer to peer network based on SDN paradigm

Similar ao artigo anterior, aqui Deshpande et al. (2022) mencionam que, apesar dos diversos benefícios da utilização de redes peer-to-peer em Blockchain, um problema ainda é o desempenho. Neste caso, a preocupação é com dispositivos de capacidade computacional limitada, que podem não suportar aplicações Blockchain.

Para resolver esse problema, os autores focam no controle de topologia, propondo uma maneira de reduzir esse controle mantendo as características que tornam esse tipo de aplicação viável, como flexibilidade, reconfigurabilidade, conectividade, etc. Essa maneira é a utilização do paradigma Software-Defined Networking (SDN) para gerenciamento da rede Blockchain.

Utilizando este paradigma, o controle de topologia que era de responsabilidade dos “peers”, passa para uma camada segura composta de múltiplos servidores com bancos de dados sincronizados. Essa camada constrói a estrutura topológica da rede em dígrafos r-out, que são grafos em que todos os nodos têm a mesma quantidade de saídas para outros nodos. Além disso, são estabelecidos limites inferiores e superiores de conexão para os nodos, mantendo a conectividade e viabilidade da rede P2P.

4. Aspectos relevantes

A popularidade da blockchain vem crescendo bastante nos últimos anos, tendo alguns picos de popularidade com “booms” de algumas tecnologias (bitcoin, NFT, cryptogames). A blockchain, por definição, é uma rede descentralizada que armazena informações de transações e, por isso, o uso de redes peer-to-peer é essencial para o funcionamento adequado dela.

Com esse aumento da popularidade, diversas aplicações vêm implementando essa tecnologia, visando os benefícios que ela proporciona, principalmente a flexibilidade e a segurança. Porém, nem toda aplicação pode fazer uso dela por conta de fatores de desempenho, portabilidade, latência, entre outros. Felizmente, como visto na seção 3, diversos autores vêm estudando essas redes e propondo soluções para alguns desses problemas.

Por exemplo, Tang et al. propõem uma adaptação de um protocolo já existente para uso nas redes P2P, a fim de minimizar latência; Howell et al. propõem um framework de processamento de dados chamado NodeMaps, cujo objetivo é analisar redes blockchain e o quão elas são descentralizadas; Sharma et al. estudam a anonimidade nas redes P2P, através da análise e comparação de diversas soluções previamente propostas.

5. Problemas existentes

Como mencionado por diversos autores e já mencionado neste artigo, um dos principais problemas das redes peer-to-peer é o desempenho. Apesar de que muitas aplicações não são afetadas por isso, o recente crescimento da tecnologia blockchain e a grande quantidade de aplicações que surgem por conta disso fazem com que um bom desempenho seja necessário em vários casos.

Além do desempenho, outro problema das redes P2P é a anonimidade. Segundo estudos de Sharma et al., o tamanho de uma rede e a anonimidade de seus peers são inversamente proporcionais, ou seja, quanto maior a rede, menor a anonimidade. Os autores propõem um framework para analisar diversas tecnologias e suas respectivas eficácias nesse quesito.

Outros desafios existentes quando falamos em redes peer-to-peer e blockchains são o gerenciamento de recursos entre seus peers, que se feito de forma inadequada, pode provocar gargalos de desempenho na rede, afetando aplicações em que a baixa latência é crucial; e a garantia de integridade dos dados, que apesar de ser um dos principais motivos da viabilidade de Blockchains, ainda é uma dificuldade em redes P2P normais.

6. Possíveis soluções

Para o problema de desempenho, existem diversas soluções. Neste trabalho, serão citadas duas delas. A primeira é de autoria de Tang et al., e já foi comentada anteriormente neste artigo. Trata de um estudo dos tipos de latência existentes em uma rede Blockchain P2P, e da eficiência de soluções já existentes. Os autores propõem uma variação do Perigee, protocolo que influencia decisões dos agentes da rede P2P a fim de otimizar latência: o Peri, que aplica modificações a esse protocolo focadas em agentes individuais. Seus testes mostraram resultados promissores, com latências mais baixas para os nodos que utilizaram o Peri.

A segunda, também já mencionada neste artigo, é de autoria de Deshpande et al., e encara o problema de uma maneira diferente. Os autores estudam a estrutura e o controle desta dentro da rede, propondo a utilização do paradigma SDN (Software-Defined Networking) para tirar o controle topológico da responsabilidade dos peers e passá-lo para um conjunto de servidores com banco de dados compartilhado. Os autores mostram testes comprovando a eficiência do método.

Já Pradhan et al. focam em resolver um outro problema: ataques cibernéticos. Mais especificamente, ataques em redes de troca de energia baseadas em redes peer-to-peer e blockchain. Os autores propõem o uso de um framework baseado em Corda que tem o objetivo de mitigar ciberataques. Esse framework faz uso de protocolos como TLS (Transport LAyer Security) e AMQP (Advanced Message Queuing Protocol) para lidar com transações, além de otimizações relacionadas ao uso de CPU e memória.

Por fim, Howell et al. propõem uma ferramenta chamada NodeMaps para analisar e visualizar dados de redes Blockchain P2P, a fim de estudar a descentralização dessas redes e perceber possíveis problemas.

7. Projeto e desenvolvimento de uma proposta

Em seu trabalho “Efficient topology control of blockchain peer to peer network based on SDN paradigm”, Deshpande et al. comentam sobre o fato de algumas blockchains serem inviáveis em dispositivos com recursos limitados. Também falam sobre os diferentes tipos de “blockchains permissionadas”, que tipo de rede P2P cada uma necessita, e como essa rede pode ser visualizada.

Fazendo essa análise, os autores concluem que grande parte dos frameworks de blockchain podem ser visualizados como dígrafos *r-out* aleatórios (grafo direcionado onde cada nodo tem exatamente r arestas de saída). Com base nisso, o objetivo da pesquisa é desenvolver um dígrafo *r-out* aleatório para blockchains que pode ser usado em dispositivos com recursos limitados. O valor de r de cada grafo deve ser adaptado dinamicamente de acordo com a conectividade, diâmetro e agrupamento de cada blockchain.

O artigo estuda melhorar o controle da topologia de blockchains, que pode ser dividido em duas partes: construção e manutenção. Construção da topologia se refere ao descobrimento de peers e seus vizinhos, e manutenção está relacionada ao mantimento da estrutura topológica quando peers entram ou saem. Essa abordagem traz dois problemas: custo adicional e falta de flexibilidade.

- **Custo adicional:** vem por conta da quantidade de operações extras que uma rede P2P precisa executar, assim consumindo mais energia, processamento, banda larga e memória, fazendo com que dispositivos com recursos limitados tenham problemas ao utilizar essas blockchains.
- **Falta de flexibilidade:** quando um peer entra ou sai da rede, a manutenção da topologia é feita pelos peers envolvidos, causando lentidão especialmente em redes maiores. Os autores propõem o uso do paradigma SDN, que desloca a responsabilidade de manutenção da topologia dos peers para uma camada dedicada, com múltiplos servidores, a fim de melhorar o desempenho da rede.

Outros conceitos importantes para a proposta são:

- **Conectividade:** boa conectividade facilita a rápida disseminação de informações e evita a formação de bifurcações prejudiciais. Quando a rede se desconecta, formando sub-redes independentes, isso cria oportunidades para ataques de gastos duplos. Além disso, sub-redes isoladas podem não ter um histórico completo de transações, tornando bifurcações inválidas. Isso pode facilitar, também, ataques DDoS.
- **Diâmetro menor:** Um diâmetro menor na rede P2P proporciona uma disseminação mais rápida de informações e, como resultado, reduz o número de bifurcações transitórias em uma blockchain específica. Isso melhora a

confiabilidade geral da blockchain, diminui o tempo de mineração e garante a inclusão efetiva das transações na cadeia principal.

- **Eficiência de consenso:** Os protocolos de consenso em blockchain buscam manter uma cópia idêntica do livro-razão entre nós honestos, tolerando um número limitado de falhas. A capacidade de resolver problemas de consenso depende da sincronia da rede, que pode ser síncrona, parcialmente síncrona ou assíncrona. O consenso é impossível em redes completamente assíncronas sem uma referência de tempo global. Portanto, o estudo se concentra no cenário parcialmente síncrono.

A otimização da topologia de blockchain para cenários específicos envolve a modelagem dos principais tópicos usando a teoria dos grafos. A construção da rede P2P começa com a descoberta de pares, que pode ser distribuída ou centralizada. O foco está na geração de um tipo especial de grafo chamado r-out digraph para modelar a rede P2P. Esses dígrafos r-out podem ser gerados de duas maneiras: centralizada e distribuída, considerando as propriedades de descoberta de pares em ambas as abordagens.

- **Geração centralizada:** A geração de um grafo r-out centralizado permite uma rápida descoberta de pares, o que é vantajoso para dispositivos móveis e nós remotos com recursos limitados, como no contexto da IoT. No entanto, essa abordagem é vulnerável a ataques de negação de serviço (DoS) e à falha do servidor centralizado (SPoF), exigindo a presença de servidores de backup para mitigar esses problemas. O controle da topologia é mais simples com a abordagem centralizada, permitindo uma reconstrução eficiente da topologia quando nós entram ou saem da rede.
- **Geração distribuída:** O método distribuído de geração de grafo r-out é amplamente utilizado em arquiteturas de blockchain, especialmente em blockchains públicas ou não-permissionadas. Nesse método, cada nó individual escolhe seus próprios r pares de vizinhos, o que simplifica o processo, não envolvendo uma entidade centralizada. Essa abordagem é mais resiliente contra falhas de outros nós, mas requer mais recursos. No entanto, ela torna a arquitetura da blockchain imune a ataques como DDoS, pois qualquer nó pode participar sem controle de acesso centralizado. No entanto, existem desvantagens, como a dificuldade de controlar a topologia da rede e os recursos adicionais necessários para o protocolo de descoberta de vizinhos. A falta de um banco de dados centralizado torna mais difícil verificar transações de dados em redes de blockchain não-permissionadas.

Na proposta, o foco está na geração centralizada, por conta da dificuldade em criar redes otimizadas por geração distribuída

De acordo com o modelo proposto anteriormente usando SDN, a rede fica dividida em duas camadas:

- **Camada superior - servidores:** Como descrito anteriormente, essa camada é composta por diversos servidores com banco de dados compartilhado, e é responsável por construir e manter a topologia da rede.
- **Camada inferior - peers:** Os peers são divididos entre contribuintes e não-contribuintes. Contribuintes são os que suportam o banco de dados da blockchain, roteamento, informações, etc. São ideais para o funcionamento da rede. Não-contribuintes são fontes de novas informações, e não são essenciais para o funcionamento.

Assim, através de testes e experimentos, os autores demonstraram maior desempenho e menor consumo de recursos desse modelo.

8. Conclusão e Trabalhos futuros

Com base nos estudos e trabalhos mencionados, conclui-se que o uso de redes P2P em blockchain é essencial para a viabilidade da mesma, porém ainda apresenta diversos problemas com relação a desempenho, custo, segurança, etc. Felizmente, vários pesquisadores e profissionais estão trabalhando para criar soluções para esses problemas, e algumas destas soluções mais recentes foram vistas neste artigo.

Percebe-se que existem possíveis soluções para muitos desses tópicos: Pradhan et al. sugeriram um framework para mitigar ataques cibernéticos nas redes; Tang et al. sugeriram um protocolo para reduzir a latência entre os nodos de uma rede; Deshpande et al. sugeriram um modelo de controle topológico que melhora a eficiência de uma rede; Howell et al. sugeriram um framework para monitorar a descentralização de redes blockchain a fim de encontrar possíveis problemas.

Apesar de todo o ótimo trabalho feito por esses pesquisadores, a área de blockchain ainda está em constante evolução, e muito mais esforço será necessário para reduzir e combater alguns dos problemas e vulnerabilidades que algumas aplicações apresentam.

REFERÊNCIAS

HOWELL, Andrew; SABER, Takfarinas; BENDECHECHE, Malika. Measuring node decentralisation in blockchain peer to peer networks. **Blockchain: Research and Applications**, v. 4, n. 1, 2023. ISSN 2096-7209. Disponível em: https://doi.org/10.1016/j.bcra.2022.100109. Acesso em: 08 set. 2023.

TANG, Weizhao et al. Strategic Latency Reduction in Blockchain Peer-to-Peer Networks. Proc. **ACM Meas. Anal. Comput. Syst**., v. 7, n. 2, p. 32-33, jun. 2023. ISSN 2576-5514. Disponível em: https://doi.org/10.1145/3589976. Acesso em: 08 set. 2023.

DESHPANDE, Varun; BADIS, Hakim; GEORGE, Laurent. Efficient topology control of blockchain peer to peer network based on SDN paradigm. **Peer-to-Peer Networking and Applications**, v. 15, n. 1, p. 267-289, 2022. ISSN 1936-6450. Disponível em: https://doi.org/10.1007/s12083-021-01248-6. Acesso em: 08 set. 2023.

SHARMA, Piyush Kumar; GOSAIN, Devashish; DIAZ, Claudia. On the Anonymity of Peer-To-Peer Network Anonymity Schemes Used by Cryptocurrencies. In: Network and **Distributed System Security (NDSS) Symposium 2023**, 27 de fevereiro a 3 de março de 2023, San Diego, CA, USA. ISBN 1-891562-83-5. Disponível em: https://dx.doi.org/10.14722/ndss.2023.23241. Acesso em: 08 set. 2023.

PRADHAN, Nihar Ranjan et al. Performance Evaluation and Cyberattack Mitigation in a Blockchain-Enabled Peer-to-Peer Energy Trading Framework. ***Sensors***, v. 23, n. 2, artigo 670, 2023. Disponível em: https://www.mdpi.com/1424-8220/23/2/670. ISSN 1424-8220. DOI: 10.3390/s23020670.