AVALIAÇÃO DOS IMPACTOS DA REMOÇÃO DOS COMITÊS DE VALIDAÇÃO EM MECANISMOS DE CONSENSO PROOF-OF-STAKE PARA BLOCKCHAINS PÚBLICAS

Palavras-Chave: Blockchain, consenso distribuído, comitê de validação

Autores(as):

Filipe Franco Ferreira – FEEC - UNICAMP

Prof. Dr. Marco Aurélio Amaral Henriques – FEEC - UNICAMP

INTRODUÇÃO:

Nos últimos anos, as Blockchains públicas têm ganhado muita atenção devido a suas diversas aplicações, principalmente na criação de criptomoedas. Uma blockchain pode ser entendida como um livro razão distribuído, replicado de forma consistente entre todos os participantes da rede. Ela é formada de transações agrupadas em blocos, os quais formam uma sequência com uma ordem específica e, por isso, recebe o nome de cadeia de blocos. Após decorrido um período de consolidação em que um consenso é atingido pelos membros da rede, cada bloco (e consequentemente as transações neles contidas) é considerado confirmado e se torna imutável.

O mecanismo de consenso é uma das partes mais importantes de uma blockchain. Ele é definido por Bashir [1] como um conjunto de passos que são dados pelos nós que compõem a rede para entrar em consenso a respeito de um valor. Um mecanismo de consenso deve ser resistente à participação de nós desonestos na rede e capaz de lidar com uma rede assíncrona, em que não há garantia que as mensagens enviadas pelos participantes sejam recebidas por todos os demais dentro de um intervalo de tempo definido.

Os dois tipos de mecanismos de consenso mais utilizados são o Proof-of-Work (PoW) e o Proof-of-Stake (PoS). Nos mecanismos PoW, como aquele utilizado na blockchain da criptomoeda Bitcoin, para que um participante ganhe o direito de produzir um bloco, ele deve resolver um desafio computacional muito custoso em pouco tempo. Uma das principais desvantagens deste tipo de mecanismo é o grande desperdício energético na operação da blockchain. Assim, mecanismos PoS, que possuem um gasto energético menor, tornam-se mais atraentes.

Os mecanismos PoS utilizam a prova de posse de um "stake", um recurso associado ao nó como sua quantidade de moedas (por exemplo), para controlar o direito da criação de blocos, que normalmente ocorre por meio de sorteio. Dentre os mecanismos PoS, existem aqueles que necessitam de um comitê para validar os blocos produzidos e determinar quais deles poderão ser inseridos na

cadeia. São exemplos de mecanismos com comitês: Ouroboros [2], Algorand [3], Casper [4] e Tendermint [5]. No entanto, foi demonstrado recentemente que também é possível desenvolver mecanismos PoS seguros e mais simples sem utilizar um comitê de validação, optando por critérios probabilísticos para decidir a aceitação de um novo bloco. Essa é a abordagem proposta no Committeeless Proof-of-Stake (CPoS) [6], que está sendo desenvolvido pelo Grupo de Pesquisa em Segurança Aplicada (ReGrAS) da FEEC– Unicamp.

O trabalho desenvolvido nesta Iniciação Científica teve como objetivo estudar os mecanismos de consenso Proof-of-Stake com e sem comitê de validação, avaliando se um mecanismo Proof-of-Stake sem comitê é capaz de produzir um consenso e confirmar blocos com segurança e mais eficientemente que mecanismos que dependem de um comitê.

METODOLOGIA:

O CPoS é um mecanismo em que a geração e o compartilhamento de blocos é feito em intervalos de tempo pré-definidos, denominados de rodadas. A cada rodada os membros da rede participam de um sorteio que define quais participantes têm o direito de produzir um bloco (que armazena as transações divulgadas previamente na rede). Os vencedores do sorteio divulgam os blocos produzidos para os outros membros.

Para avaliar as vantagens e desvantagens de um mecanismo de consenso PoS sem um comitê de validação, partimos de códigos inicialmente desenvolvidos para o CPoS [7]. Estes códigos receberam diversos aprimoramentos ao longo da Iniciação Científica para permitir a escalabilidade do sistema, suportar uma blockchain com milhares de blocos, diminuir o número de mensagens trocadas pelos participantes, otimizar a estrutura da rede utilizada e a tornar mais resistente a problemas de conexão e a queda de participantes durante a execução do mecanismo.

Com o objetivo de avaliar o desempenho do CPoS, realizamos diversas execuções do mecanismo de consenso em uma rede distribuída. Utilizando a tecnologia de contêineres, foi construída uma rede de 25 participantes. A partir de informações da quantidade média de blocos e transações confirmadas por segundo, foram feitas diversas comparações com o mecanismo Casper utilizado na criptomoeda Ethereum, as quais destacaram as diferenças de desempenho entre as duas abordagens e mostraram os cenários em que CPoS é mais eficiente.

Para as análises de segurança, neste trabalho um nó desonesto é aquele que, ao produzir um bloco, não o divulga para outros participantes da rede. A partir de uma análise teórica do CPoS, é esperado que quanto mais participantes desonestos existam na rede, mais difícil seja a confirmação de blocos, gerando um atraso para ou impossibilitando o consenso. Foram feitas diversas execuções do mecanismo, variando a porcentagem de nós desonestos na rede e, a partir dos dados coletados sobre o atraso médio de confirmação de blocos, foi feita uma análise do nível de tolerância do CPoS à presença de nós desonestos.

RESULTADOS E DISCUSSÕES:

Dentre as melhorias feitas no código do CPoS, uma delas foi a troca do armazenamento de blocos feito em memória por um armazenamento em banco de dados (disco). Foi utilizado o banco MariaDB, um fork open source do MySQL. Isso permite que o sistema mantenha um bom funcionamento mesmo em uma blockchain com milhares de blocos.

Também foram implementados mecanismos que tornam a rede mais resistentes a problemas de comunicação e a queda de participantes. Para isso, quando um determinado nó para de responder e enviar mensagens para seus parceiros (normalmente devido a um problema de conexão), estes param de se comunicar com tal nó e conseguem continuar o mecanismo de consenso sem problemas. Além disso, foi criado um mecanismo para evitar que um participante que apresenta problemas de comunicação seja recomendado como parceiro para novos nós que entram no sistema.

Foram implementados um número máximo e mínimo de parceiros que cada participante da rede pode conhecer. O limite máximo ajuda a limitar o número total de conexões na rede, e consequentemente o número de mensagens trocadas, o que permite melhorar a eficiência e escalabilidade do mecanismo. O limite mínimo permite que nenhum participante fique isolado devido à queda da maioria de seus parceiros, já que, assim que o limite mínimo é atingido, ele consegue novos. Assim, um nó que poderia ficar isolado na versão anterior do código pode agora continuar a contribuir para o consenso.

A coleta de dados em relação ao número médio de blocos e transações por segundo é muito importante para analisar a escalabilidade do CPoS, já que um consenso que possui uma baixa taxa de aprovação para transações pode não ser viável em uma aplicação prática. Ao estabelecer uma comparação com o mecanismo Casper da criptomoeda Ethereum, que já é consolidada no mercado, poderemos ter uma visão da viabilidade do CPoS em cenários similares aos de uma blockchain amplamente utilizada ao redor do mundo.

Uma das características mais importantes do mecanismo de consenso de uma blockchain é a sua resistência contra a presença de nós desonestos. Ele deve impedir que os participantes desonestos influenciem o consenso de maneira ilegítima para benefício próprio e permitir um consenso em tempo apropriado mesmo em uma rede com uma rede com muitos atacantes. Por isso, o estudo realizado sobre o atraso médio de confirmação de blocos em função da porcentagem de nós desonestos é de grande importância para avaliar o nível de segurança do sistema.

CONCLUSÕES:

A partir dos trabalhos realizados, foi possível promover diversas melhorias no código do CPoS, tornando-o mais eficiente, robusto e estável. Além disso, com o estudo desenvolvido e as comparações realizadas, foi possível analisar vantagens e desvantagens de um mecanismo de

consenso PoS sem comitês de validação para blockchains públicas em relação à eficiência e ao nível de tolerância à presença de participantes desonestos.

BIBLIOGRAFIA

[1] I. Bashir, Mastering Blockchain. Packt Publishing Ltd., 1 ed., 2017.

[2] A. Kiayias, A. Russell, B. David, and R. Oliynykov, “Ouroboros: A provably secure proof-of-stake blockchain protocol,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 10401 LNCS, (Santa Barbara, CA, United States), pp. 357–388, Springer International Publishing, 2017.

[3] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, “Algorand: Scaling byzantine agreement for cryptocurrencies,” ArXiv e-prints, 2018.

[4] V. Buterin and V. Griffith, “Casper the friendly finality gadget,” ArXiv e-prints, 2017.

[5] J. Kwon, “TenderMint : Consensus without Mining.”, 2014. [Online]. https://tendermint.com/docs/tendermint.pdf (último acesso em 05/08/2024).

[6] Martins,D.F.G.(2021), “Um novo mecanismo de consenso probabilístico para blockchains públicas”. Dissertação de Mestrado, FEEC-Unicamp, 2021, [Online] https://repositorio.unicamp.br/Busca/Download?codigoArquivo=507683, (último acesso em 05/08/2024)

[7] Código fonte do Committeeless Proof-of-Stake (CPoS), https://github.com/regras/cpos_v2 (último acesso em 05/08/2024).