XXIX Congresso de Iniciação Científica UNICAMP 2021

Avaliação da eficiência e segurança de mecanismos de consenso probabilístico baseados em Proof-of-Stake para blockchains públicas

Palavras-chave: Blockchain, Proof-of-Stake, Mecanismo de consenso

Autores:
Felipe Benedet da Silva
Prof. Dr. Marco Aurélio Amaral Henriques

Resumo

A Blockchain é um tecnologia que ganhou popularidade devido à expansão de criptomoedas no mercado, se mostrando um recurso promissor para o futuro. De maneira geral, a blockchain é um sistema de registro de transações financeiras e informações sigilosas aplicado em redes distribuídas e, para manter a segurança dos registros, é necessário que seja estabelecido um protocolo que deve ser seguido por toda a rede garantindo que eventualmente exista um consenso entre os participantes da rede. Atualmente, o *Proof-of-Work* é o mecanismo de consenso mais popularmente utilizado; porém, ele possui restrições ligadas a eficiência e consumo de energia. Por essa razão, surgem novas propostas que buscam superar essas deficiências, como o *Proof-of-Stake*. Durante o período deste projeto, esses mecanismos foram estudados mantendo o foco em um mecanismo *Proof-of-Stake* proposto pelo nosso grupo de pesquisa cujo propósito é a obtenção do consenso sem a formação de comitês de validação, estrutura comum em outro mecanismos Proof-of-Stake e que diminuem sua eficiência. Além disso, foram propostos métodos para avaliação do novo mecanismo de consenso considerando seu funcionamento em uma rede real, onde existe a criação de transações que transitam por toda a rede e devem ser manipuladas durante a mineração dos nós, que realizam a criação de blocos preenchidos por transações tornando a execução do protocolo mais próxima de uma aplicação real.

1 Introdução

As Blockchains são sistemas distribuídos que buscam viabilizar, sem a necessidade de uma entidade centralizada regulamentadora, a realização de transações entre duas partes que não possuem necessariamente um vínculo de confiança entre si. Para isso, os nós disputam o direito de inserir várias transações em blocos, os quais são organizados em cadeia fortemente amarrados uns aos outros por funções criptográficas. Todos os nós da rede podem (e devem) avaliar os blocos propostos e entrar em um consenso sobre a validade das transações inseridas neles.

Cada blockchain estabelece um mecanismo de consenso que define para toda a rede as regras que devem ser seguidas ao avaliar os blocos propostos. De acordo com Bashir [1],

um mecanismo de consenso define um conjunto de regras que a maioria dos nós (usuários) devem seguir para que se atinja o acordo sobre um valor ou um estado do sistema. Em redes públicas, não há como diferenciar nós falhos de nós maliciosos, uma vez que são redes assíncronas [2]. Portanto, não há como controlar sua presença e esses nós podem desejar atrapalhar a ocorrência de um consenso sobre uma transação ou reverter uma transação já confirmada, de maneira que possam realizar novas transações com moedas já utilizadas. Nesses casos, é necessário que o protocolo estabelecido garanta que o consenso seja confiável mesmo em uma rede sem controle central. Neste sentido, o Proof-of-Work (PoW) é o mecanismo de consenso mais utilizado nas blockchains públicas; porém, este mecanismo exige dos nós mineradores a prova de seu trabalho para produção de blocos, resultando em um baixo desempenho e um grande consumo de energia no processo.

Alternativamente, o Proof-of-Stake (PoS ou Prova-de-Posse) propõe a validação da participação dos nós através de um *stake* controlado por ele, geralmente associado a uma quantidade de moedas na posse do nó, atingindo assim um melhor desempenho e menor consumo de energia. No trabalho de mestrado de Martins [3] foi apresentada uma nova proposta de mecanismo de consenso baseada em Proof-of-Stake, a qual não utiliza comitês de validação, uma vez que essas estruturas costumam trazer maior complexidade ao mecanismo de consenso. Entretanto, naquele trabalho foram feitos testes sob condições que podem não refletir totalmente os casos práticos em que o tamanho das mensagens trocadas entre os nós participantes pode trazer impactos ao desempenho do mecanismo.

Neste trabalho foram desenvolvidos métodos para modelar o funcionamento desse mecanismo em situações que submetem os nós a cargas mais pesadas de trabalho e mais próximas de uma rede com grandes demandas de processamento e comunicação.

2 Panorama atual

Dentre os mecanismos de consenso o Proof-of-Work (PoW) é o mais utilizado, estando presente no Bitcoin e na maioria das criptomoedas existentes. O PoW exige dos nós a realização de um grande esforço computacional para que um bloco seja proposto na rede o que, consequentemente, leva a uma baixa eficiência e a um grande custo computacional e energético. Outra limitação desse mecanismo está na sua baixa capacidade de descentralizar o consenso em torno de um grande número de participantes. Essa dificuldade está associada ao custo da mineração, ou seja, para que um nó tenha uma chance maior de produzir blocos e obter recompensas, ele precisa realizar um grande investimento em hardware especializado para essa atividade. Como poucos nós são capazes de realizar esses investimentos, o processo de produção de blocos torna-se centralizado em nós com maior disponibilidade financeira.

Uma vez que o PoW é o mecanismo mais utilizado, as limitações enfrentadas por ele representam as limitações de toda a tecnologia blockchain atual, visto isso, a implementação de novas propostas capazes de substituir esse mecanismo é fundamental para expandir o alcance dessa tecnologia. Assim surgem as propostas baseadas no PoS, sendo que as mais relevantes utilizam a formação de comitês que são responsáveis por decidir qual dos blocos propostos será de fato mantido permanentemente na blockchain. Esses mecanismos, limitam as ações do nó a fim de proporcionar um maior grau de sincronismo na rede, uma vez que, de acordo com Fischer et al. [2], é impossível alcançar um consenso determinístico em uma rede distribuída, que seja assíncrona e tenha nós maliciosos.

Além dos mecanismos PoS tradicionais, destaca-se um novo mecanismo de consenso baseado em PoS. Esse mecanismo está em desenvolvimento na FEEC pelo grupo de pesquisa ReGrAS [4]. Nesse mecanismo, os comitês de validação são substituídos por uma

confirmação probabilística dos novos blocos propostos na rede, tornando sua aplicação mais simples e menos dependente de um alto sincronismo na rede.

No processo de mineração, são definidas rodadas com tempo fixo (estabelecendo o sincronismo na rede) e os nós participam de sorteios baseados na quantidade de *stakes* controlados por eles dando-lhes a oportunidade de propor um bloco à rede. Quando um nó é sorteado, ele propõe um bloco para a rede de maneira que todos os participantes do consenso possam verificar a validade das transações no bloco e se o nó foi mesmo contemplado em sorteio na rodada. Nas rodadas seguintes, os nós recebem novas informações da cadeia que permitem uma avaliação probabilística dos blocos recebidos anteriormente, possibilitando suas confirmações na cadeia.

3 Novas avaliações de desempenho para o mecanismo PoS sem comitês

3.1 Motivação

Em uma aplicação real, os participantes do consenso devem realizar operações com as transações da rede, transmitir as transações recebidas, armazená-las em uma estrutura de dados local e, ao minerar novos blocos, os nós devem escolher as melhores para inserir nos blocos. Apesar de já terem sido realizados testes a respeito do funcionamento do mecanismo de consenso, o cenário de operação com transações reais ainda não foi avaliado integralmente. Para simular o funcionamento do mecanismo em uma rede com operações mais próximas das reais, foi elaborado um modelo capaz de replicar a criação das transações na rede, além de integrar as operações realizadas pelos nós mineradores com as transações, permitindo uma avaliação mais realista do mecanismo de consenso.

3.2 Transações

Em uma rede real, são implementados mecanismo de verificação do saldo disponível para moedas utilizadas em transações. Para isso, é necessário um controle rigoroso das moedas utilizadas realizando um encadeamento entre elas, como descrito em [5]. Porém, considerando o objetivo de determinar a eficiência do protocolo operando com transações individuais, não foram inseridos métodos de controle de saldo neste trabalho. Assim, as características consideradas relevantes para o modelo foram: o tamanho da transação, seu *hash* identificador e a taxa relativa àquela transação, de maneira a criar uma hierarquia de priorização das transações que devem ser inseridas na rede mais rapidamente com base na taxa paga pelo volume de bytes da transação.

Para a produção de transações, foi criada uma nova entidade na rede, a qual é independente da execução do protocolo e é responsável por simular a presença de *wallets* no sistema. Estas criam e distribuem transações na rede de maneira periódica utilizando parâmetros consistentes com as operações que ocorrem em redes reais. Essa entidade segue uma taxa de produção adaptável de forma que, a cada ciclo é selecionado um número preestabelecido n de nós que estão participando da rede para receberem as transações e compartilhá-las com seus *peers* até que todos os nós da rede recebam a transação, garantindo assim que os experimentos sejam independentes do ponto da rede nos quais as transações são inseridas.

O processo de criação de novas transações é ilustrado na Figura 1. O tempo de espera para iniciar um novo ciclo, a taxa da transação, o tamanho do payload e os nós

selecionados para enviar a transação são parâmetros que seguem distribuições aleatórias tornando cada transação única. Já o endereço de destino e de origem são parâmetros arbitrários incluídos somente para manter a estrutura da transação. Para identificar as transações de forma única, foi utilizado o tempo *UTC* de criação da transação e o ID do gerador da transação permitindo que, mesmo com vários geradores, cada transação possua um identificador único.

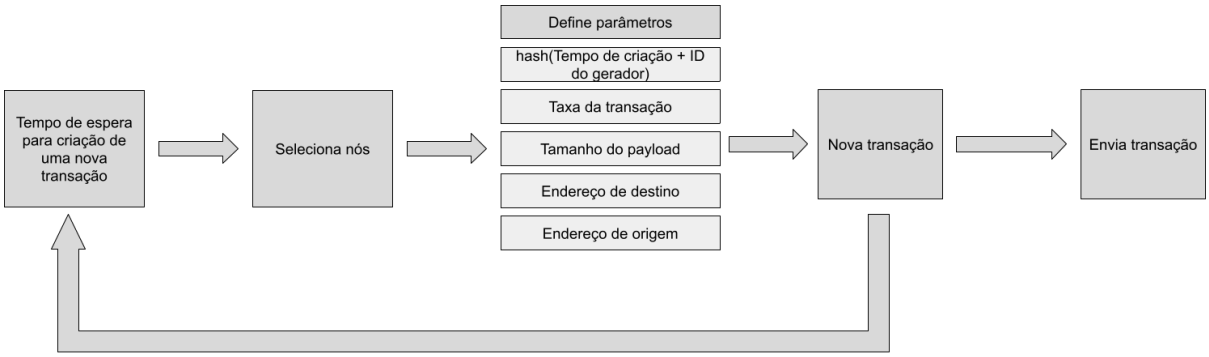

Figura 1: Diagrama de funcionamento do gerador de transações.

Uma vez resolvida a criação de transações, os nós precisam que protocolos específicos de recepção e administração sejam inseridos em suas atividades de mineração. Para isso, foi criado uma *mempool*, estrutura de dados auxiliar responsável por armazenar todas as transações recebidas em cada nó de maneira temporária. No modelo proposto, não existe diferenciação entre os nós e, portanto, todos possuem uma *mempool* própria que deve ser administrada adequadamente. Uma vez que essas estruturas armazenarão todas as transações recebidas, é a partir delas que são selecionadas as transações que serão inseridas nos blocos durante a mineração.

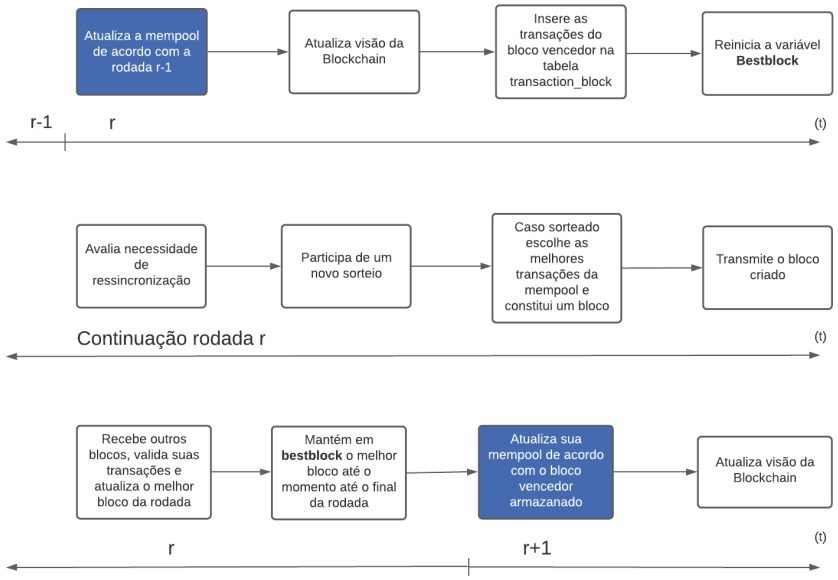

Figura 2: Diagrama de operações no nó durante uma rodada.

No mecanismo de consenso adotado, a seleção de blocos a cada rodada precisa seguir alguns requisitos para definir os blocos vencedores de cada rodada. Para ser vencedor,

o bloco deve possuir a menor rodada dentre os blocos propostos ou possuir uma rodada igual aos blocos de menor rodada e ter o menor hash de prova dentre eles. Para selecionar o melhor bloco, é usada uma variável *bestblock* de forma que, para cada bloco recebido durante uma rodada, o nó avalia se este é melhor do que os blocos anteriormente recebidos. Se as condições forem atendidas, o *bestblock* é atualizado armazenando as informações do novo bloco juntamente com suas transações e, dessa forma, ao final da rodada o *bestblock* conterá o bloco vencedor da rodada.

Uma vez definido o bloco vencedor da rodada, é necessário inseri-lo na *blockchain* e, para isso, é utilizada uma tabela *transactions_block*, responsável por armazenar todas as transações inseridas na cadeia e associá-las aos seus respectivos blocos. O procedimento seguido pelos nós é mostrado no diagrama da Figura 2, onde é possível notar que, em uma rodada r, o nó realiza as operações relativas ao bloco vencedor da rodada $r-1$, atualizando sua visão da *blockchain*. Em seguida são realizados os protocolos padrão do mecanismo de consenso, realizando a seleção do *bestblock* durante o decorrer da rodada. Por fim, no início da rodada $r+1$ o nó atualiza novamente sua visão da *blockchain* de acordo com os eventos da rodada r.

3.3 Testes e avaliações

O novo modelo de teste viabiliza avaliações mais precisas do novo mecanismo de consenso proposto em [3]. Para isso é necessária a utilização de uma rede distribuída geograficamente. Foram feitos testes preliminares, que mostraram um funcionamento adequado dos elementos da rede com as operações descritas. Porém, para testes em maior escala, surgiram limitações relacionadas ao banco de dados utilizado (SQLite3), visto que o sistema passou a demandar a manipulação de um maior volume de dados. Por isso, está sendo feita a troca do banco para MySQL a fim de viabilizar testes mais completos e realistas de desempenho do mecanismos de consenso em questão.

4 Conclusão

Neste trabalho foi possível propor novos esquemas de criação e processamento de transações que são mais realistas e permitem uma avaliação mais precisa do novo mecanismo de consenso baseado em PoS desenvolvido pelo grupo ReGrAS na FEEC.

Bibliografia

[1] I. Bashir, *Mastering Blockchain Second Edition*. Packt Publishing, 2 ed., 2018.

[2] M. J. Fischer, N. A. Lynch, and M. D. Paterson, "Impossibility of distributed consensus with one faulty process," *Journal of ACM*, vol. 32, no. 2, pp. 374–382, 1985.

[3] D. F. G. Martins, *Um novo mecanismo de consenso probabilístico para blockchains públicas*. Campinas, SP: Unicamp, 2021. Dissertação de Mestrado, FEEC.

[4] M. A. A. Martins, D. F. G; Henriques, "Avaliação da incidência de forks no algoritmo de consenso probabilistic proof-of-stake," in *XXXVIII SimpósioBrasileiro de Redes de Computadores e Sistemas Distribuídos - Blockchains Workshop*, (Rio de Janeiro - RJ), Sociedade Brasileira de Computação, dezembro 2020.

[5] A. M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*. O'Reilly, 2 ed., 2017.