XXXI Congresso de Iniciação Científica Unicamp 2023

Estudo sobre a relação custo-benefício de mecanismos de consenso Proof-of-Stake para blockchains públicas

Matheus Acauã Dias **Prof. Dr. Marco Aurélio Amaral Henriques**

[1]Faculdade de Engenharia Elétrica e de Computação (FEEC)
Universidade Estadual de Campinas (Unicamp) - Campinas - SP

Palavras-chave: blockchain, Proof-of-Stake, mecanismo de consenso

1. Introdução

Neste trabalho, fornecemos uma explicação sobre os mecanismos de consenso distribuído usados em blockchains, com foco nos algoritmos Proof of Work (PoW) e Proof of Stake (PoS). Damos uma visão geral do PoW (por ser o mais antigo e usado) e, em seguida, nos aprofundamos no PoS, abordando duas variações específicas: o Casper, que utiliza comitês de validação na rede Ethereum, e o Committeeless Proof of Stake (CPoS), que foi proposto por nosso grupo de pesquisa e não depende de comitês. Após essa explanação, analisamos o desempenho de cada mecanismo PoS, levando em consideração a vazão de cada um em termos de transações confirmadas por tempo. O objetivo é entender melhor a relação custo-benefício de cada mecanismo, identificar suas limitações e propor melhorias.

2. Mecanismos de Consenso

Um mecanismo de consenso em uma blockchain é um conjunto de regras que permite que os participantes concordem sobre o estado e a validade das transações armazenadas nos blocos [1]. Ele desempenha um papel fundamental na segurança, confiabilidade e integridade da blockchain, prevenindo fraudes. Existem diferentes mecanismos de consenso como, por exemplo, o Proof-of-Work (PoW) e o Proof-of-Stake (PoS), que são os mais utilizados atualmente para alcançar esse acordo.

2.1. Consenso Proof-of-Work

Proof-of-Work (PoW) é o mecanismo de consenso usado na primeira blockchain criada: a da criptomoeda Bitcoin. Os participantes, chamados de mineradores, competem para calcular funções de hash até que um valor menor que um determinado limite seja produzido [4]. Esse cálculo é chamado de ”prova de trabalho”e determina qual participante adicionará um novo bloco à cadeia existente e validará as transações. O PoW é valorizado por sua segurança e resistência a ataques, pois o invasor deve controlar a maior parte do poder computacional de uma extensa rede para criar uma cadeia paralela com transações irregulares. No entanto, o PoW também apresenta desvantagens, como alto consumo de energia e necessidade de hardware especializado para mineração em alta velocidade.

2.2. Consenso Proof-of-Stake

Proof-of-Stake (PoS) é uma alternativa ao PoW, com validação de blocos e transações baseadas na participação (financeira) dos nós na rede, em vez do poder computacional. Os nós que colocam mais stake (apostam mais alto) na rede têm mais chances de serem selecionados para criar blocos e receber recompensas, incentivando a participação e aumentando a segurança do sistema. É como se o stake fosse o número de bilhetes de loteria com os quais um participante está concorrendo a um sorteio. Em PoS só se faz um sorteio a cada certo intervalo de tempo (rodada) e, por isso, ele é mais eficiente em termos

de consumo de energia, não exigindo computação intensiva e nem hardware especial. A maioria dos mecanismos PoS garante a lisura do processo de validação de blocos por meio de comitês de validação, os quais necessitam gerenciamento. Para evitar problemas de corrupção e/ou conluio entre os membros do comitê, alguns protocolos PoS implementam mecanismos como seleção aleatória de membros, rotação de validadores no comitê, ou substituição de comitês de validação por métodos probabilísticos, como o caso do Committeeless Proof-of-Stake (CPoS).

2.2.1. Particularidades do Casper como mecanismo PoS

Em Casper, os blocos são produzidos por um conjunto de validadores selecionados de maneira aleatória, segundo um esquema de seleção proporcional ao stake depositado. Os checkpoints são blocos que definem uma *epoch* (ou época) e que estão posicionados em múltiplos predefinidos dentro da blockchain, como cada 100 blocos, na versão original[1] [2]. A finalização dos checkpoints é realizada pela obtenção de 2/3 dos votos emitidos pelos validadores, garantindo a confirmação de todos os blocos anteriores. Casper define "supermajority links": ocorrem quando mais de 2/3 dos validadores votam em um link que vai do checkpoint s ao checkpoint t, validando todos os blocos nesse intervalo. Um checkpoint t é considerado justificado se ele for o bloco gênesis ou se o checkpoint s for justificado e o link $s \rightarrow t$ for um supermajority link. Um checkpoint t é finalizado se for justificado e existir um supermajority link $t \rightarrow u$, onde u é o checkpoint sucessor direto de t, isto é, está 32 blocos adiante. O fato de Casper se basear em comitês de validação traz alguns problemas de gerenciamento de tais comitês, já que na prática eles são dinâmicos, permitindo que alguns tipos de ataques sejam possíveis, como revisões de longo prazo e falhas catastróficas (acidentais ou intencionais) [2].

2.2.2. Particularidades do CPoS como mecanismo PoS

A proposta do Committeeless Proof-of-Stake é eliminar a necessidade de um comitê de validação por meio de um consenso probabilístico [3] e, assim, tornar o consenso mais eficiente e seguro. Nesse mecanismo, os nós são sorteados de forma proporcional ao seu stake para produzir os blocos. Quando um nó recebe um bloco, ele verifica vários critérios para determinar sua aceitação ou rejeição. Primeiramente, verifica se o bloco foi criado dentro do intervalo de tolerância e se a rodada registrada no bloco é menor que a anterior. Se mais de um bloco for recebido satisfazendo esses critérios, o bloco aceito é aquele com o menor hash de prova, calculado com base em vários parâmetros. O protocolo garante uma confirmação em um cenário ideal onde todos os blocos são recebidos por toda a rede dentro do intervalo definido. No entanto, no mundo real com atrasos, falhas de transmissão e desonestidade, diferentes nós podem ter visões de blockchain divergentes.

O mecanismo realiza uma confirmação probabilística, onde o nó determina se sua visão atual da blockchain está sendo seguida por outros sem a necessidade de votação. A probabilidade de visões conflitantes relacionadas a um bloco é suficientemente baixa. O cálculo detalhado dessa probabilidade e o nível mínimo necessário para que um bloco seja confirmado são explicados na referência [3].

3. Desempenho Casper

O Casper é um mecanismo de consenso baseado em participação, onde a rapidez na finalização dos checkpoints e o tempo médio entre os blocos influenciam seu desempenho [2]. O tempo médio entre os blocos multiplicado pelo número de blocos em uma época determina o tempo necessário para justificar e finalizar o próximo checkpoint. Um tempo de rodada adequado é fundamental para manter a mesma visão da blockchain entre os validadores.

[1] Reduzido para 32 blocos segundo https://ethereum.org/en/glossary/#epoch.

A Tabela 1 contém dados atuais do desempenho da rede Ethereum, os quais foram levantados para se fazer uma estimativa do desempenho do CPoS em uma situação semelhante. De acordo com essa tabela[2] podemos observar dados médios da rede ethereum em diferentes datas. Os valores em questão são a vazão, em transações por segundo (Tx/s), o tamanho médio do bloco ($block_{size}$), em bytes, e o número médio de transações por bloco. A última linha da Tabela 1 representa a média aritmética de cada coluna e essa média foi utilizada na seção seguinte para os cálculos e estimativas do CPoS. Com base nesses dados médios, podemos obter o tamanho médio das transações: $Tx_{size} = 113.406/149,6 = 758,1$ bytes. Observa-se que o Casper tem um tempo médio entre blocos (chamado de block time) de 12 segs.

Tabela 1. Dados medidos da rede ethereum (Fonte: blockchair.com)

Data	Tx/s	$block_{size}(B)$	$Tx/block$
01/05/2023	13	102.487	155,0
01/06/2023	12	113.935	150,9
01/07/2023	12	123.797	142,9
Média	12,3	113.406	149,6

Outro parâmetro importante para o desempenho é o tempo de confirmação T_{conf} das transações em um bloco, que depende do tempo necessário para que esse bloco seja definitivamente aceito pela blockchain, isto é, finalizado. Não está sendo considerado o tempo que os nós validadores podem levar para chegar a um consenso em suas votações, mas apenas o tempo médio entre blocos.

Uma transação é confirmada em um tempo mínimo se várias condições favoráveis são satisfeitas. A primeira é que seja inserida em um bloco s que é um checkpoint. A segunda é que esse checkpoint s seja votado pelo comitê (nem todos são) e seja justificado. Finalmente, é preciso que o próximo checkpoint t (exatamente 32 blocos adiante) também seja justificado, o que torna o bloco s finalizado (confirmado) [2]. Assim, o tempo de confirmação mínimo $T_{conf,0}$ do bloco s e suas transações será o tempo de criação dos 32 blocos até t, o que resulta em $T_{conf,0} = 32 \cdot 12 = 384$ seg.

Em contraste, um segundo cenário ocorre quando uma transação é adicionada em um bloco x criado após um checkpoint s que já foi justificado. Nesse caso, o bloco x terá que esperar a criação de dois "supermajority links": um entre s e um futuro checkpoint t, justificando t, e outro entre t e u, que precisa ser o sucessor direto de t (exatos 32 blocos adiante), finalizando t e confirmando todos os blocos e transações entre s e t (inclusive x). Esse bloco x pode estar em uma faixa entre $s + 1$ e $s + 31$. Dessa forma, o tempo de espera dependeria da posição de x em relação a s: se $x = s + 1$ (ou $x = s + 31$), seria necessário aguardar a criação de 31 (ou 1) blocos até t e mais outros 32 blocos até u, resultando em $T_{conf,1} = 63 \cdot 12 = 756$ (ou $T_{conf,1} = 33 \cdot 12 = 396$) seg. Para fins de comparação, podemos tomar o caso médio, em que a transação é inserida em um bloco x equidistante de s e t. Nesse caso, $T_{conf,médio} = 48 \cdot 12 = 576$ seg.

Deve ser notado que o pior caso pode ser mais demorado, já que uma condição para a finalização de um checkpoint é que seja criado um "supermajority link"entre ele seu seu sucessor imediato (32 blocos adiante). Isso não é garantido que ocorra, já que Casper prevê a possibilidade de criação de "supermajority links"entre checkpoints que não são sucessores diretos uns dos outros [2]. Entretanto, a especificação atual do Casper[3] prevê um mecanismo para penalizar o stake dos nós que não estão colaborando se não ocorrer uma finalização por mais que quatro épocas seguidas. Mesmo assim, pode ser necessário um número não conhecido de épocas até que o sistema volte a finalizar checkpoints novamente. Isso vai depender do volume de stake envolvido. Aparentemente esse caso é pouco provável e não chegou a ocorrer na prática até hoje, o que nos leva a considerar que o tempo médio de confirmação é o de 576 seg. calculado acima.

[2]Fonte: https://blockchair.com

[3]https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/#finality

4. Desempenho Committeeless Proof-of-Stake

A vazão do CPoS é dada por $Tx/s = block_{size}/(Tx_{size} \times T) \times Bc/round$ transações por segundo, onde $block_{size}$ e Tx_{size} têm o mesmo significado já definido, T é o periodo da rodada e $Bc/round$ é o número de blocos confirmados por rodada [3]. O valor de $Bc/round$ depende de dois parâmetros básicos no CPoS: τ e ϵ.

O parâmetro τ é definido como $\tau = p \times W$, isto é, o produto da probabilidade p de um sorteio ser bem-sucedido pelo número total W de sorteios dentro de uma rodada e representa o número esperado de sorteios bem-sucedidos dentro de uma rodada. Um sorteio é bem-sucedido se ele produz um valor aceitável dentro dos parâmetros definidos pelo CPoS [3].

O parâmetro ϵ é chamado de limiar de segurança e é estabelecido como o valor máximo que pode ser alcançado pela probabilidade de haver mais sorteios bem-sucedidos em uma rodada que o valor τ. Ao estabelecer esse limite, temos uma visão clara sobre a probabilidade de blocos divergentes serem aceitos e criarem forks na rede. Ao ajustar esse limite de segurança, podemos aumentar ou diminuir o desempenho da nossa rede. Dessa forma, podemos adaptar a tolerância a forks indesejados, garantindo a estabilidade e a segurança do sistema.

Esses parâmetros atuam diretamente sobre o valor do $Bc/round$ e foram variados em diferentes execuções do CPoS com o fim de obter melhores taxas de transações por segundo [3]. Na Tabela 2 são apresentados alguns resultados dessas execuções do CPoS em um ambiente formado por um conjunto de 25 hosts, distribuídos geograficamente. Cada host funcionou como um nó da rede e o período de cada rodada foi $T = 20s$. O tamanho do bloco neste caso particular foi de 1MB e o tamanho das transações foi de 400 bytes, o que resultou em uma média de 2500 transações por bloco. No CPoS, os parâmetros ϵ, τ e T determinam o tempo de confirmação de um bloco (T_{conf}), o qual é expresso em segundos e apresentado na última coluna da Tabela 2.

Tabela 2. Diferentes vazões e taxas de confirmação para combinações de τ e ϵ (Fonte: Tabela 7.2 em [3])

τ	ϵ	T	Tx/s	$Bc/round$	T_{conf}
25	10^{-4}	20	90,00	0,72	27,78
25	10^{-3}	20	99,58	0,80	25,00
25	10^{-2}	20	114,43	0,92	21,74
19	10^{-2}	20	113,11	0,90	22,22
16	10^{-2}	20	97,56	0,78	25,64

5. Resultados e Análise

Para melhor entender as relações custo-benefício em questão, focaremos, neste momento, na escalabilidade do mecanismo por meio do parâmetro de vazão. Os outros dois parâmetros importantes, segurança e descentralização, serão abordados em trabalhos futuros, após a conclusão da refatoração do CPoS, que está atualmente em andamento.

Com os parâmetros usados na Tab. 2, escolhidos de forma a otimizar o funcionamento do CPoS, nota-se que a vazão do mesmo varia entre 90 e 114,43 transações por segundo. Nesse cenário, a taxa de blocos confirmados por rodada varia de 0,72 a 0,92, não atingindo o máximo teórico de 1, devido ao fato de que em algumas rodadas pode não ocorrer sorteios bem-sucedidos. No caso em que se atinja esse patamar máximo, o número de transações por segundo alcança a marca de 125. Tais valores de vazão são cerca de 10 vezes superiores aos do Casper e isso se deve ao fato de se ter considerado um bloco de 1MB para o CPoS, que é um valor 8,8 vezes maior que o bloco do Casper. Essa diferença praticamente já justifica a diferença na vazão, ficando uma parte a cargo da diferença entre tempos de rodada, 20 seg.

no CPoS contra cerca de 12 seg. no Casper, e outra parte a cargo da diferença de tamanho médio de transações (400 vs. 758,1 B).

Podemos fazer um exercício de transposição do CPoS para o cenário do Casper, adotando rodada de 12 segs. e os tamanhos médios de bloco e de transações obtidos da Tab. 1. Consideremos inicialmente o caso ideal de um bloco confirmado por rodada ($Bc/round = 1$): $Tx/s = 113.406/(758,1 \times 12) \times 1 = 12,5$. Nesse caso, temos exatamente um décimo da vazão original do CPoS, o qual é um pouco superior à vazão média do Casper (12,3). Entretanto, se aplicarmos os valores reais de $Bc/round$ variando entre 0,72 e 0,92, temos que a vazão do CPoS em condições similares ao Casper varia na faixa de 9,0 a 11,5, valores um pouco abaixo da média deste último.

Uma possibilidade para alcançar um desempenho semelhante ou superior ao do Casper seria aumentando o tamanho do bloco e/ou diminuindo o periodo de rodada T. Deve ser observado que o tamanho médio das transações depende dos clientes e está fora do controle dos nós que mantêm a blockchain. Deve ser adotado o pior caso (tamanho máximo de transações permitido). A redução da rodada tem seus limites, como mostrado na referência [3], pois a confirmação probabilística depende que grande parte dos nós recebam todos os blocos produzidos e, para tanto, é necessário que o valor de T seja suficiente para que os blocos trafeguem pela rede.

Comparando os tempos de confirmação de um bloco, observamos que o protocolo Casper possui uma latência média de 576 seg. Uma opção para reduzir esse tempo de latência, sem modificar o protocolo, seria diminuir o parâmetro $blocktime$, por exemplo, o que não é recomendável, pois isso torna o protocolo menos estável e menos seguro. Por outro lado, o protocolo CPoS, conforme apresentado na tabela 2, possui uma latência entre 21,74 e 27,78 segs., sendo possível ajustá-la por meio de vários parâmetros, como ϵ, τ e T. Nota-se, portanto, que além do tempo de confirmação de um bloco do CPoS poder ser bem mais curto, este também pode ser ajustado por meio da regulagem dos parâmetros internos em busca de um ponto de operação mais otimizado.

6. Conclusões e trabalhos futuros

Com base nos dados de desempenho da rede Ethereum, foi observado que o Casper apresenta uma vazão média de transações por segundo cerca de dez vezes inferior ao CPoS, quando este último está trabalhando com parâmetros otimizados. No entanto, ao se adotar no CPoS parâmetros similares aos do Casper, vemos que a vazão do primeiro fica ligeiramente inferior á do segundo. Quanto ao tempo de confirmação de um bloco observamos que o CPoS possuí uma latencia de confirmação bem menor e mais flexível que a do Casper. Foram discutidas maneiras de se melhorar o desempenho do CPoS, mas as mesmas precisam ser confirmas em novos experimentos feitos em condições mais reais de operação da rede. A refatoração do código do CPoS, que está em andamento para corrigir alguns problemas operacionais e torná-lo mais eficiente permitirá a realização de testes e comparações mais sofisticados e mais próximos do contexto que temos na prática hoje para o Casper, principal mecanimo PoS em uso. Além disso, para uma análise mais completa, é necessário considerar outros aspectos, como segurança e descentralização e escalabilidade. Testes em diferentes cenários e casos de uso deverão ser realizados em trabalhos futuros para obter uma visão mais completa do custo-benefício do CPoS em comparação, não só com o Casper, como também com outros mecanismos que utilizam de comites de validação.

Referências

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

[2] V. Buterin and V. Griffith. Casper the friendly finality gadget. 2017. ArXiv e-prints. https://arxiv.org/abs/1710.09437. Acesso em: 26 jul. 2023. .

[3] Diego F. G. Martins. Um novo mecanismo de consenso probabilístico para blockchains públicas. 2021. Unicamp - FEEC. Disponível em: https://hdl.handle.net/20.500.12733/1641758. Acesso em: 26 jul. 2023.

[4] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2009. Whitepaper. Acesso em: 26 jul. 2023.