AVALIAÇÃO DE SEGURANÇA DE MECANISMOS DE CONSENSO PROOF-OF-STAKE COM E SEM COMITÊS DE VALIDAÇÃO

Palavras-Chave: blockchain, mecanismo de consenso, segurança

Autores(as):

VINÍCIUS DE OLIVEIRA PEIXOTO RODRIGUES - FEEC - UNICAMP

Prof(ª). Dr(ª). MARCO AURÉLIO AMARAL HENRIQUES - FEEC - UNICAMP

INTRODUÇÃO:

Blockchains são um tema que tem ganhado grande relevância ao longo da última década. Podendo ser definidas como bancos de dados distribuídos, compartilhados e criptografados, elas possuem a propriedade especial de serem imutáveis e irreversíveis: todos os dados (guardados dentro de uma unidade mínima de informação denominada *bloco*) são matematicamente atrelados a todas as entradas anteriores na *blockchain*, tornando impossível alterar quaisquer registros que já tenham sido inseridos na cadeia. (TRAUTMAN e MOLESKY, 2019).

Além das garantias de integridade, há também a vantagem da descentralização: *blockchains* são construídas sobre redes *peer-to-peer*, onde cada nó possui uma cópia local da *blockchain* (seja parcial ou em sua totalidade); essa redundância serve como uma garantia de segurança, assim como de tolerância a falhas (GAO et. al., 2018). Além disso, *blockchains* são completamente abertas e transparentes, permitindo a qualquer nó na rede ler e (potencialmente) escrever novos blocos.

Contudo, a descentralização inerente às redes *peer-to-peer* faz com que surjam diversos desafios técnicos no que diz respeito à confiabilidade das *blockchains*. O primeiro deles é a necessidade de algum tipo de esquema de sincronização que faça com que os nós escrevam novos blocos de maneira organizada; isto é, somente um nó por vez pode adicionar um bloco e todos os outros nós devem concordar a respeito da validade do bloco e de seu conteúdo, de modo a manter consistência entre as visões locais que os nós têm da cadeia. O segundo desafio é a necessidade de *tolerância bizantina*: a rede deve ser capaz de seguir funcionando independentemente da presença de nós defeituosos ou desonestos (LAMPORT et. al., 1982).

Para solucionar esses desafios, diversos protocolos, denominados *mecanismos de consenso*, foram desenvolvidos. Existem duas grandes classes de mecanismos de consenso: o *proof-of-work* (PoW) e o *proof-of-stake* (PoS). No PoW, ganha o direito de criar um bloco o nó que resolver primeiro um problema computacionalmente custoso; isso serve tanto para desencorajar comportamento

desonesto da parte dos nós quanto para garantir que só um deles vai criar um novo bloco. Já no PoS é escolhido periodicamente e de forma aleatória um *comitê de validação*, composto por nós (*validadores*) que investiram uma certa quantidade de moeda corrente (*stake*) para se tornarem validadores. O comitê realiza então um processo de sorteio e eleição que vai selecionar um novo bloco para ser adicionado à *blockchain*. O comportamento desonesto é desencorajado pelo fato de que os nós podem ser punidos por meio do confisco do *stake* investido para entrar no comitê.

Apesar de o PoS ser a alternativa mais promissora para o futuro das *blockchains*, em especial devido ao seu impacto energético ser ordens de magnitude menos elevado que o do PoW, os comitês de validação introduzem complexidades de implementação adicionais e aumentam a superfície de ataque da rede. Desse modo, foi proposto um mecanismo denominado *committeeless proof-of-stake* (CPoS) que elimina a necessidade de um comitê de validação por meio de um esquema de sorteios determinísticos que podem ser verificados de forma autônoma e independente pelos nós (MARTINS, 2021).

O objetivo deste projeto de iniciação científica foi avaliar detalhadamente e sugerir melhorias para a segurança do mecanismo CPoS, em especial quando comparado às implementações tradicionais de PoS baseadas em comitês.

METODOLOGIA:

Durante a primeira etapa do projeto de pesquisa foi realizado um estudo teórico extensivo sobre o panorama geral das tecnologias de *blockchain.* Foram estudados diversos conceitos em criptografia (funções de hash, criptografia assimétrica, esquemas de assinatura digital) e as suas aplicações em mecanismos de consenso. Foi feito também um trabalho de pesquisa sobre as principais implementações do PoS na atualidade (Algorand, Ouroboros, Casper, entre outros).

Na segunda etapa, foi realizado um cuidadoso escrutínio do funcionamento interno do protocolo CPoS, abordando os aspectos teóricos do algoritmo de sorteio criptográfico e do mecanismo de confirmação de blocos. Os trabalhos foram discutidos em seminários realizados periodicamente junto a outros membros do grupo de pesquisa ReGrAS-FEEC (*Research Group on Applied Security*) de modo a identificar vulnerabilidades e pontos a serem melhorados no algoritmo de consenso.

Já na etapa final, os esforços foram concentrados em realizar testes práticos com o CPoS. Uma prova de conceito já havia sido implementada em trabalhos anteriores sobre o mecanismo de consenso, mas foram encontrados diversos problemas que tornaram extremamente difícil a reutilização dela para realização de testes. Dentre eles estava o fato de que o código estava implementado em Python 2.7 (uma versão da linguagem tornada obsoleta já há vários anos), fazendo uso de uma série de dependências desatualizadas que já não forneciam mais suporte para versões tão antigas da linguagem Python. Além disso, havia diversos outros problemas (relacionados, por

exemplo, à dificuldade de configuração de topologia da rede *peer-to-peer* do CPoS, assim como ao armazenamento persistente de dados usando um banco de dados relacional).

Tendo em vista as dificuldades encontradas e o risco de segurança trazido por elas, assim como a preocupação com a qualidade do código (como uma forma de reduzir a chance de erros inesperados que comprometam a robustez do CPoS), investiu-se uma quantidade considerável de esforço em reescrever todas as camadas do mecanismo de consenso na versão mais moderna da linguagem Python, fazendo correções e melhorias em relação ao código antigo ao longo do caminho. Também houve a preocupação em montar uma infraestrutura sólida fazendo uso da tecnologia *Docker* para a criação de ambientes de *containers*, tornando estável e automatizado o processo de compilação, empacotamento e *deploy* do código novo.

RESULTADOS E DISCUSSÃO:

Como resultado dos esforços de refatoração e revisão do protocolo CPoS, foi escrita uma nova implementação *open-source* do mecanismo de consenso.

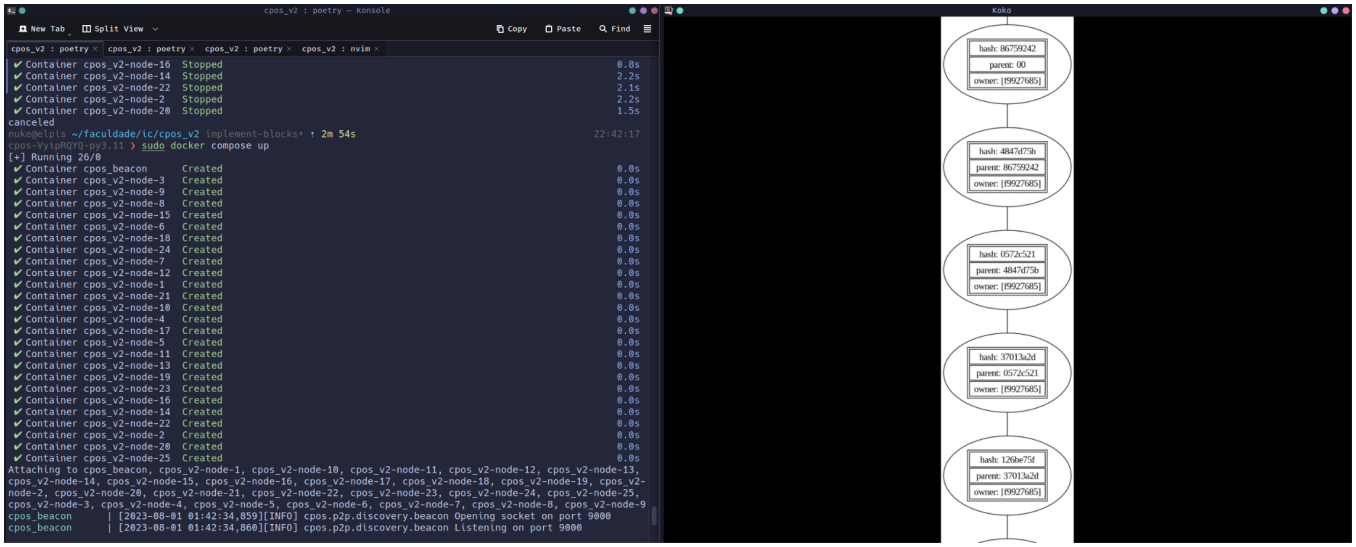

Figura 1: Nova implementação do mecanismo CPoS em funcionamento, demonstrando a evolução de uma *blockchain* com 25 nós criados usando *Docker containers*. Código disponível em https://github.com/regras/cpos_v2/tree/implement-blocks.

A versão refatorada do mecanismo conta com diversas melhorias, como a implementação de uma camada *peer-to-peer* robusta (com suporte a descoberta dinâmica de *peers*) e a escrita de uma bateria de testes unitários de modo a garantir a segurança e robustez do comportamento da CPoS (evitando regressões ao fazer mudanças de implementação em relação ao código antigo). Além disso, a infraestrutura *Docker* montada permite executar testes de forma automatizada tanto em um host local quanto em hosts distribuídos. Os esforços se mostraram frutíferos, visto que, além de possibilitar a execução de testes com maior facilidade e estabilidade, permitiram a descoberta de alguns problemas de segurança do protocolo CPoS.

O primeiro ponto de destaque é que, durante a reimplementação do mecanismo de sorteio, notou-se que na especificação antiga do mecanismo CPoS havia uma vulnerabilidade crítica relacionada ao cálculo de hashes de provas de blocos (MARTINS, 2021) que punha em risco a garantia de que novos blocos a serem inseridos são matematicamente atrelados a todos os blocos anteriores. Essa vulnerabilidade foi solucionada na nova versão do CPoS.

O segundo ponto de destaque, para o qual ainda não foi encontrada uma solução satisfatória, diz respeito ao mecanismo de confirmação de blocos. Durante a execução de testes, foi verificado que o mecanismo de confirmação por vezes pode causar um atraso muito grande no tempo médio de confirmação de blocos quando a rede se recupera de um período de instabilidade. Por exemplo, ao se criar uma nova blockchain vazia, vários nós geram simultaneamente blocos que se propagam pela rede. Ao final da rodada inicial, somente um bloco será escolhido para ser inserido, mas o algoritmo de confirmação de blocos (que funciona essencialmente como um *feedback loop*) se mantém relutante em confirmá-lo visto que a rede passou por um período de grande instabilidade (com muitos *forks* acontecendo simultaneamente), necessitando de várias rodadas para conseguir confirmar novos blocos com um grau de certeza aceitável.

Por fim, um outro ponto relevante foi o estudo de um ataque que toma vantagem da estratégia conservadora do mecanismo de confirmação de blocos para diminuir a performance da blockchain. O ataque é possibilitado quando um agente malicioso adquire o controle de uma porção considerável do *stake* total da rede e passa a premeditadamente sabotar o funcionamento do mecanismo ao, na ocasião em que é sorteado para gerar blocos, se recusar a divulgar blocos. Isso impacta negativamente o mecanismo de confirmação que, por constatar que estão divulgados menos blocos que o esperado, passa a suspeitar da existência de forks na rede e reluta em confirmar novos blocos. Esse problema havia sido discutido em trabalhos anteriores sobre o CPoS e também afeta a nova versão do protocolo.

CONCLUSÕES E TRABALHOS FUTUROS:

Os resultados obtidos indicam que o protocolo CPoS, e em particular o seu mecanismo de confirmação de blocos, no estado atual, possui algumas vulnerabilidades que o tornam suscetível a ataques maliciosos. Contudo, como foi discutido em (MARTINS, 2021), é possível melhorar a resiliência do mecanismo de confirmação ao fazer com que mais blocos circulem pela rede, mitigando assim o impacto das vulnerabilidades encontradas. Isso traz, contudo, um impacto não trivial no aumento de volume de dados em circulação na rede *peer-to-peer,* podendo causar estresse na rede como um todo. É necessário, portanto, realizar mais testes envolvendo a calibração cuidadosa dos parâmetros da rede (em especial o número de blocos gerados por rodada) para se encontrar um balanço entre a resiliência da confirmação de blocos e o volume de tráfego na rede.

Acreditamos que, solucionados esses problemas, o mecanismo CPoS tem um grande potencial competitivo frente a outras implementações do PoS baseado em comitês, devido à sua relativa simplicidade e autonomia, dispensando a formação de comitês que exigem inevitavelmente uma interação de alta complexidade e sincronismo entre os validadores.

BIBLIOGRAFIA

TRAUTMAN, L. J.; MOLESKY, M. J. A Primer for Blockchain. **UKMC Law Review**, v. 88, 2019

Gao, W. et. al. A Survey of Blockchain: Techniques, Applications and Challenges. **27th International Conference on Computer and Communication Networks (ICCCN)**, p. 1-11, 2018

LAMPORT et. al. The Byzantine Generals Problem. **ACM Transactions on Programming Languages and Systems**, v. 4, 1982

MARTINS, D. F. G. **Um novo mecanismo de consenso probabilístico para blockchains públicas**. 2021