Análise de redes blockchain baseadas em Hyperledger do tipo privada/consorciada quanto a ataques DoS internos

João Henrique Faes Battisti[1], **Charles Christian Miers**[1]

[1]Programa de Pós-Graduação em Computação Aplicada (PPGCA)
Universidade do Estado de Santa Catarina (UDESC)

joao.battisti@edu.udesc.br, charles.miers@udesc.br

Resumo. *O blockchain surge para solucionar problemas de segurança em sistemas distribuídos através da aplicação de diversas tecnologias. Este artigo tem como objetivo apresentar uma proposta de análise de sobrevivência de serviços blockchains privados/consorciados em Hyperledger Fabric aplicadas aos mecanismos de consenso PBFT e PoA submetidas a ataques DoS internos.*

1. Contexto & Motivação

A aplicação de máquinas virtuais (MVs) é bastante diversificada, possibilitando a hospedagem de aplicações tradicionais e aplicações distribuídas mais complexas. Serviços blockchain são formados por redes *Peer-to-Peer* (P2P), criptografia, algoritmos e um mecanismo de consenso [Lin and Liao 2017]. Contudo, a descentralização requer garantias de funcionamento para que a rede blockchain opere corretamente, tornando os mecanismos de consenso uma das áreas críticas de uma solução blockchain. Entre os mecanismos de consenso, para modelos de blockchain privado e consorciado, destacam-se *Practical Byzantine Fault Tolerance* (pBFT) e *Proof of Authority* (PoA).

Uma prática empregada por companhias e instituições que adotam soluções baseadas em blockchain privado ou consorciado é a criação de seus nós de blockchain usando MVs dentro de suas nuvens privadas. Entretanto, a segurança de serviços hospedados dentro de uma nuvem *Infrastructure as a Service* (IaaS) pode ser um problema quando os nós da blockchain possuem acesso dos usuários destas organizações. Um usuário malicioso pode causar um ataque *Denial-of-Service* (DoS) acidentalmente ou maliciosamente.

As aplicações blockchain, em grande maioria, possuem os mesmos objetivos de busca por melhor eficiência. Entretanto, é crescente a preocupação em questões relacionadas ao blockchain, questões como escalabilidade, consumo energético, alto custo computacional, *etc*. Outra questão é a relacionada ao ambiente em que os nós do blockchain são criados, neste quesito destaca-se as nuvens computacionais. Quanto às configurações recomendadas dos *flavors* para MVs em modelos privado e consorciado variando de acordo com a plataforma aplicada. A plataforma Hyperledger Fabric possui recomendações em que cada MV possua 2 núcleos de vCPU, 4GB RAM e está disponível para diversos sistemas operacionais [The Linux Foundation 2018].

Uma questão que surge refere-se às configurações adequadas do *flavor* da instância. Outra questão é a quantidade de transações que são necessárias para a operacionalização da tecnologia. Com as configurações mínimas do *flavor* exigidas pelas plataformas, percebe-se que há uma considerável possibilidade de ataques de DoS simples afetarem o correto funcionamento da aplicação blockchain.

2. Proposta

A configuração do *flavor* de uma MV representa a quantidade de recursos(memória, vCPUs e rede) disponibilizados para utilização do nó da blockchain. Estes recursos relacionam-se a quantidade de transações que a instância consegue realizar, mas estes valores também variam de acordo com o mecanismo de consenso que é aplicado. Quanto as configurações de um *flavor* e a quantidade de transações, estas podem ser suficientes para atender as demandas que são necessárias para operacionalizar as aplicações. Contudo, podem ser fáceis de serem afetas através de ataques como o DoS.

A proposta deste trabalho é a realização de um experimento com objetivo geral de realizar uma análise de desempenho e segurança de redes blockchain privadas/consorciadas baseadas em Hyperledger Fabric, quanto a ataques DoS internos. Quanto ao objetivo específico, é analisar a quantidade de transações que uma instância consegue realizar sem prejudicar o serviço, a imutabilidade, procedência dos dados e estabelecer uma relação entre *flavor* da instância e tipo de ataque DoS. A escolha pelo modelo privado/consorciado está relacionado às nuvens computacionais, pois os principais responsáveis pela violação de dados nestes ambientes são funcionários internos. Quanto a aplicação do ataque DoS é que ataques relacionados a exploração de vulnerabilidades de recursos possuem impactos relacionados ao desempenho, ao nó e a funcionalidade da rede, podendo estes problemas não afetarem somente o nó, mas todo sistema em si [Rot and Blaicke 2019].

3. Considerações & Trabalhos futuros

O desenvolvimento desta análise é baseado em trabalho anterior [Miers et al. 2019], relacionado às questões de segurança e mecanismos de consenso em plataformas Multichain e Ethereum. A pesquisa atual está com o ambiente de experimentação já implementado e os experimentos em execução com Hyperledger Fabric. Os resultados iniciais revelaram que apenas um computador executando um DoS simples é suficiente para comprometer um nó blockchain operando em uma MV com *flavor* padrão.

Agradecimentos: Os autores agradecem o apoio do LabP2D/UDESC e a FAPESC.

Referências

Lin, I.-C. and Liao, T.-C. (2017). Survey of blockchain security issues and challenges. International Journal of Network Secutiry. http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5-p653-659.pdf.

Miers, C., Koslovski, G., Pillon, M. A., Jr, M. S., Carvalho, T., Rodrigues, B., and Battisti, J. (2019). Análise dos métodos para consenso distribuído aplicados à tecnologia blockchain. In *SBSeg 2019 - Minicursos*, chapter 3, pages 1–49. USP - São Paulo.

Rot, A. and Blaicke, B. (2019). Blockchain's future role in cybersecurity. analysis of defensive and offensive potential leveraging blockchain-based platforms. In *2019 9th International Conference on Advanced Computer Information Technologies (ACIT)*.

The Linux Foundation (2018). An introduction to hyperledger. https://www.hyperledger.org/wp-content/uploads/2018/07/HL_Whitepaper_IntroductiontoHyperledger.pdf.