Análise dos impactos de ataques DoS em Blockchain Hyperledger hospedadas em máquinas virtuais

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

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

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

Resumo. *As soluções que utilizam a tecnologia blockchain estão ganhando cada vez mais suporte das instituições e de desenvolvedores de sistemas. Este artigo tem como objetivo apresentar uma proposta de análise de sobrevivência de serviços blockchains do Hyperledger Fabric hospedados em máquinas virtuais (MVs) submetidos à ataques Denial-of-Service (DoS) internos.*

1. Contexto & Motivação

São diversas as aplicações suportadas por MVs, desde aplicações tradicionais como um servidor web até aplicações mais complexas como sistemas distribuídos com serviços baseados em redes *Peer-to-Peer* (P2P). Neste contexto, a tecnologia blockchain é formada por um grupo de tecnologias, como redes P2Ps, criptografia, algoritmos e mecanismo de consenso [Lin and Liao 2017]. Contudo, a descentralização deste sistema distribuído exige garantias para o seu correto funcionamento, tornando o mecanismo de consenso um dos aspectos críticos desta solução. Entre os algoritmos existes para modelos privados e consorciados destacam-se o RAFT, *Practical Byzantine Fault Tolerance* (pBFT) e *Proof of Authority* (PoA).

A Figura 1 ilustra uma prática empregada pelas instituições que adotam soluções blockchain, que é a criação de seus nós de blockchain a partir de MVs, em suas nuvens computacionais. Entretanto, a Figura 2 ilustra uma questão de segurança existente e preocupante em nuvens computacionais *Infrastructure as a Service* (IaaS) que usuários internos possuem acesso aos nós da blockchain. A Figura 2 também ilustra a ocorrência de um ataque DoS que pode ocorrer de forma maliciosa ou não maliciosa.

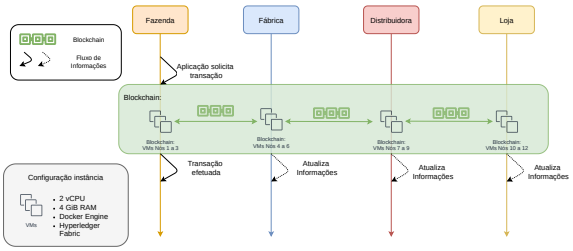

Figura 1. Cadeia de Suprimentos

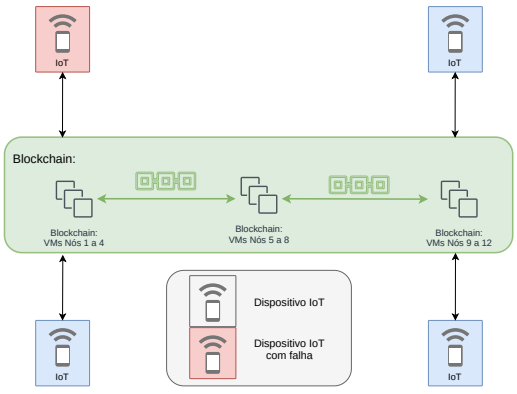

Figura 2. Blockchain com IoT

De maneira geral, os estudos relacionados ao blockchain, possuem o mesmo objetivo de busca por melhor eficiência e desempenho. Contudo, é crescente a preocupação com questões relacionadas à segurança, escalabilidade, consumo de recursos e também relação ao ambiente em que as aplicações são inseridas, em destaque as nuvens computacionais. Quanto as configurações que são recomendadas para o *flavors* das MVs, variam de acordo com a plataforma utilizada. A plataforma Hyperledger em ambientes de produção, possui como recomendação instâncias com 2 vCPUs e 4 GB RAM [The Linux Foundation 2018]. Assim, surgem questões como: Qual é a configuração adequada para a instância, a quantidade de transações necessárias para operacionalizar a aplicação blockchain? Quais as métricas e critérios para detecção de um problema na blockchain?

2. Proposta

Os recursos são disponibilizados às MVs em termos de vCPUs, memória e tráfego de rede. No caso de um nó de uma blockchain os recursos representam a quantidade de transações e tráfego que uma instância pode realizar, variando de acordo com o mecanismo de consenso aplicado. Entretanto, estes recursos disponíveis podem ser suficientes para operacionalizar todo o processo necessário da blockchain, mas podem ser facilmente afetados a partir de um ataque DoS. Este trabalho possui como objetivo realizar uma análise dos impactos de ataques DoS em uma blockchain privada ou consorciada, que estão hospedadas em MVs. De modo mais específico, este trabalho pretende analisar a quantidade de transações por minuto que uma instância consegue realizar sem prejudicar o serviço, analisar a imutabilidade e integridade destas transações e estabelecer uma relação entre o *flavor* da instância e a intensidade do ataque DoS sobre os recursos que estão sendo monitorados. Em relação ao ataque DoS são aplicados ataques de exploração de vulnerabilidades em instâncias, principalmente relacionadas aos protocolos de comunicação e também ataques de inundação na rede blockchain.

3. Considerações & Trabalhos futuros

A análise realizada neste trabalho, possui como base um trabalho anterior [Miers et al. 2019], este relacionado à questões de mecanismos de consenso nas plataformas Multichain e Ethereum. Este trabalho encontra-se atualmente com os ambientes de experimentação implementados e os experimentos do Cenário I em execução. Quanto ao resultados iniciais da pesquisa, revelam que um agente malicioso que executa um simples ataque DoS é o suficiente para comprometer um nó da blockchain e causar impactos negativos na rede blockchain, que operam 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.

The Linux Foundation (2018). An introduction to hyperledger.