Análise de segurança e desempenho de redes blockchains privadas/consorciadas quanto aos 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. *Soluções que utilizam a tecnologia blockchain estão ganhando cada vez mais suporte dos desenvolvedores de sistemas. As instituições tem integrado redes blockchain em seus sistemas, e uma maneira usual de incluir nós de blockchain é através de máquinas virtuais (MVs). Este trabalho possui como objetivo de realizar uma análise de segurança e desempenho para verificar o comportamento das MVs perante à ataques Denial-of-Service (DoS), uma vez que o flavor destas instâncias normalmente possui poucos recursos computacionais.*

1. Contexto & Motivação

Aplicações de MVs são muito diversas, podendo hospedar aplicações tradicionais como servidores web e também mecanismos distribuídos mais complexos como serviços baseados em *Peer-to-Peer* (P2P). Neste contexto, serviços blockchain são formados por redes P2P, criptografia, algoritmos e um mecanismo de consenso [Lin and Liao 2017]. Entretanto, a descentralização requer garantias funcionais para que uma rede blockchain opere corretamente, tornando o mecanismo de consenso um dos aspectos críticos de uma solução baseada na tecnologia blockchain. Dentre os mecanismos de consenso, para modelos blockchains privados e consorciados destacam-se *Practical Byzantine Fault Tolerance* (pBFT), *Proof of Stake* (PoS) e *Proof of Authority* (PoA). Comumente, instituições que tem investido na tecnologia no modelo privado ou consorciado, tem empregado como prática a criação de seus nós de blockchain utilizando MVs em nuvens computacionais, sejam estas públicas ou privadas. A Figura 1 ilustra o fluxo de uma cadeia de suprimento que faz o uso de MVs para o desenvolvimento de uma aplicação blockchain.

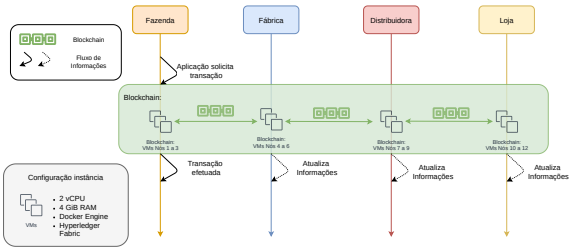

Figura 1. Cadeia de Suprimentos

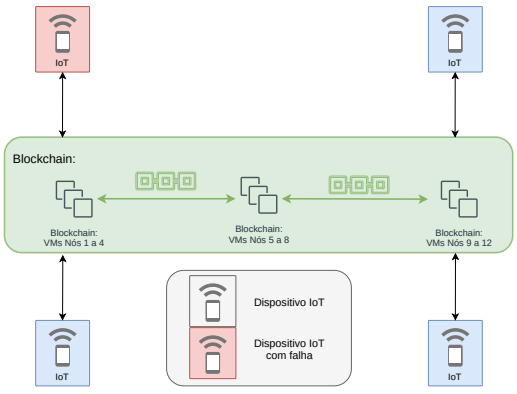

Figura 2. Blockchain com IoT

A partir da Figura 1 é possível observar o processo de uma rede blockchain de uma cadeia de suprimentos. Cada entidade participante, possui suas MVs para realizar o processo de validação das transações e inserção de novos blocos. Outra questão observada é relacionada às questões de segurança e vulnerabilidade da aplicação/ambiente. De maneira geral, a segurança de serviços hospedados dentro de uma nuvem *Infrastructure as a Service* (IaaS) são questionados quando os usuários destas instituições possuem acesso aos nós da blockchain [Security Report 2019]. Exemplos destas violações são ataques DoS realizados por usuários de forma acidental ou maliciosa.

Quanto as redes blockchains, é crescente a preocupação quanto às questões relacionadas ao consumo energético, escalabilidade, custo computacional e *etc*. Outra questão é relacionado ao ambiente em que os nós da blockchain são criados, destacando-se os serviços de virtualização das nuvens computacionais. Quanto às configurações recomendadas de *flavors* para a criação das MVs variam de acordo com a plataforma blockchain escolhida.Por exemplo a plataforma Hyperledger Fabric possui recomendações para ambientes de testes e de produção, e aplicados pelas plataformas IBM, AWS e Azure, em ambientes de produção é indicado que a MV possua 2 vCPU e 4 GB de RAM [The Linux Foundation 2018, IBM 2020, Reinmueller 2018, Contributor 2019]. Com estas características de *flavor* apresentadas e baseando-se em um caso real de uma cadeia de suprimentos (Figura 1) é observado um ambiente de interação e troca de mensagens entre as MVs na rede blockchain. A partir deste cenário dois possíveis cenários que retratam situações que podem ocorrer em ambientes reais.

No cenário ilustrado pela Figura 2 é apresentado uma rede blockchain com MVs e dispositivos *Internet of Things* (IoT) que enviam transações para a rede blockchain. Este cenário reflete um ambiente de produção que em determinado momento um dos dispositivos IoT apresenta uma falha que realiza o envio de diversas transações para a rede blockchain. Com a ocorrência desta situação, a rede blockchain não possui a capacidade de distinguir as transações verdadeiras enviadas por este dispositivo e pelos demais, ocasionando um ataque DoS. É importante ressaltar que este DoS foi produzido de uma maneira não intencional, sem a intervenção de nenhum usuário malicioso e produz instabilidade para a aplicação e ao ambiente.

O segundo cenário é formado por um ambiente blockchain com um usuário malicioso, que possui o objetivo de subverter o sistema com um ataque DoS. Neste cenário, para realizar a subversão do sistema através de um DoS é possível através do esgotamento dos recursos, explorando vulnerabilidade dos protocolos de comunicação e diminuição da largura de banda. Assim, a primeira forma de ataque é através da exporação de vulnerabilidades dos protocolos de comunicação, gerando ataques contra uma única MV, com este ataque uma considerável quantidade de recursos é consumida, ocasionando em uma subversão da MV. A segunda forma é que a instância maliciosa envia uma quantidade significativa de transações falsas-positivas para a rede blockchain, deixando-a sobrecarregada e dificultando o processo de validação das transações lícitas, da mesma forma que ocorre no cenário ilustrado pela Figura 2, ocasionando instabilidade para a rede.

A partir destas possibilidades de cenários e necessidades de cada sistema, surgem algumas questões. Questões relacionadas as configurações adequadas do *flavor* de instância, a quantidade de transações necessárias para operacionalizar o uso da tecnologia e também quanto as métricas e critérios para detecção dos problemas na blockchain ou

não aplicação. Estas questões tornam-se importantes para o desenvolvimento de uma rede blockchain, pois as quantidades de transações que são necessárias e suportadas pela MV estão diretamente relacionados com as configurações das MV.

2. Requisitos & Trabalhos Relacionados

A partir da definição do problema existente é necessário o levantamento de pré-requisitos para propor uma solução para o problema levantado. O primeiro pré-requisito é o acesso a uma nuvem computacional privada IaaS, que possua MVs com o *flavor* definido na Seção 1. O segundo pré-requisito é a criação de cenários pertinentes e com MVs com privilégios para coleta de tráfego de rede e informações quanto às instâncias. Com a adoção destes pré-requisitos, é possível a determinação dos requisitos funcionais e não funcionais (Tabela 1. Estes requisitos possuem como objetivo apresentar as funcionalidades que o sistema deve interagir e também apresentar o comportamento do sistema.

Tabela 1. Requisitos Funcionais (RF) & Não Funcionais (RNF).

Requisitos	Descrição
RF1	O ambiente deve permitir a realização de transações através de *Application Programming Interface* (API) ou mecanismos automatizados para a rede blockchain
RF2	O envio das transações deve ser coletado, seu *hash* para eventuais verificações
RF3	Coletar as métricas como: processamento, memória, redes (TCP e UDP) e latência de transações
RNF1	O sistema deve fornecer meios de parametrizar o sistema, permitindo que seja adequado às características do experimento
RNF2	As técnicas adotas para captura das métricas e transações não devem afetar o desempenho

Com a definição dos requisitos funcionais e não funcionais e com o objetivo de conduzir análises quanto ao desempenho e segurança em redes blockchain privadas é realizado uma revisão sistemática com finalidade de identificar trabalhos que possuam escopo similar ao objetivo da pesquisa. Para condução desta revisão foi aplicado a revisão de [Kitchenham et al. 2009] que apresenta critérios para inserção e exclusão de trabalhos a partir das bases da IEEE, ACM, SciELO, Springer e Elselvier. A partir da revisão sistemática e aplicação dos critérios pré-determinados, a revisão obteve um total de cinco trabalhos que possuem relação com os temas da pesquisas. A Tabela 2 apresenta uma comparação entre os trabalhos relacionados com os requisitos funcionais.

Tabela 2. Trabalhos relacionados *vs.* Requisitos Funcionais.

	[Dorri et al. 2017]	[Rouhani and Deters 2017]	[Pongnumkul et al. 2017]	[Hao et al. 2018]	[Vatcharatiansakul and Tuwanut 2019]
RF1	Sim.	Sim	Sim	Sim	Sim.
RF2	Não.	Não.	Não.	Não.	Não.
RF3	Parcialmente	Parcialmente	Parcialmente	Parcialmente	Parcialmente

Os trabalhos relacionados (Tabela 2) não possuem ligação direta ao objetivo deste trabalho ou com as questões relacionadas a segurança ou MVs. Contudo, estes possuem como objetivo a realização de testes relacionados ao desempenho de mecanismos de consenso e a plataforma blockchain, em particular ao Ethereum e o Hyperledger. Tornando-os importante pelo seu relacionamento com os objetivos específicos, auxiliando a obtenção de um maior escopo para seleção dos critérios para realização da análise de desempenho e segurança deste trabalho.

3. Proposta

O ambiente ilustrado pela Figura 1 é composto por MVs que possuem como configurações de *flavor* 2 vCPU e 4 GB de RAM, neste ambiente dois possíveis cenários são apresentados, um que ocorre DoS de forma não intencional e outro de forma intencional.

Em um ambiente de produção que ocorra um ataque DoS de forma não intencional ocorre algumas situações.A primeira destas ocorre a partir do acúmulo de diversas transações que a plataforma recebe, que ocasiona em uma alta de taxa de tráfego de rede que resultam na latência da rede. A segunda situação mantém o mesmo raciocínio da primeira, mas que através da latência e redução do tráfego de rede ocorre a indisponibilidade do serviço ou descarte de pacotes que estão na fila.

Em um ambiente de produção em que ocorra um ataque DoS de forma intencional há outras possíveis situações. Neste ambiente, a primeira situação que possa ocorrer é quando o nó malicioso realiza ataques contra a rede blockchain através do envio de diversas transações falsas/positivas para a rede, buscando um acumulo de transações no tráfego de rede que resultam na latência, ocasionando atrasos no processo de validação e uma possível indisponibilidade do serviço. A segunda situação, neste ambiente, é quando o nó malicioso realiza ataques diretamente à um nó íntegro com o objetivo de consumir recursos do nó e subversão da instância, deixando a rede blockchain com um nó a menos e produzindo instabilidade na mesma.

A partir das situações de ataques DoS não intencionais e intencionais e apresentação dos comportamentos que são esperados, este trabalho propõe-se em realizar uma análise de segurança e desempenho em uma rede blockchain, durante a execução de um ataque DoS interno. De modo mais específico, este trabalho possui alguns aspectos para serem analisados: A quantidade de transações por minuto que uma instância consegue receber sem prejudicar o serviço, a imutabilidade e integridade das transações e estabelecer uma relação entre o configuração da MV e a intensidade dos ataques DoS sobre os recursos computacionais monitorados.

Visando o objetivo de atingir os aspectos propostos, é exigido o monitoramento de alguns recursos no experimento aplicado. Em questões relacionadas a instâncias o monitoramento do processamento e memória são realizados para monitoramento de ocupação destes recursos durante o período do ataque. Em relação as questões da plataforma blockchain, é necessário realizar o monitoramento das quantidades de transações enviadas, a latência e o tráfego de rede. Estes recursos relacionados a plataforma blockchain, apresentam o comportamento do sistema durante a realização do ataque DoS.

Para a realização da análise proposta, são desenvolvidos três cenários de testes, que diferenciam-se pelo mecanismos de consenso que aplicado. A decisão pela aplicação de três diferentes mecanismos de consenso deve-se ao fato da importância que um mecanismos de consenso exerce sobre uma rede blockchain, sendo este um fator relevante para a realização destes experimentos. A Figura 3 ilustra as principais características destes cenários para a realização dos testes.

A partir da Figura 3 é possível observar a topologia aplicada nos cenários de experimentos. Estes cenários são compostos por seis instâncias com imagens de distribuição GNU/Linux CentOS 8. As instâncias possuem como configuração de *flavor* de 2 vCPUs e 4 GB de RAM, sendo este *flavor* o indicado pela plataforma Hyperledger Fabric aplicada neste trabalho [The Linux Foundation 2018]. Estes cenários são diferenciados pela aplicação dos mecanismos de consenso pBFT, PoS e PoA.

Com a definição dos três cenários para experimentos e com a apresentação das hipóteses, a primeira trata-se da ocorrência de um ataque DoS de forma não intencional e

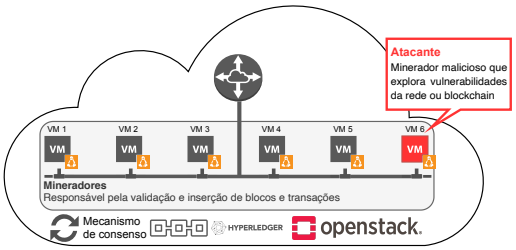

Figura 3. Arquitetura cenários

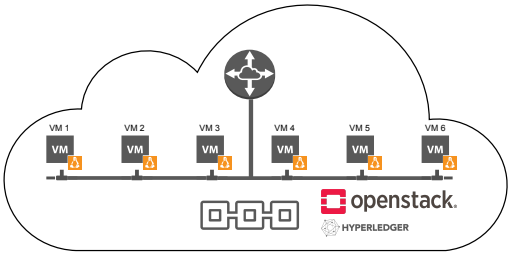

Figura 4. Arquitetura ambiente

a segunda trata-se de um ataque DoS de forma intencional. É importante ressaltar que nos três cenários de experimentos definidos, nenhuma das MVs possuem habilitadas recursos de memória virtual *swap*, apenas utilizam a memória principal, pois os experimentos possuem o objetivo de esgotarem os recursos destas instâncias. Neste sentido, são executados os seguintes experimentos em cada um dos cenários:

- Experimento 1: Realizar diversas transações através de um usuário/cliente na rede blockchain, com o objetivo de redução do tráfego de rede ou indisponibilidade de serviço, visando a identificação, a partir do monitoramento dos recursos e transações, da estabilidade da rede na ocorrência de um ataque DoS de forma não maliciosa.
- Experimento 2: Neste experimento há um usuário malicioso que envia transações diretamente para uma nó de uma blockchain, com objetivo de consumo de recursos desta instância, visando a identificação da estabilidade da instância e também da rede blockchain perante a ocorrência de um ataque DoS de forma maliciosa.

4. Ambiente de Experimentos

O experimento foi construído na nuvem computacional do Laboratório de Processamento Paralelo e Distribuído (LabP2D) de modelo IaaS e solução OpenStack. A abordagem escolhida foi a utilização de MVs com as configurações de *flavor* 2 vCPU e 4 GB de RAM e solução da plataforma Hyperledger Fabric e o modelo privado. Ainda que o uso de uma rede blockchain, comumente, não seja aplicado em apenas uma nuvem computacional, a escolha se deu pela praticidade de execução dos experimentos e isolamento de outros fatores (e.g., tráfego de *background*) que tornam a análise mais subjetiva e complexa. A partir desta questão, a arquitetura foi construída através de três principais componentes: rede, roteador e MVs (Figura 4).

Tabela 3. Experimentos *vs.* Requisitos Funcionais e Não Funcionais.

	Experimento 1	Experimento 2
RF1	Sim	Sim
RF2	Sim	Sim.
RF3	Sim	Parcialmente, somente métricas das instâncias.
RNF1	Sim	Sim
RNF2	Sim	Sim

A Tabela 3 apresenta um comparativo entre os requisitos funcionais e não funcionais com os Experimentos 1 e 2. Quanto ao Experimento 1 é possível observar que este possui maior relacionamento aos requisitos, este motivo deve-se ao fato que o Experimento 1 aborda somente as questões de exploração de um ataque DoS que estão diretamente relacionadas a rede blockchain. Enquanto o Experimento 2 possui o objetivo de consumo de recursos direcionados para uma única instância.

5. Considerações & Trabalhos Futuros

Esta análise baseia-se em um trabalho produzido anteriormente [Miers et al. 2019], que é relacionado à questões de segurança e mecanismos de consenso nas plataformas Multichain e Ethereum. A pesquisa atualmente encontra-se com o ambiente de experimentos implementado e os experimentos em execução. Os resultado iniciais apresentam que com apenas uma instância executando um ataque DoS e o suficiente para comprometer um nó da rede blockchain operando com uma MV com *flavor* padrão.

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

Referências

Contributor, A. W. S. (2019). Amazon Web Services BrandVoice: How Sony Is Protecting Rights Of Digital Creators Using Blockchain on AWS. Library Catalog: www.forbes.com Section: Innovation.

Dorri, A., Kanhere, S., Jurdak, R., and Gauravaram, P. (2017). Blockchain for iot security and privacy: The case study of a smart home. In *2017 IEEE PerCom Workshop*, pages 618–623.

Hao, Y., Li, Y., Dong, X., Fang, L., and Chen, P. (2018). Performance analysis of consensus algorithm in private blockchain. In *2018 IEEE Intelligent Vehicles Symposium (IV)*, pages 280–285.

IBM (2020). Módulos do IBM Food Trust.

Kitchenham, B., Brereton, P., Budgen, D., Turner, M., Bailey, J., and Linkman, S. (2009). Systematic literature reviews in software engineering – a systematic literature review. *Information and Software Technology*, pages 7–15.

Lin, I.-C. and Liao, T.-C. (2017). Survey of blockchain security issues and challenges. *International Journal of Network Secutiry*.

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.

Pongnumkul, S., Siripanpornchana, C., and Thajchayapong, S. (2017). Performance analysis of private blockchain platforms in varying workloads. In *26th ICCCN*, pages 1–6.

Reinmueller, J. (2018). Blockchain spotlight: Singapore Airlines - KPMG Global.

Rouhani, S. and Deters, R. (2017). Performance analysis of ethereum transactions in private blockchain. In *8th IEEE ICSESS*, pages 70–74.

Security Report (2019). Funcionários são responsáveis por nove em cada dez violações de dados na nuvem.

The Linux Foundation (2018). An introduction to hyperledger. page 33.

Vatcharatiansakul, N. and Tuwanut, P. (2019). A performance evaluation for internet of things based on blockchain technology. In *5th ICEAST*, pages 1–4.