Análise de Segurança dos Mecanismos de Consenso no PBFT usando Multichain e PoW usando Ethereum Aplicados em Redes Blockchain Privadas_Consórcio

No trabalho é apresentado um experimento para determinar aspectos relacionados a vulnerabilidade de blockchains. A problemática apresentada é a falta de trabalhos na área que relacionem essas questões com casos reais e testes. Também é mencionado a falta de critérios para comparar mecanismos de consensos do blockchain e seu relacionamento com essas vulnerabilidades.

Para o experimento foram testados dois mecanismos: pBTF e PoW em blockchain privado submetidos a ataques de negação de serviços. Os experimentos foram realizados em um ambiente Ubuntu Server 16.04 LTS. Foram testados dois cenários: uma plataforma Ethereum com mecanismo PoW em rede privada e o segundo usando a plataforma Multichain com mecanismo pBTF em rede privada também.

No primeiro cenário foram testados dois algoritmos para DoS: Transaction Flood e UDP Flood. O primeiro não demonstrou alteração no processamento e memória que causassem instabilidades. Já o segundo algoritmo apresentou uma diminuição significativa de mineração, além de ocorrerem interrupções temporárias na troca de informações. Para o segundo cenário foram testados o Transaction Flood, assim como no cenário anterior, porém o segundo algoritmo testado é o SSH Flood. No primeiro algoritmo houve um aumento significativo na quantidade de memória consumida, enquanto que no segundo não foram identificados alterações que causassem impactos negativos.

Por fim os autores comentam que é necessário atenção com relação a inserção de blockchains do tipo privado em instituições, de modo a diminuir a superfície de ataque.