Avaliação de segurança em Smart Contracts através de ferramentas de testes

Valentine Soares Piagetti[1], Roben Castagna Lunardi[1*]
[*]Orientador(a)

[1]Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS) - *Campus* Restinga. Porto Alegre, RS

A tecnologia blockchain se popularizou através da criptomoeda Bitcoin, sendo responsável por armazenar seus registros de transações. Esta blockchain tinha como objetivo inicial promover transferências monetárias confiáveis sem a necessidade de uma instituição centralizadora. Com a maturidade, a tecnologia de blockchain pode ser encontrada em diversas áreas de serviços, como por exemplo, garantir o direito autoral de músicas através da aplicação BMCProtector, auxiliar e rastrear doações para caridade com Charity-Chain, coordenar redes de abastecimentos agrícolas através do Supply chain model, entre outros. Tudo isso é possível, pois a tecnologia blockchain provê confiabilidade em seus dados sendo uma rede descentralizada, não-repúdio e imutável. Além de apresentar tais características, também há a funcionalidade de armazenar e executar trechos de códigos. Nomeados como smart contracts, ou contatos inteligentes, esses trechos de códigos são executados no topo da cadeira de blocos buscando facilitar, executar e se fazer cumprir um acordo entre partes não confiáveis, sem o envolvimento de uma terceira parte confiável. Para evitar a adulteração, os smart contracts são copiados para cada nó da rede blockchain. Com a automação, erros humanos podem ser reduzidos. Contudo, smart contracts também podem se tornar vulneráveis a ciberataques. Por exemplo, quando um smart contract foi manipulado para roubar cerca de 2 milhões de Ether através da vulnerabilidade de reentrada. Além do problema de vulnerabilidade, os smart contracts enfrentam vários desafios como questões jurídicas, de privacidade e de desempenho. Este trabalho tem por objetivo realizar uma pesquisa sobre trabalhos já publicados abordando o uso de smart contracts e também a análise de suas vulnerabilidades. Buscando fazer uma comparação entre as diferentes áreas de estudo e destacando a importância de todas no momento de desenvolver smart contracts mais seguros e eficientes. Para realizar esta comparação, está sendo feito buscas por diferentes artigos na área de estudo e selecionando algumas ferramentas para exemplificar o uso de smart contracts e também analisar suas vulnerabilidades. As ferramentas pré-selecionadas são SmaCoNat, Oyente, ContractFuzzer e Reguard.

Palavras-chaves: Blockchain. Smart Contracts. Testes.