Análise comparativa de ferramentas de teste de smart contracts

André Jonatan dos Santos[1], Roben Castagna Lunardi[1*]

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

Os Smart Contracts, ou Contratos Inteligentes, são uma tecnologia que permite que códigos sejam executados de forma descentralizada e/ou colaborativa por diferentes usuários/nós/entidades. Para que isso seja possível, os Smart Contracts são regidos e gerenciados por alguma blockchain. Por sua vez, blockchains são sistemas distribuídos, podendo ser compreendidos como uma corrente de blocos compartilhada por todos os "nós" participantes. A blockchain oferece um alto nível de segurança das informações, uma vez que os algoritmos de hash juntamente às assinaturas digitais permitem que torne difícil a adulteração de alguma informação inserida na blockchain. Dessa forma, um Smart Contract não pode ser excluído após a sua implementação e inserção de um na blockchain. Portanto, qualquer problema que eventualmente ocorra no código Smart Contract, permanecerá nele para sempre. Ou seja, erros em Smart Contracts podem levar a perda de grandes quantidades de dinheiro, extravio de tokens, transações indesejadas, etc. Este trabalho visa analisar e avaliar a utilização de diversas ferramentas de testes de vulnerabilidades em Smart Contracts e sintetizar um guia para o desenvolvimento de Smart Contracts seguros. Dos resultados parciais obtidos, foi a análise e comparação das ferramentas de testes de vulnerabilidade em Smart Contracts chamadas Mythril e Slither, ferramentas de código aberto e disponíveis de forma gratuíta. Pretende-se, a partir deste estudo, poder categorizar as ferramentas de testes em Smart Contracts. Primeiramente foram desenvolvidos scripts para automatizar o processo de configuração das ferramentas, visto que precisa ser adaptada uma configuração para cada Smart Contract. Após a análise, conclui-se que a ferramenta Slither apresenta melhor resultado para testes instantâneos durante o desenvolvimento, pois traz análises com tempo menor de execução e com erros/falhas descritas de forma precisa. Além disso, esta ferramenta apresenta análises informacionais sobre o código do contrato, tendo uma documentação extensa sobre as falhas, as explicando e mostrando como resolvê-las. Por outro lado, a ferramenta Mythril tem testes mais lentos, onde as análises podem demorar desde alguns segundos até várias horas para ser concluída. Porém, esta ferramenta traz análises com maior detalhamento e profundidade. Ainda, a ferramenta Mythril traz uma opção de configuração da análise para definir a profundidade de estados testados nela, assim possibilitando ao desenvolvedor/testador definir de acordo com sua necessidade. Ressalta-se que as duas ferramentas se complementam, pois há falhas de segurança que uma encontra e a outra não, portanto o uso conjunto das duas agrega mais do que o seu uso individual.

Palavras-chave: Smart Contracts; Análise de segurança; Vulnerabilidades.

CNPq FAPERGS