

Revisão de ferramentas para testes em smart contracts

Eduardo Fraga de Freitas¹, Roben Castagna Lunardi¹

*Orientador(a)

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

Smart Contracts, como sua tradução diz, são contratos inteligentes, ou seja, eles são programados para operar completamente ou parcialmente sem maiores interferências depois de seus deploys e com alto nível de segurança. Para isso, esses contratos são mantidos e gerenciados em blockchains, que podem ser entendidos como um sistema distribuído, onde os nós participantes compartilham uma cadeia de blocos ligados pelo hash criptográfico. Desta forma, dados de uma blockchain possuem alta resistência à adulteração da informação. O projeto realizado consiste em identificar e comparar ferramentas de testes para Smart Contracts, reunindo informações que serão coletadas e verificadas cautelosamente. Este trabalho servirá de base para desenvolvedores de Smart Contracts, que poderão usá-lo para consultas e comparações entre diferentes ferramentas. Dessa forma, o objetivo deste trabalho consiste em criar um material em que seja possível consultar e receber comparações prévias entre diversas ferramentas de testes para Smart Contracts, particularmente para aqueles codificados em Ethereum. Ainda, pretendemos elencar as ferramentas que possuem documentação atualizada e que possuem suporte a diferentes linguagens de Smart Contracts. Para a obtenção de resultados serão selecionados códigos prontos com erros e sem erros, para verificar a confiabilidade das ferramentas e, logo, será feita uma lista com as principais funcionalidades de cada ferramenta, citando seus pontos fortes e fracos. Os testes ainda estão em processo inicial, portanto ainda não há resultados parciais numéricos, mas de acordo com as pesquisas realizadas, esta área de testes não é muito explorada, poucos materiais e tutoriais são encontrados, por mais que seja de extrema importância para a segurança de um contrato. Como resultados esperados pretende-se elencar as ferramentas de pentest mais adequadas para cada tipo de contrato. Ademais, espera-se difundir o uso de metodologias de testes no desenvolvimento de Smart Contracts, aprimorando a corretude e segurança de aplicações distribuídas que utilizam Smart Contracts (também conhecidas como Dapps).

Palavras-chaves: Smart contracts; ferramentas; testes.