World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:15, No:06, 2021

A Survey on the Blockchain Smart Contract System: Security Strengths and Weaknesses

Authors : Malaw Ndiaye, Karim Konate

Abstract : Smart contracts are computer protocols that facilitate, verify, and execute the negotiation or execution of a contract, or that render a contractual term unnecessary. Blockchain and smart contracts can be used to facilitate almost any financial transaction. Thanks to these smart contracts, the settlement of dividends and coupons could be automated. Smart contracts have become lucrative and profitable targets for attackers because they can hold a great amount of money. Smart contracts, although widely used in blockchain technology, are far from perfect due to security concerns. Since there are recent studies on smart contract security, none of them systematically study the strengths and weaknesses of smart contract security. Some have focused on an analysis of program-related vulnerabilities by providing a taxonomy of vulnerabilities. Other studies are responsible for listing the series of attacks linked to smart contracts. Although a series of attacks are listed, there is a lack of discussions and proposals on improving security. This survey takes stock of smart contract security from a more comprehensive perspective by correlating the level of vulnerability and systematic review of security levels in smart contracts.

Keywords : blockchain, Bitcoin, smart contract, criminal smart contract, security
Conference Title : ICBC 2021 : International Conference on Blockchain and Cryptocurrencies
Conference Location : New York, United States
Conference Dates : June 03-04, 2021