World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:15, No:04, 2021

Cryptocurrency Crime: Behaviors of Malicious Smart Contracts in Blockchain

Authors : Malaw Ndiaye, Karim Konate

Abstract : 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. The blockchain would allow all these transactions to be saved in a single ledger rather than in many databases through many organizations as is currently the case. Smart contracts have become lucrative and profitable targets for attackers because they can hold a large amount of money. This paper takes stock of cryptocurrency crime by assessing attacks due to smart contracts and the cost of losses. These losses are often the result of two types of malicious contracts: vulnerable contracts and criminal smart contracts. Studying the behavior of malicious contracts allows us to understand the root causes and consequences of attacks and the defense capabilities that exist although they do not definitively solve the crime problem. It makes it possible to approach new defense perspectives which will be concretized in future work.

Keywords : blockchain, malicious smart contracts, crypto-currency, crimes, attacks
Conference Title : ICBSCC 2021 : International Conference on Blockchain, Smart Contracts and Cryptocurrencies
Conference Location : Jerusalem, Israel
Conference Dates : April 29-30, 2021