World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:17, No:04, 2023

Bitcoin, Blockchain and Smart Contract: Attacks and Mitigations

Authors : Mohamed Rasslan, Doaa Abdelrahman, Mahmoud M. Nasreldin, Ghada Farouk, Heba K. Aslan

Abstract : Blockchain is a distributed database that endorses transparency while bitcoin is a decentralized cryptocurrency (electronic cash) that endorses anonymity and is powered by blockchain technology. Smart contracts are programs that are stored on a blockchain. Smart contracts are executed when predetermined conditions are fulfilled. Smart contracts automate the agreement execution in order to make sure that all participants immediate-synchronism of the outcome-certainty, without any intermediary's involvement or time loss. Currently, the Bitcoin market worth billions of dollars. Bitcoin could be transferred from one purchaser to another without the need for an intermediary bank. Network nodes through cryptography verify bitcoin transactions, which are registered in a public-book called “blockchain”. Bitcoin could be replaced by other coins, merchandise, and services. Rapid growing of the bitcoin market-value, encourages its counterparts to make use of its weaknesses and exploit vulnerabilities for profit. Moreover, it motivates scientists to define known vulnerabilities, offer countermeasures, and predict future threats. In his paper, we study blockchain technology and bitcoin from the attacker’s point of view. Furthermore, mitigations for the attacks are suggested, and contemporary security solutions are discussed. Finally, research methods that achieve strict security and privacy protocol are elaborated.

Keywords : Cryptocurrencies, Blockchain, Bitcoin, Smart Contracts, Peer-to-Peer Network, Security Issues, Privacy Techniques
Conference Title : ICECS 2023 : International Conference on Engineering and Computer Science
Conference Location : New York, United States
Conference Dates : April 24-25, 2023