Utilizing Blockchain to Overcome Cyber Security Concerns in the Internet of Things: A Review

Bandar Alotaibi

Abstract— The Internet of Things (IoT) is a wide network consisting of Internet-connected objects using installed software, such as home appliances, vehicles, and other entities embedded with sensors, actuators, radio-frequency identification (RFID), and electronics to exchange data. In the last two decades, numerous IoT solutions have been developed by small, medium-sized, and large enterprises to make our lives easier. Furthermore, private and academic researchers have extensively investigated some practical IoT solutions. The rapid expansion of IoT solutions accompanies numerous security concerns because the underlying IoT protocols and communication technologies have not considered security. Recently, blockchain has emerged to become one of the promising technologies that might overcome some of the IoT limitations (security limitations, in particular). Blockchain technology is a database ledger that uses a peer-to-peer (P2P) network and stores transactions and asset registries. Blockchain can be described as a mounting list of records (i.e., blocks) with the following properties: distributed, decentralized, immutable, and shared. This paper surveyed recent security advances to overcome IoT limitations using blockchain. In this article, the blockchain attempts to overcome IoT limitations that are related to cyber security have been classified into four categories: end-to-end traceability; data privacy and anonymity; identity verification and authentication; and confidentiality, data integrity, and availability (CIA). Intended as a guideline for future research, this paper also explores systematic processes.

For the published version of record document, go to:
http://dx.doi.org/10.1109/JSEN.2019.2935035