Chapter 69
A Review on the Importance of Blockchain and Its Current Applications in IoT Security

Manjula Josephine Bollarapu
Koneru Lakshmaiah Education Foundation, India

Ruth Ramya Kalangi
Koneru Lakshmaiah Education Foundation, India

K. V. S. N. Rama Rao
Koneru Lakshmaiah Education Foundation, India

ABSTRACT

In recent years, blockchain technology has attracted considerable attention. As blockchain is one of the revolutionary technologies that is impacting various industries in the market now with its unique features of decentralization, transparency, and incredible security. Blockchain technology can be used for anything which requires their transactions to be recorded in a secure manner. In this chapter, the authors survey the importance of the blockchain technology and the applications that are being developed on the basis of blockchain technology in area of IoT and security.

BLOCKCHAIN IN IOT

Decentralized Framework for IoT Digital Forensics for Efficient Investigation: A Blockchain-based

Jung Hyun Ryuet.al.(2019) proposed 2 outlines the diagram of proposed advanced legal sciences system for IoT condition. The proposed structure is partitioned into three layers: cloud; blockchain; and IoT gadgets. For the most part, in an IoT domain, gadgets speak with the cloud. By 2020, the quantity of IoT gadgets is relied upon to increment to 26 billion . For this situation, it is practically difficult to examine count-

DOI: 10.4018/978-1-6684-7132-6.ch069

less IoT gadgets utilizing existing advanced measurable strategies. Figure 2 shows a review of proposed computerized criminological structure for IoT condition in this paper. Each IoT gadget stores information produced during the time spent speaking with different gadgets in the blockchain as an exchange. The IoT condition incorporates every little condition utilizing IoT gadgets: sensors; keen vehicle; savvy building; shrewd industry; brilliant home; brilliant matrix. In these conditions, cybercrime can happen whenever, and legitimate criminological system for it must be built up. In the IoT gadget classification, gadgets have different purposes, administrations, makers, advances, and information types. IoT gadgets send and receivelarge measures of information paying little heed to gadget client's will. For this situation, if the current criminological strategy is applied to every gadget framing an enormous number of connections, the examination turns out to be very difcult. Along these lines, in the proposed structure, the information created during the time spent correspondence of each IoT gadget are put away as an exchange in the blockchain. The computerized scientific agent abuses the put away trustworthiness of squares and the simplifed chain of guardianship process.

Secure Firmware Update for Embedded Devices in an IoT Environment: A Block chain Based

Boohyung Leeet.al.,(2017) In this paper, we center around a safe firmware update issue, which is an essential security challenge for the implanted gadgets in an IoT domain. Another firmware update conspire that uses a blockchain innovation is proposed to safely check a firmware adaptation, approve the accuracy of firmware, and download the most recent firmware for the installed gadgets. In the proposed plot, an inserted gadget demands its firmware update to hubs in a blockchain arrange and gets a reaction to decide if its firmware is modern or not. If not most recent, the implanted gadget downloads the most recent firmware from a distributed firmware sharing system of the hubs. Indeed, even for the situation that the variant of the firmware is upto-date, its respectability, i.e., accuracy of firmware, is checked. The proposed conspire ensures that the inserted gadget's firmware is state-of-the-art while not altered. Assaults focusing on known vulnerabilities on firmware of installed gadgets are in this manner moderated.

Blockchain Mechanisms for IoT Security

MatevžPustišeka(2018) et.al.,present three potential designs for the IoT front-end BC applications. They vary in situating of Ethereumblockchain customers (nearby gadget, remote server) and in situating of key store required for the administration of active exchanges. The functional limitations of these structures, which use the Ethereum arrange for believed exchange trade, are the information volumes, the area and synchronization of the full blockchain hub and the area and the entrance to the Ethereum key store. Consequences of these tests demonstrate that a full Ethereum hub isn't probably going to dependably run on a compelled IoT gadgets. In this manner the design with remote Ethereum customers is by all accounts a feasible methodology, where two sub-alternatives exist and contrast in key store area/the executives. Likewise, we proposed the utilization of designs with an exclusive correspondence between the IoT gadget and remote blockchain customer to additionally diminish the system traffic and improve security. We anticipate that it should have the option to work over low-power, low-bitrate portable innovations, as well. Our exploration explains contrasts in compositional methodologies, yet ultimate conclusion for a specific record convention and front-end application design is at emphatically dependent on the specific planned use case.