Chapter 4
A Novel Survey on Blockchain for Internet of Things

Jay Kumar Jain
Sagar Institute of Research and Technology, India

Varsha Jain
Bansal Institute of Science and Technology, Bhopal, India

ABSTRACT

Internet of things (IoT) is ready to change human life and release tremendous financial benefits. It may be that lack of information security and the belief of the current IoT are actually restricting its selection. Blockchain changes in an appropriated and secure record holds reliable records of information in various areas and possibly resolves information security concerns in the IoT system. This chapter presents a thorough review on the existing blockchain progress with an accent on IoT applications. The authors first give an overview of blockchain architecture including blockchain technologies and key characteristics of blockchain. The authors then discuss the blockchain for the internet of things including blockchain for IoT: technologies. Furthermore, they list some challenges and problems that will hinder blockchain development and summarize some existing approaches for solving these problems. Some possible future directions are also discussed. Future research bearings are ordered for a viable mix of blockchains in the IoT system.

INTRODUCTION

A blockchain is a decentralized, distributed database that is used to maintain a continuous growing list of records, which is called a block. This is a digital ledger of records which is shown in a network to capture transactions between different parties. For use as a distributed ledger, a blockchain is autonomously managed by a peer-to-peer network, which adheres to a protocol for inter-node communication and validates new blocks and after its creation includes all transactions. Each block contains a cryptographic hash of the past block, a timestamp, and exchange information. All members like businesses or people, utilizing the common database are "hubs" associated with the blockchain each keeping up an indistinguishable

DOI: 10.4018/978-1-6684-7132-6.ch004

Copyright © 2023, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

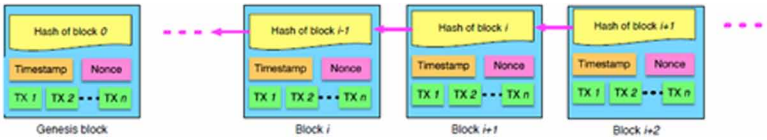
duplicate of the record. Each section into a blockchain is an exchange and all these exchanges show a trade of significant worth among members (i.e., an advanced resource that demonstrate rights, commitments or proprietorship). By and by, a wide range of sorts of blockchains are being developed and tried. Nonetheless, most blockchains pursue this essential system and approach. When one member needs to make an exchange with another, the various hubs in the system speak with one another utilizing a predecided component to watch that the new exchange is legitimate.

This mechanism is referred to as an assent calculation. When a transaction has been acknowledged by the system, all duplicates of the record are refreshed with the new data. Different exchanges are generally joined into a "hinder" that is attached to the record. Each square contains data that alludes back to past squares and along these lines all squares in the steel together in the dispersed indistinguishable duplicates. Taking an interest hub can include new, time-stepped exchanges, however, members can't erase or adjust the passages once they have been approved and acknowledged by the system. On the off chance that a hub changed a past square, it would not synchronize with the remainder of the system and would be prohibited from the blockchain. A legitimately working blockchain is in this manner changeless in spite of coming up short on a focal head.

Blockchain Architecture

According to Lee KuoChuen, D. et al. (2015), Blockchain is a series of blocks, which carries a complete list of transaction records like a traditional public ledger. Figure 1 outlines the case of a blockchain. Each block indicates the immediately previous block via a reference that is fundamentally a hash value of the previous block known as parent block. According to Buterin, et al. (2014) it is worth noting that uncle blocks (offspring of the block's predecessor) hashes will likewise be stored in ethereum blockchain. The initial block of a blockchain is known as genesis block which has no parent block. The author then presents the block structure in section 2.1, digital signature working in section 2.2. Additionally, authors also give a precise of blockchain key attributes in section 2.3. Also, Blockchain taxonomy is shown in section 2.4.

Figure 1. Sequence of blocks.



Block

A block comprises of the block header and the block body as mentioned in Figure 2. In particular, the block header includes:

1. Block version: implies which set of block validation rules to pursue.
2. Parent block hash: it is 256-bit hash values that indicate to the previous block.
3. Merkle tree root hash: the hash value of all the transactions in the block.

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/a-novel-survey-on-blockchain-for-internet-of-things/310439

Related Content

Security Issues in Blockchain-Based Businesses
Rajesh Yadavand Digvijay Singh (2023). *Cybersecurity Issues, Challenges, and Solutions in the Business World (pp. 186-195).*
www.irma-international.org/chapter/security-issues-in-blockchain-based-businesses/313866

Are Online Privacy Policies Readable?
M. Sumeeth, R. I. Singhand J. Miller (2010). *International Journal of Information Security and Privacy (pp. 93-116).*
www.irma-international.org/article/online-privacy-policies-readable/43058

Pharming Attack Designs
Manish Gupta (2007). *Encyclopedia of Information Ethics and Security (pp. 520-526).*
www.irma-international.org/chapter/pharming-attack-designs/13520

A Privacy-Aware Data Aggregation Scheme for Smart Grid Based on Elliptic Curve Cryptography With Provable Security Against Internal Attacks
Ismaila Adeniyi Kamiland Sunday Oyinlola Ogundoyin (2019). *International Journal of Information Security and Privacy (pp. 109-138).*
www.irma-international.org/article/a-privacy-aware-data-aggregation-scheme-for-smart-grid-based-on-elliptic-curve-cryptography-with-provable-security-against-internal-attacks/237213

Large Key Sizes and the Security of Password-Based Cryptography
Kent D. Boklan (2009). *International Journal of Information Security and Privacy (pp. 65-72).*
www.irma-international.org/article/large-key-sizes-security-password/4002