Enhanced security in IOT environment using Blockchain: A survey

S. Ramamoorthi [a], B. Muthu Kumar [b],*, M. Mohamed Sithik [a], T. Thinesh Kumar [a], J. Ragaventhiran [b], M. Islabudeen [b]

[a] Department of Computer Science and Engineering, Mohamed Sathak Engineering College, Kilakarai, Tamilnadu, India
[b] Department of Computer Science and Engineering, Syed Ammal Engineering College, Ramanathapuram, Tamilnadu, India

ARTICLE INFO

ABSTRACT

Blockchain (BC) methods is one of the best technologies in the Internet of Things (IoT) environments, it is a distributed sharing mechanism and communicate the IoT devices with secure manner. A blockchain is a connection of blocks and each block is linked to its earlier blocks. All block has the security hash code, previous block hash, and its data. The transaction between the BlockChain are the data is transfer between one IoT block nodes to another IoT Block node. The IoT device nodes are various types of physical devices like smart devices with embedded sensors, actuators, and capable of be in touch with other IoT device nodes. The responsibility of BlockChain in IoT is to grant a method to provide protected data transmission through IoT device nodes. In this paper discussed about the blockchain technology is how to secure the IoT transmission data and what are the challenges comes into these technologies. BlockChain is a safe method that can be used widely. IoT needs this type of skill to permit protected communication among IoT device nodes in mixed atmosphere.

© 2021 Elsevier Ltd. All rights reserved.
Selection and peer-review under responsibility of the scientific committee of the Emerging Trends in Materials Science, Technology and Engineering.

1. Introduction

The blockchain is a chain of consecutive blocks, which connecting an all list of transaction records like predictable user data. Figure 1 shows an example of a blockchain. Each block is point to previous block with hash code and point to next block with another hash code. The each block contain the timestamp, nonce and transaction history. The first block have no parent block that is called genesis block. We can create the block structure, digital signature mechanism and blockchain taxonomy. The blockchain is like a linked list in data structure architecture. The each and every node is connected by reference point value. The starting node containing the next block node reference point address, the second block node contain the previous node reference point address and next block node reference point address value. The last block node contains the previous block node address only. This is the structure of blockchain architecture which consists of a continuous sequence of blocks Fig. 1.1. [1]. Fig. 3.1. Fig. 3.2. Fig. 4.1.

The decentralization is main concept in blockchain technology. The computer or other organization network is not form a chain. As an alternative, the circulated user data ledger via the nodes connected to the chain [2–5]. The block Nodes is one type of electronic device that stores user data in the secure manner.

1.1. Block

A block contains block header and the block body as shown in Fig. 1.2.

In exacting the block header contains:

Parent block hash: it denotes the previous block hash value (256-bit hash value).

- Merkle tree root hash: all transaction in the block hash value.
- Timestamp: it denotes the current transaction value.
- nBits
- Nonce: it normally starts with 0 and increases for every hash value calculation(16-bits field,)

2. Literature survey

The authors **Sujit Biswas, Kashif Sharif, Fan Li, Sabita Maharjan, Saraju P. Mohanty, and Yu Wang** represents that many of the business organization relies on IoT. These include educational

* Corresponding author.
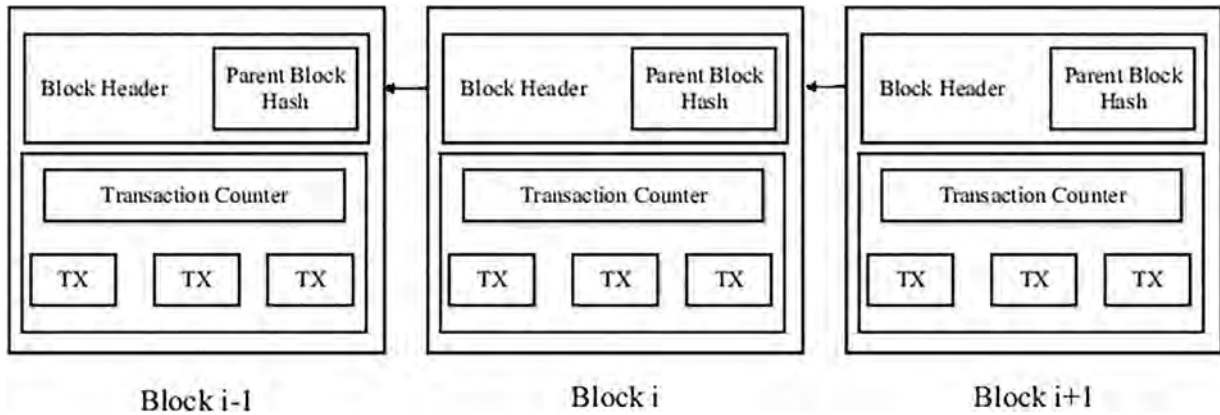E-mail address: muthu122@gmail.com (B. Muthu Kumar).

S. Ramamoorthi, B. Muthu Kumar, M. Mohamed Sithik et al.

Fig. 1.1. An example of blockchain which consists of a continuous sequence of blocks.
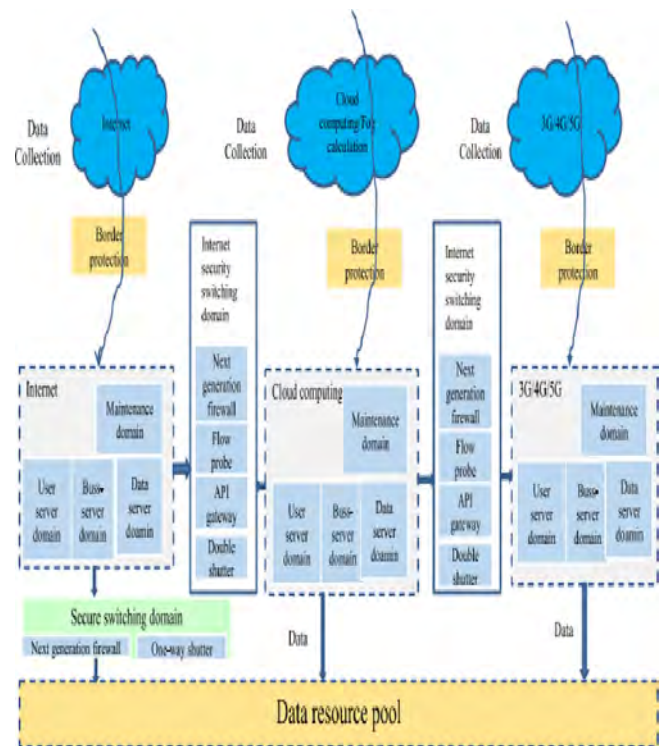

Fig. 1.2. Block structure.

Fig. 3.1. Blockchain IoT information security structure.

organization, manufacturing organization, medicine and other organization. All the above mentioned organization uses dissimilar networks for complete their task [6–8].This leads to many security challenges in the respective field. Already we have been using blockchain for providing security but this method is not sufficient due to dynamic challenges arises with respect to the security. So they are proposing PoBT algorithm for enhancing security as well as coping dynamic challenges in security. This method allows us to verify any blocks with in the short span. Also they were proposing ledger distribution mechanism for less memory utilization. End of their analysis process they have concluded that this mechanisms enhance the security level in IoT based application.

The author **Tanweer Alam** represents that IoT has been used for storing the node information including each and every transaction states. Blockchain is made by using normal chain mechanism where each part of the chain is associated with its previous and next part. In blockchain contains message digest function; previous part hash value and the information. IoT consist of dissimilar node includes sensors, actuators and any other physical devices and machines. Blockchain allows IoT to verify each and every process which is taking place within the environment. Author discusses about blockchain opportunities and challenges in IoT.

The authors **Hong-Ning Dai, Zibin Zheng and Yan Zhang** represents that IoT drives the industry towards smart devices based dissimilar network for their development process. Internal features

of IoT leads to many difficulties like interoperability, security related issues and optimization issues. In this paper they analyze about the blockchain method integration with IoT. Blockchain with IoT I shortly denoted as BCoT by the authors. Also the list out the challenges of integrating BC with IoT. Finally they were proposing BCoT architecture for combining BC with IoT [9].

The authors **Riya, Raj Chintan and Nishant** represents that Blockchain and IoT are two distinguished technology ruling the digital world. IoT make each and every physical as smart enabled one. SO this actually helps us to have the link between any two things. And exchange of information between those linked things possible. But the problem is who is going to take care of connecting and disconnecting those things when required. If we don't have verifier security will become very complicated one to achieve. Blockchain provide security for any IoT things and its network by verifying. Author proposes BIoT architecture for all issues related to integrating IoT with BC [10].

S. Ramamoorthi, B. Muthu Kumar, M. Mohamed Sithik et al.

Fig. 3.2. Security Framework for information Sharing in IoT.

Fig. 4.1. Representative application domains of Blockchain.

The authors **Mohamed Amine Ferrag , Lei Shu, Abdelouahid Derhab and Leandros Maglaras** represents that challenges are more in IoT field with respect to provide security. Describe about

4 tier green IoT model for managing smart agri. They suggest method for classifying security related matters in smart agri based IoT. How IoT is adapted for agri has been discussed by the authors. They analyze how blockchain can be used for green IoT most effectively. Finally they concluded that challenges and research directions in green IoT field.

The authors **Haiping Si, Changxia Sun, Yanling Li, Hongbo Qiao and Lei Shi** represents that blockchain is the first distributed security related mechanism. It achieves reliability for peer to peer environment. In this paper they proposed a lightweight IoT security framework based on BC. Method includes both data blockchain and transaction blockchain. Distributing the information and integrity of the information is achieved by practical Byzantine fault-tolerant. Security mainly depends on partial blind signature algorithms. They proposed a dynamic game method for node cooperation. Hidden node state is predicted by institutional reputation value. Malicious node can be managed by high-trust reference report. They conclude that this framework is most effectively and feasibly work against intruder activities.

3. IoT information sharing based on blockchain

The successful secure sharing method in the IoT is very difficult. There are many issues and a problem comes in the connectivity of data. The security difficulty comes in IoT information sharing has become important point and a complicated point in the information security. The information sharing is the user device data will be viewed by another secure IoT device. The method of information sharing is more important in the cryptographic algorithms [11–13]. The data may be off line or cloud based data in the Internet of Things. These technologies have many shortcut and methods: Facing a massive IoT information network Fig 3.1

Simplified Payment Verification (SPV) is one of the payment methods in digital transactions. In blockchain mechanism, it can be achieved by The Merkle tree algorithms.

3.1. Double-chain mode based on blockchain technology

The blockchain method was collects all data from IoT node and form the data book for private agreement mechanism. The IoT source data is reliable and the data is stored by centralized network systems. In IoT sensors devices, infrared sensor and other IoT devices are used to storage, transmission and computing the frequency of sensors. The blockchain methodology having capabilities of reduce the redundancy and improve the efficiency of the IoT devices. The IoT data is necessary to categorize, combine data expression and allocate storage operations.

3.2. Time stamp method for blockchain structure

Data blocks and chain structure used to store data in blockchain. Every block contains block header and block body. In each bock is assigned by unique address value and pointer reference value. The current block is stored the previous block address and next block address. Each block is denoted by timestamp. The timestamp contains the address value of block node and time of executions in the transactions [14].

3.3. IoT information security by blockchain

The combinations of information and IoT devices are main characteristic of blockchain IoT. The important basic operation contains real-time monitoring The real time program of blockchain IoT is that enables the energy information system to be altered by particular network [15]. The standard protocol of blockchain is provide

S. Ramamoorthi, B. Muthu Kumar, M. Mohamed Sithik et al.

the technical support of smart electronic IoT device sensor and information system. It solves the network security problems.

4. Applications of blockchain

Applications of blockchain technology classified into various aspects like finance, IoT, public and social services, reputation system, security and privacy. **Figure No: 4.1**

4.1. Finance

In established financial and business activities, Bitcoin and hyperledger has bring massive role. In banking sector blockchain is the prospective to affect the world. Blockchain knowledge is very much useful in financial activities and IT industries. Blockchain is used in Microsoft Azure and IBM service sector..

4.2. Internet of things (IoT)

IoT is the most potential area of ICT and its planned to combine the effects into the various services like Atzori, Miorandietal, logistic management with RFID, smart systems, online health services,

4.3. Public and social services

Different public and social aspects like Land registration, Energy saving, Education, Free-speech right are developed by Blockchain. It also involved in municipal services such as marriage registration, patent management and Income Tax systems.

4.4. Reputation system

In community confident, Reputation is the essential computation. The reputation of a human being computed on before business communications with the society. Reputation involved major role in academics and web community.

5. Conclusion

The block chains extremely appraised and authorized for its decentralized structure and peer-to-peer nature. In more developer and researchers find out the blockchain are secured by Bitcoin. But blockchain is used to a different fields far beyond Bitcoin. Blockchain has different personality like decentralisation, persistency, ambiguity and audit ability. In this paper, we present a broad survey on the blockchain. We describe an overview of blockchain technology like blockchain architecture and main blockchain characteristics. We discuss various blockchain algorithms. We list the different characters and various applications are used in blockchain IoT security. We explain the problems and

problems of blockchain implementation. In future we will develop a smart blockchain for enhanced security in the block node of IoT devices.

CRediT authorship contribution statement

S. Ramamoorthi: Conceptualization, Methodology, Writing - original draft. **B. Muthu Kumar:** Visualization, Writing - review & editing. **M. Mohamed Sithik:** Software. **T. Thinesh Kumar:** Investigation. **J. Ragaventhiran:** Supervision. **M. Islabudeen:** Validation.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] H. Si, C. Sun, Y. Li, H. Qiao, L. Shi, Future Generation Computer Systems 101 (2019) 1028–1040.
[2] Sujit Biswas, Kashif Sharif, Fan Li, Sabita Maharjan, Saraju P. Mohanty, and Yu Wang "PoBT: A Light Weight Consensus lgorithm for Scalable IoT Business Blockchain" IEEE Internet of Things Journal 2019
[3] D. Li, Z. Cai, L. Deng, X. Yao, H.H. Wang, Information security model of block chain based on intrusion sensing in the IoT environment, Cluster Comput. 22 (S1) (2019) 451–468.
[4] P.K. Sharma, S. Singh, Y.S. Jeong, DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks, IEEE Commun. Mag. 55 (9) (2017) 78–85.
[5] A. Ouaddah, A. Abou Elkalam, A. Ait Ouahman, FairAccess: a new Blockchain-based access control framework for the IoT, Secur. Commun. Netw. 9 (18) (2016) 5943–5964.
[6] W. He, Computational neuroscience applied in surface roughness fiber optic sensor, Trans. Neurosci. 10 (1) (2019) 70–75, http://dx.doi.org/10. 1515/tnsci-2019- 0012.
[7] M.H. Miraz, M. Ali, Blockchain enabled enhanced iot ecosystem security, Soc. Sci. Electron. Publ. 9 (3) (2018) 38–46.
[8] P.K. Sharma, M.-Y. Chen, J.H. Park, A software defined fog node based distributed blockchain cloud architecture for IoT, IEEE Access 6 (2018) 115–124.
[9] P. Alfonso, T. Nachiket, M. Giovanni, L. Francesco, P. Antonio, Blockchain and iot integration: a systematic survey, Sensors 18 (8) (2018) 2575.
[10] Z. Yu, J. Wen, The IoT electric business model: Using blockchain technology for the IoT, Peer-to-Peer Netw. Appl. 10 (4) (2017) 983–994.
[11] O. Novo, Blockchain meets IoT: An architecture for scalable access management in IoT, IEEE IoT J. 5 (2) (2018) 1184–1195.
[12] K.R. Ozyilmaz, A. Yurdakul, Designing a blockchain-based IoT with ethereum, swarm, and LoRa: The software solution to create high availabil- ity with minimal security risks, IEEE Consum. Electron. Mag. 8 (2) (2019) 28–34.
[13] M.-C. Chen, S.-q. Lu, Q.-L. Liu, Global regularity for a 2D model of electro-kinetic fluid in a bounded domain, Acta Math. Appl. Sin. Engl. Ser. 34 (2) (2018) 398–403.
[14] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, On blockchain and its integration with IoT, challenges and opportunities, Future Gener. Comput. Syst. 88 (2018) 173–190.
[15] M.A. Ferrag, M. Derdour, M. Mukherjee, Blockchain technologies for the IoT: Research issues and challenges, IEEE IoT J. 6 (2) (2018) 2188–2204. [14] G. Feng, L. Zhu, S. Meng, A blockchain-based privacy-preserving pay- ment mechanism for vehicle-to-grid networks, IEEE Netw. 32 (6) (2018) 184–192..