Secure Transactions Management Using Blockchain as a Service Software for the Internet of Things

Prince Waqas Khan and Yung-Cheol Byun

Abstract The Internet of Things (IoT) has enabled communication anywhere between physical devices. Currently, concerns have been raised about suspicious transactions in IoT systems. Suspicious transactions may have a logical structure inconsistent with current information in the context of IoT. This article describes suspicious transactions in IoT systems and manages them using the blockchain as a service software plans. This study builds software-specific components for blockchain functions to implement in IoT networks. This study was conducted using Hyperledger Fabric as a blockchain service to test the software-defined blockchain components blockchain. The model was evaluated using average transaction throughput and latency. We observed that using blockchain as a software service system can provide excellent performance and security.

Keywords Internet of things (IoT) · Suspicious transactions · Blockchain · Hyperledger fabric

1 Introduction

With the rapid development of the internet of things, incumbent operators are beginning to make a big difference in digitization. In the age of the Internet of Things, millions of devices and links to the Internet of Things are a big problem for data management. Many systems today use centralized systems to manage IoT devices, creating privacy, and security concerns while also managing IoT data [1]. Because of the blockchain's level, traceability, and latency, the blockchain has generated considerable interest in the IoT region. However, integrating current blockchain technology into the IoT is difficult due to the lack of scalability and high cost. Various blockchain

P. W. Khan · Y.-C. Byun (✉)
Department of Computer Engineering, Jeju National University, Jeju-si, Republic of Korea
e-mail: ycb@jejunu.ac.kr

P. W. Khan
e-mail: princewaqas12@hotmail.com

H. Kim and R. Lee (eds.), *Software Engineering in IoT, Big Data, Cloud and Mobile Computing*, Studies in Computational Intelligence 930,
https://doi.org/10.1007/978-3-030-64773-5_10

platforms have unique advantages in IoT data management mode. In work by Jiang et al. [2], the methods to integrate multiple blockchains to manage IoT data efficiently is explained. Their solution builds a shared server access system using a single blockchain as a control number. Other blockchain platforms dedicated to the defined IoT environment serve as the basis for all IoT devices. Their model is based on a notary approach and engages transactions in this way for certainty. They analyzed the system's performance evaluated through extensive testing.

Blockchain is a crucial technology for decentralized system management and is becoming increasingly popular when implementing smart grids and healthcare systems. However, due to the high resource requirement and low scalability due to frequent and frequent transactions, mobile devices with limited resources are limited. Integrate edge accounts to offload mining operations from mobile devices to cloud resources. This integration ensures reliable access, distributed processing, and tamper-free archiving for scalable and secure transactions. Therefore, critical issues related to security, scalability, and resource management must be addressed to achieve effective integration. Nyamtiga et al. [3] draw on peer-to-peer technology and blockchain to implement the Internet of Things (IoT) design, supported by cutting-edge computing to achieve the level of security and scalability required for integration. To successfully integrate the blockchain into the IoT system, they explored the existing blockchain and related technologies to create solutions to anonymity, integrity, and resilience. Research has been conducted to verify proper architecture requirements, and some researchers have applied a combination to popularize specific applications. Despite these efforts, the anonymity, resilience, and integrity of functional and secure distributed data storage still need to be further investigated.

Figure 1 illustrates some of the benefits that blockchain and IoT can bring together. High data security, robust data validation process, etc. Using the IoT blockchain use case, companies will get a complete information security network that can provide facilities that third-party providers cannot offer. IoT blockchain use cases can provide a validation process based on consensus algorithms to make data entry fairer. Users can trust this combo for added privacy of data and privacy. A fully transparent network is a trusted network. The problem with our shared centralized server is the lack of full transparency. Most companies also need a personal channel, so the IoT blockchain use case can only provide a particular chain between two parties.

Furthermore, IoT devices can use this channel to communicate with each other without problems. The main components of the IoT are sensors and RFID tags [4]. These tags allow anyone to track the object and ensure full reliability.

The rest of the article comprises related work explained in Sect. 2, Proposed architecture is explained in Sect. 3. Chapter 4 describes the transaction flow. Part 5 contained the simulation setup and evaluation results. We concluded the article in the conclusion section.

Fig. 1 Blockchain and IoT: Possible use cases

2 Related Work

Internet of Things and Blockchain technology is dominating many areas of research. The Internet of Things can find good results in various fields, but the BBC offers a reliable communication system for home communications. IoT devices for data exchange have been implemented since the blockchain. This led to a step-by-step integration process. The biggest downside to this combination is that blockchain's internal processing of information is complete and fast. On the other hand, due to many IoT devices, current blockchain solutions generate data at a faster rate than they can afford. On the other hand, Blockchain files cannot run on IoT devices due to a lack of resources. This way, the two technologies won't merge into their current state. The work by the Biswas et al. [5] uses a network of a local peer network to address these issues and provide solutions to close the gap. Domestic and global peer-to-peer data connections offer the number of transactions sent globally without connecting to the complete information on the local server. The test values show a significant reduction in the weight and size of the reader through international comparison.

Blockchain is a distributed ledger that contains transactions related to blockchain. The ability to create, store, and send digital assets in a decentralized, decentralized, and tamper-proof manner is of great practical value for IoT systems. The biggest challenge in providing blockchain as a service to the Internet of Things is the host environment. Peripherals are usually very limited in terms of computer resources and available bandwidth, and the cloud or fog can be a potential host. The author

evaluates the use of fog and cloud as possible platforms [6]. Recently, the Software-Defined Industrial Internet of Things (SDIIoT) has emerged. This is considered an effective way to manage the Internet of Things dynamically. SDIIoT implements multiple SDNs to improve scalability and flexibility, forming a physical distributed control plane that processes large amounts of data generated by industrial equipment. However, it is difficult to reach consensus among many SDN controllers as the core of multiple SDNs. With the advent of blockchain technology, some IoT network management functions could be transferred from centralized systems to distributed certification bodies. The cloud-based blockchain application has been successfully implemented. However, the Internet of Things does not require the specific functionality of the blockchain.

An example of this is a competitive consensus. In their study, Samaniego et al. [7] explored the blockchain's capabilities in editing and hosting software-defined components. They provide ideas for customization and packaging. Therefore, blockchain resources allow electronic miners to collaborate and work closely together.

On the one hand, both blockchain cryptographic operations and non-crypto operations can access a set of computing resources such as the Mobile Edge Cloud (MEC). To improve the system's energy efficiency, Luo et al. [8] adjust the computing resources and block batch size, considering the trust characteristics of the SDN controller and the resource requirements of non-encryption operations. To realize a genuinely decentralized blockchain technique, we propose a partially observable Markov decision process (POMDP) and a new deep reinforcement learning (DRL) method to explain the problem and solve it. The simulation results compared three blockchain protocols and proved the effectiveness of each protocol scheme. Oktian et al. [9] propose a scalable, hierarchical blockchain architecture for the internet of things, consisting of a base engine and three auxiliary engines: payroll, computing, and storage stations. All of this makes it easy to run a workflow from IoT applications in documentation and proxies. They implemented a custom base engine and suggested the idea of using demand configuration and prioritization to improve its performance effectively. They also provided preliminary evidence for a conceptual implementation to evaluate engine-to-engine interoperability and implement concurrency in a pilot application for IoT car rental. Their evaluation results show that their proposal is feasible and works well in the local online environment.

To date, most IoT operating systems are cloud-centric and use an integrated platform provided by the cloud. However, cloud-based infrastructure primarily implements static sensor and data flow systems that do not support IoT components' direct configuration and management. To solve this problem, the virtualization of IoT components at the edge of the IoT network, Samaniego et al. [10], introduce an authentication-based blockchain protocol for providing virtualized resources directly to end devices. The proposed architecture focuses on deploying configuration tasks at the edge of an IoT network, using virtual resources and blockchain protocols as management tools. Their work also provides an evaluation of the implementation of the two permission-based blockchain protocol methods. The idea of connecting material things and networks to create new and productive interactions is a critical component of the concept of smart spaces. One of the significant challenges of these

new intelligent spaces is controlling access to data, services, and things. Blockchain technology has become the most promising solution for distributed access management. Function-based access control allows users to access data/services/things by sending texts between decentralized account books. Of course, managing the access test transport path is a big deal. In IoT, smart contracts are the main component of access control in most blockchain network proposals [11]. One of the biggest problems with using smart contracts as verification of access codes that can be transferred from one account to another is that smart contracts and chain codes must be immutable by design since they represent a bond between the two parties.

IoT systems are made more attractive by enabling ubiquitous connectivity. More and more trends today are focusing on suspicious deals on smartphones. Another study by Samaniego et al. [12] looks at suspicious smart business transactions and studies blockchain technology's characteristics to manage them. Besides, their study reveals new concepts of blockchain operating systems and interactive contracts that will help explore how to navigate different markets in an unfamiliar environment through provenance.

3 Proposed Architecture

We have proposed a secure transaction management using blockchain as a service software for IoT. We have used Hyperledger as a private blockchain for simulation purposes. The transaction of Hyperledger are recorded securely and are publicly available. All transactions are digitally signed before transmission over the network [13]. So, the transaction is something more secure, which represents the authenticity and integrity of Hyperledger.

The following can be considered as properties of blockchain:

- Blockchain is a decentralized public decentralized, secure database between IoT nodes.
- Each IoT node has a function to verify a block.
- Some IoT nodes can be considered controllers of the blockchain.
- Peer-to-peer topology is being used in the blockchain.
- Hyper Ledger stores all recorded transactions. The blockchain will be updated after recording.

Figure 2 explains the client interaction model with blockchain and IoT platforms. IoT consist of different devices blockchain acts as the middleware between those devices and users of different subnetworks. It helps to manage the transaction between nodes, devices, and users securely.

Figure 3 shows the proposed architecture. It has two main parts one is IoT layers, and the other is blockchain structure. IoT layers are composed of collaboration, application, data abstraction, data accumulation, edge computing, connectivity, and physical devices. They send several types of information through sensors to the

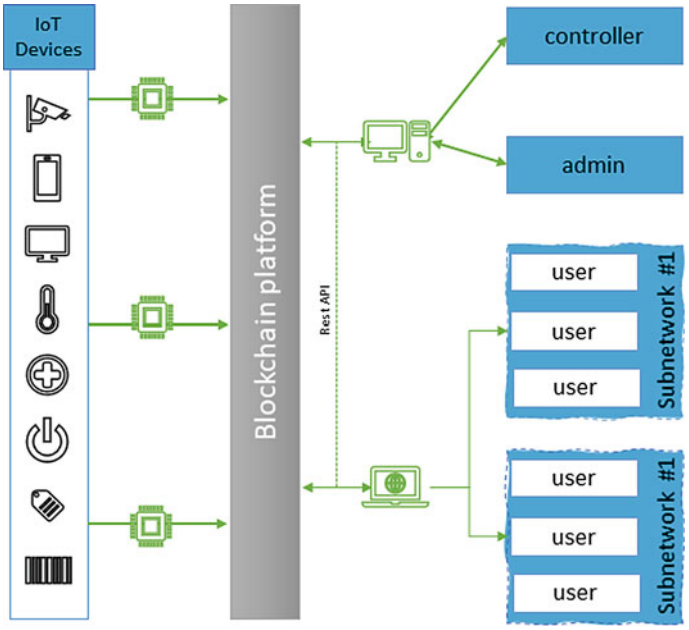

Fig. 2 Client interaction model

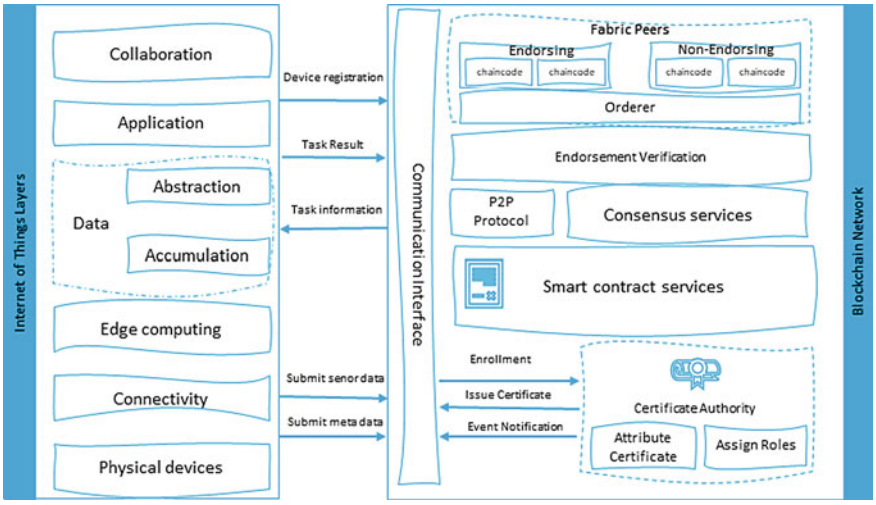

Fig. 3 Proposed architecture

blockchain. Blockchain interacts with these devices using the communication interface. Participants can have one or more peer nodes on the network. This structure defines several types of peer nodes on the model.

The first one is committing peer. As a key-value store, each peer maintains a current snapshot of the current state of the ledger. Such peers cannot call chaincode functions. The second one is endorser peer. Chaincode is installed on the Endorser peer. When they receive a transaction offer, they simulate transaction execution in an isolated container. Based on the simulation, such peers prepare transaction proposals and send them to the orderer's peers. Approving the existence of peers prevents all peers from executing transactions sequentially [14]. The third peer is called an orderer peer. The orderer receives the approved transaction and puts it in the block. After grouping the transactions, the orderer guarantees the agreement by propagating such blocks to the submitted peers, and the peers are verified and sent to the shared ledger. The orderer's peers record valid and invalid transactions, while other peers only include legitimate transactions [15].

4 The Transaction Flow

Transactions are transmitted in a peer-to-peer topology within the proposed framework. There are private IoT nodes in the network called miners and typically used to verify transactions. When the transaction is confirmed, it is converted into a block, added to the existing blockchain, and transmitted to the system. Miners play an essential role in coordinating newly created blocks on the blockchain. Follow the execution order confirmation form as follows.

4.1 Transaction Proposal

The blockchain client representing the organization writes a transaction proposal and sends it to colleagues identified in the referral policy [16]. The project includes the bidder ID, transaction burden and negligence, and transaction ID.

4.2 Endorsement

Recommendations include transaction simulation. Approvers create write and read groups that contain keys and modified values. The approval also verifies the legality of the execution of the transaction. Approval is sent after the proposal and includes the write package, read package, transaction ID, approver ID, and approver's signature [17]. When the customer has collected enough approvals (which should have the

same result), a transaction is created and sent to the ordering service. The approval phase eliminates the final uncertainty.

4.3 Order

In this stage, the order is executed after approval. The requested service verifies that the blockchain client sending the transaction proposal has the rights (broadcast and receive rights) on the specified channel. The sorted block contains the approved parameters for each channel. With this request, the network can reach a consensus. The customer sends the results of the transaction to all colleagues.

4.4 Validate

First, each party confirms the transaction received by making sure the transaction matches its recommended strategy. Then it scans all the transactions in the block to read and write collisions in sequence. For each transaction, the read key view is compared to the current default ledger view. Make sure the values are the same. If they do not match, the other party rejects the transaction. Finally, update the ledger [18]. The ledger is based on the created block—additional ledger validation test results, including invalid transactions.

5 Performance Evaluation

This section presents the results of the proposed system evaluation.

Figure 4 shows the command-line interface for the starting the Hyperledger Fabric. After installation, we can use the Hyperledger composer for designing the underlying architecture of private blockchain. Table 1 shows the modeling environment used in the beta phase. Hyperledger Fabric Version 1.4.1 is used to define the operating system. The operating system used for modeling is Ubuntu Linux 18.04.1 LTS.

The Fig. 5 shows the transactions list of blockchain transactions. The user can view the immutable date and time of any transaction. It also shows the entry type and relevant participant. It allows the user to view the extended information of any record as well.

Figure 6 shows the bar graphs of these three groups. The network diagram shows that as the number of users increases, the delay changes. However, this does not affect performance. The average values for 300, 400, and 500 user groups are 148, 215, and 342 ms. And at least 73, 79, and 124. The maximum quality difference for a group of 500 users with a length of 561 ms. The Latency for the get request

Fig. 4 Installation of Hyperledger Fabric

Table 1 Simulation setup

System component	Description
Operating system	Ubuntu Linux 18.04.1 LTS,
CPU	Intel ®Core ™ i5–8500 CPU at 3.00 GHz
Hyperledger Fabric	v1.4.1
Docker Engine	Version 18.06.1-ce
CLI Tool	composer-cli,
Docker-Composer	Version 1.13.0
Primary memory	16 GB RAM
Language	JavaScript
IDE (Platform)	Hyperledger composer-playground

transaction query evaluation results shows that the system will Indicates an increase in latency as the number of users increases [19].

6 Conclusion

This article uses a blockchain-as-a-service software package to describe and manage suspicious transactions in IoT systems. This research builds specific software components for blockchain functions to be implemented in IoT networks. This research is conducted using Hyperledger Fabric as a blockchain service to test software-defined blockchain components in the blockchain. We have used the transaction latency evaluation model to test the performance of the proposed system. We have confirmed that

Date, Time	Entry Type	Participant	
2020-06-24, 19:29:31	AddAsset	admin (NetworkAdmin)	view record
2020-06-24, 19:29:25	AddAsset	admin (NetworkAdmin)	view record
2020-06-24, 19:29:16	AddParticipant	admin (NetworkAdmin)	view record
2020-06-24, 19:29:12	AddParticipant	admin (NetworkAdmin)	view record
2020-06-24, 19:29:08	AddParticipant	admin (NetworkAdmin)	view record
2020-06-24, 19:29:04	AddParticipant	admin (NetworkAdmin)	view record
2020-06-24, 19:28:58	AddParticipant	admin (NetworkAdmin)	view record
2020-06-24, 19:28:49	AddParticipant	admin (NetworkAdmin)	view record
2020-06-24, 19:25:01	ActivateCurrentIdentity	none	view record
2020-06-24, 19:24:44	StartBusinessNetwork	none	view record

Fig. 5 List of transactions

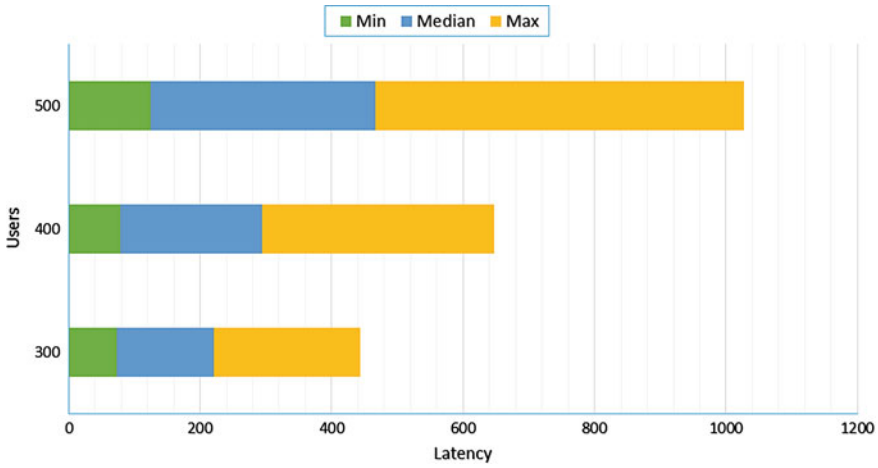

Fig. 6 Latency for the get request transaction query

using blockchain as a software service system can provide excellent performance and security. In the future, we aim to extend this work to do a practical implementation of the proposed method. We will also work on the specific use cases of the proposed transaction management system.

Acknowledgements This work was supported by Korea Institute for Advancement of Technology (KIAT) grant funded by the Korea Government (MOTIE) (N0002327, The Establishment Project of Industry-University Fusion District).

References

1. Novo O (2018) Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet Things J 5(2):1184–1195
2. Jiang Y, Wang C, Wang Y, Gao L (2019) A cross-chain solution to integrating multiple blockchains for IoT data management. Sensors 19(9):2042
3. Nyamtiga BW, Sicato JCS, Rathore S, Sung Y, Park JH (2019) Blockchain-based secure storage management with edge computing for IoT. Electronics 8(8):828
4. Jia X, Feng Q, Fan T, Lei Q (2012) RFID technology and its applications in Internet of Things (IoT). In: 2012 2nd international conference on consumer electronics, communications and networks (CECNet). IEEE, pp 1282–1285
5. Biswas S, Sharif K, Li F, Nour B, Wang Y (2018) A scalable blockchain framework for secure transactions in IoT. IEEE Internet Things J 6(3):4650–4659
6. Samaniego M, Jamsrandorj U, Deters R (2016) Blockchain as a service for IoT. In: 2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData). IEEE, pp 433–436
7. Samaniego M, Deters R (2019) Pushing software-defined blockchain components onto Edge Hosts. arXiv preprint arXiv:1909.09936
8. Luo J, Chen Q, Yu FR, Tang L (2020) Blockchain-Enabled software-defined industrial internet of things with deep reinforcement learning. IEEE Internet Things J
9. Oktian YE, Lee SG, Lee HJ (2020) Hierarchical multi-blockchain architecture for scalable internet of things environment. Electronics 9(6):1050
10. Samaniego M, Deters R (2018) Virtual resources & blockchain for configuration management in IoT. J Ubiquitous Syst Pervasive Networks 9(2):1–13
11. Samaniego M, Deters R (2018) Detecting suspicious transactions in iot blockchains for smart living spaces. In: International conference on machine learning for networking. Springer, Cham, pp 364–377
12. Samaniego M, Espana C, Deters R (2019) Suspicious transactions in smart spaces. arXiv preprint arXiv:1909.10644
13. Heilman E, Baldimtsi F, Goldberg S (2016) Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions. In International conference on financial cryptography and data security. Springer, Berlin, pp 43–60
14. Sukhwani H, Wang N, Trivedi KS, Rindos A (2018) Performance modeling of hyperledger fabric (permissioned blockchain network). In: 2018 IEEE 17th international symposium on network computing and applications (NCA). IEEE, pp 1–8
15. Choudhury O, Sarker H, Rudolph N, Foreman M, Fay N, Dhuliawala M, Das AK (2018) Enforcing human subject regulations using blockchain and smart contracts. Blockchain Healthc Today 1:1–14
16. Dittmann G, Jelitto J (2019) A blockchain proxy for lightweight IoT devices. In: 2019 Crypto valley conference on blockchain technology (CVCBT). IEEE, pp 82–85

17. Khan PW, Byun YC, Park N (2020) A data verification system for CCTV surveillance cameras using blockchain technology in smart cities. Electronics 9(3):484
18. Khan PW, Byun YC (2020) Smart contract centric inference engine for intelligent electric vehicle transportation system. Sensors 20(15):4252
19. Hang L, Kim DH (2019) Design and implementation of an integrated iot blockchain platform for sensing data integrity. Sensors 19(10):2228