A Study on Lightweight And Secure Edge Computing Based Blockchain

Wenzheng Li and Mingsheng He
Faculty of Information Technology
Beijing University of Technology
Beijing 100124, China
liwww@bjut.edu.cn

Wei Zhu,Jianchun Zheng
Beijing Research Center of Urban System Engineering
Beijing 100035, China

2021 IEEE 12th International Conference on Software Engineering and Service Science (ICSESS) | 978-1-6654-1506-4/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICSESS52187.2021.9522326

Abstract—**In response to the challenges faced by edge computing in terms of storage and security, we design a lightweight and secure edge computing architecture based on blockchain. First, we conducted in-depth research on lightweight communication protocols, and propose a lightweight communication model by combining Constrained Application Protocol (CoAP) and Message Queuing Telemetry Transport (MQTT). Second, in order to ensure the security and traceability of the data on edge computing node, we propose a novel data storage mechanism based on blockchain and InterPlanetary File System (IPFS). Finally, we design an improved scheme of the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm to improve the throughput of the system. The results show that the proposed edge computing architecture has the characteristics of strong robustness and low system overhead, which provides new ideas for promoting blockchain-based edge computing to become a key technology for upgrading Internet of Things (IoT) services.**

Keywords-edge computing; blockchain; messaging protocol; consensus algorithm; smart contract

I. INTRODUCTION

The rapidly development of Internet of Things (IoT) technologies offers new opportunities in various aspects of our daily lives, such as smart home, smart agriculture, and intelligent transportation [1]. According to Machina Research, IoT devices will exceed 27 billion by 2025. At the same time, the data collected by IoT devices will increase exponentially, it is expected that there will be more than 40 ZB of data in the IoT network [2]. Although cloud computing provides an efficient computing platform for big data processing, the current growth rate of network bandwidth is far behind the growth rate of data [3]. Besides, some IoT applications might require very short response time and some might involve private data. Thus, cloud computing is not efficient enough to support these applications [4].

Edge computing is a new computing model for computing at the edge of network [5]. The emergence of edge computing breaks the traditional centralized data processing mode of cloud computing. Compared with cloud computing, edge computing model has 4 obvious advantages [6]:

(1) The data generated by IoT devices are not all uploaded to the cloud center, but preprocessed on the edge server firstly. After preprocessing, a small amount of valuable data will be uploaded, which greatly alleviates the pressure on network bandwidth caused by the data generated by massive IoT devices.

(2) The data processing is carried out on edge devices with the help of the processor deployed on it, no longer relying on cloud computing center, which eliminates the data uploading link and the interaction link with cloud center and improves the response ability of the system.

(3) The sensitive data generated by users are stored on edge devices rather than in cloud data center, which reduces the risk of being stolen by lawbreakers.

(4) In the edge computing model, the data does not all need to be uploaded to the cloud computing center for processing, which not only reduces the energy consumption of transmission, but also greatly reduces the energy consumption of the cloud computing center.

At present, edge computing has been widely valued by all walks of life, and has made some achievements in many application scenarios. However, in terms of practical application, there are still many problems to be studied:

(1) *Data privacy protection and security*. In the field of public security, the privacy protection of data and security issues are particularly essential. A large number of widely distributed smart cameras capture civilian privacy information, and although these image data are preprocessed on edge devices, they are ultimately sent to cloud storage. If such information is obtained by lawbreakers, civilian lives and property will be threatened [7].

(2) *Device access.* Identity authentication refers to a security mechanism that identifies and authenticates devices connected to IoT system before data interaction, which is the first step in IoT security. The traditional identity authentication system uses centralized technology architecture that cannot adapt to the IoT environment with a large variety of devices and complex network structure, and it has the problem of potential single point failure [8].

(3) *Messaging protocol.* For constrained devices and complex network environment of IoT, the messaging protocol

978-1-6654-1506-4/21/$31.00©2021 IEEE

is one of the main factors that determine the performance of Machine-to-Machine (M2M) communication [9]. No single protocol can apply to all possible IoT cases, and the choice of messaging protocol becomes an ongoing dilemma.

The distributed structure of edge devices in edge computing has many similar characteristics with encrypted currency [10], so it is possible to solve above problems by using the blockchain technology behind it.

Blockchain is a kind of chained data structure which combines block data in chronological order [11]. As shown in Figure 1, each block in the blockchain contains a block header and a block body, where the block header contains version number, hash value of parent block, Merkel tree root, timestamp, random number, and difficulty number, and the block body contains transaction number and transaction set. All records of transactions are stored in the blockchain to form a decentralized distributed database. Such data structure makes blockchain have some significant characteristics such as decentralization, tamper proof, traceability and autonomy. According to different application scenarios, blockchain is divided into public blockchain, private blockchain, and permissioned blockchain [12]. In edge computing scenario, the entry and exit of edge nodes (blockchain nodes) are authorized, so there is almost no risk of doing evil. As a result, applying permissioned blockchain to edge computing is the best choice.

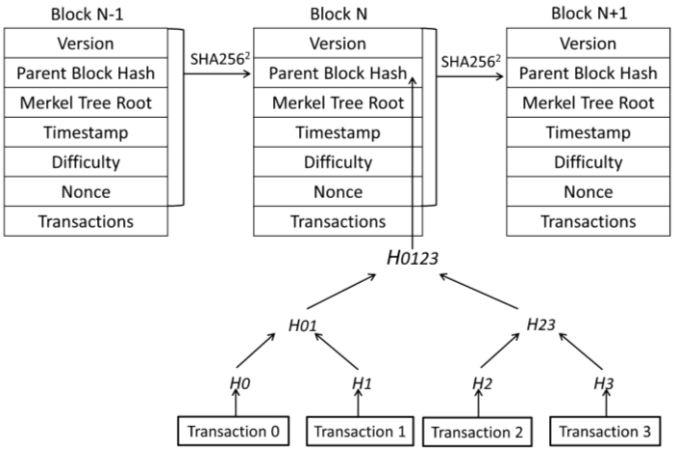

Fig. 1. Blockchain Structure

However, there are some issues that need to be addressed when introducing blockchain into edge computing:

(1) *Data storage.* In the Ethereum, the data stored in the blockchain means that data is put into the data field of the transaction. When the transaction is stored in the next new block, the data is permanently stored in the blockchain. However, there is a limit to the amount of data that can be carried by a transaction, which is about 44KB. Beyond this value, the transaction cannot be created successfully. Therefore, in order to improve the scalability of blockchain, a secure storage mechanism needs to be proposed.

(2) *Consensus algorithm.* As the core technology of blockchain, consensus algorithm is the key to ensure the consistency of distributed ledger data [13]. In edge computing scenario, Practical Byzantine Fault Tolerance (PBFT) algorithm that widely used in permissioned blockchain can be an alternative. As shown in Figure 2, PBFT algorithm achieves consensus through three-step broadcast communication and five stages. It not only ensures the security and activity of consensus network, but also provides (N-1)/3 maximum fault tolerance where N is the total number of nodes. However, PBFT algorithm has high communication cost and long consensus time. Thus, it is necessary to modify the PBFT consensus algorithm for edge computing applications.

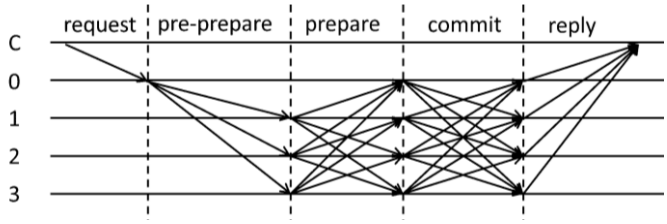

Fig. 2. PBFT Algorithm Consensus Process

(3) *Device identity authentication.* The identity authentication of devices is vital to the security of the IoT. In order to completely solve the security threat of identity authentication system, a decentralized and secure technical solution needs to be found [14]. Smart contract is a kind of decentralized and trusted program code deployed on the blockchain. Blockchain provides a trusted execution environment for smart contracts, and smart contracts expand the application of blockchain. As a result, the identity authentication of IoT devices can be completed based on the smart contract.

In this paper, we propose an edge computing system based on permissioned blockchain. The model uses permissioned blockchain, lightweight messaging protocols, improved PBFT consensus algorithm, smart contracts and InterPlanetary File System (IPFS) technology. Lightweight communication protocol solves the problem of reliable communication between IoT devices in edge computing scenarios. Blockchain combines with IPFS to ensure secure storage of data. Basic functions of the system are realized based on smart contracts. The improved PBFT consensus algorithm can enhance the throughput of the system.

The remainder of this paper is structured as follows: Section 2 introduces the relevant works in current state of art. Section 3 looks into the system architecture and key issues in the integration of edge computing and blockchain. Section 4 is the discussion of proposed edge computing system. Section 5 concludes the paper and discusses future work.

II. RELATED WORKS

At present, it is a natural trend to integrate edge computing and blockchain into one system [15]. The possibility of integration comes from the same distributed network infrastructure and the necessity of integration comes from their own merits and complementarity. The systems based on edge computing and blockchain aims at providing secure services to meet the application requirement by taking into consideration of network, storage, and computation [16].

There are two kinds of data communication in the integrated system, one is the communication between devices and edge nodes, the other is the communication between blockchain nodes [17]. The TCP-based Message Queuing Telemetry Transport (MQTT) and the UDP-based Constrained Application Protocol (CoAP) are two famous lightweight protocols, which are suitable for IoT applications [18]. [19] presented a system architecture for IoT based on the CoAP, which achieves high throughput. [20] proposed an distributed architecture combining MQTT and CoAP to enhance the scalability of gateways for the efficient IoT-cloud integration. [21] indicated that MQTT is more suitable for blockchain because of stable connection, where CoAP is appropriate for resource-constrained devices.

The size of transactions in blockchain is limited, so it is infeasible to store data in the blockchain directly [22]. [23] proposed a blockchain traceability system based on blockchain utilizing a data storage scheme combining blockchain and traditional database, which established the mapping relationship between transaction and product ID in the database so as to realize background logical operations. [16] indicated that compared with traditional database, decentralized storage systems like IPFS are more robust solution. [24] proposed a video surveillance system based on permissioned blockchain and edge computing which deployed IPFS to store videos.

[8] pointed out that the alternative model for authentication, authorization, and security protection based on blockchain is studied by scholars around the world. [25] proposed a collaborative architecture using smart contracts and blockchain to enable Distributed Denial-of-Service (DDoS) mitigation across multiple domains. [26] designed a fully distributed user authentication framework with blockchain. [27] proposed a blockchain-based trusted data management scheme to solve data trust and security issues in edge computing environment.

The above studies show that there are extensive researches on network, storage, device access, and data management in the integration of blockchain and edge computing. Our research mainly addresses the lightweight and security problems, one is the lightweight communication between nodes and the lightweight consensus algorithm, the other is the secure access of devices and the safe access of data.

III. Edge Computing System Based On Permissioned Blockchain

A. System Architecture

In this paper, we propose an edge computing system based on permissioned blockchain, lightweight IoT messaging protocols, improved PBFT consensus algorithm, and IPFS. Figure 3 represents the layered-based architecture of proposed edge computing system. It consists of three parts including perception layer, edge layer, and cloud layer.

1) Perception layer

The perception layer is composed of a large number of intelligent IoT devices which are responsible for collecting data. After the data collection, raw data will be encapsulated in JavaScript Object Notation (JSON) format and uploaded to the edge node through CoAP client module deployed on devices.

2) Edge layer

The edge layer consists of many edge servers. All edge servers are deployed with CoAP server module, MQTT client module, and blockchain node, therefore, edge nodes are also blockchain nodes. One of the edge nodes should be deployed with MQTT broker module to be responsible for the message scheduling between edge nodes and between edge layer and cloud layer. Edge layer processes the data transmitted from the perception layer and stores it into the blockchain through the consensus mechanism. At the same time, some smart contracts stored on the blockchain will be used to realize vital functions of the platform.

3) Cloud layer

The cloud layer is composed of IPFS and cloud server deployed with MQTT client module, which is used to store large files like videos. Edge layer will transfer the data that cannot be directly stored in the blockchain to cloud layer through MQTT protocol for storage. When storing data, cloud server will add large file to IPFS and get the hash value of it. File hash values are stored in the blockchain and used for file queries.

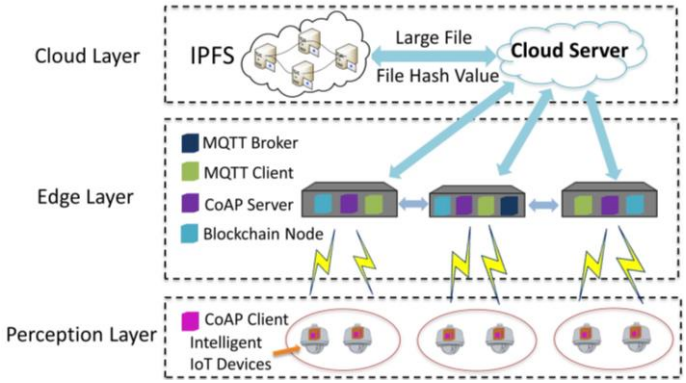

Fig. 3. System Architecture

B. Lightweight PBFT Consensus Algorithm

In order to solve the problem that PBFT consensus algorithm has high requirements for network bandwidth and high communication overhead, we propose to put forward a network model based on the clustering algorithm, in which consensus nodes are logically clustered by two layers and many groups. Figure 4 represents the logical architecture of consensus nodes. All nodes in blockchain network are divided into two categories: the primary consensus node and the secondary consensus node. All primary consensus nodes form the primary consensus cluster, and all secondary consensus nodes are divided into several secondary consensus clusters by clustering algorithm. The number of primary consensus nodes is equal to the number of secondary consensus clusters, in another words, each primary consensus node corresponds to a secondary consensus cluster.

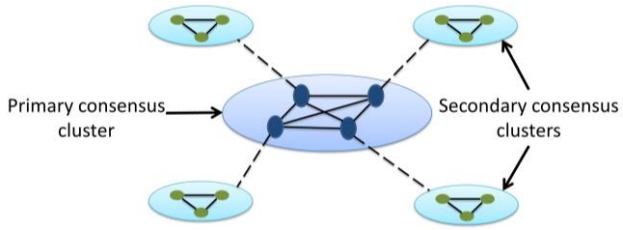

Fig. 4. Logical Architecture of Consensus Nodes

Based on above consensus node model, the process of consensus should also be improved. The improved consensus process is shown in Figure 5.

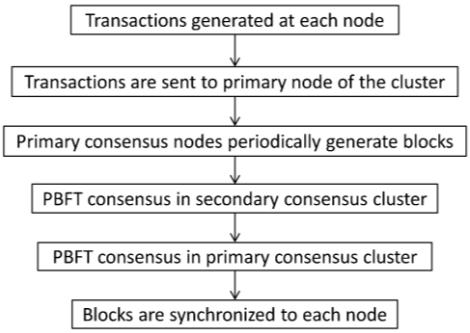

Fig. 5. Improved PBFT Consensus Process

C. Smart Contract

The business logic of proposed edge computing system is defined by the smart contract in order to ensure that functions are performed in a safe manner.

1) Device authentication

We defined three types of smart contracts to ensure the security of device identity authentication. They are device registration contract, identity authentication contract, and integrity verification contract. Before enrolled in the blockchain, each device generates a key pair by key model. The private key is stored locally, while other vital information like device ID, public key, and hash of essential data is stored in the blockchain by calling the device registration contract. When a device needs to access the network, it will provide its device ID and a message signed by its private key including the hash value of critical information. Then, the identity authentication contract will search whether the corresponding public key exists in the blockchain according to the device ID to determine device's validity. After authentication, verification contract will be verify the integrity of the hash value to detect potential intrusion.

2) Data storage

The function of data storage contract is to store regular data fields or the hash value of large files into the blockchain. The work flow of data storage in proposed system is shown in Figure 6 and the specific process is elaborated as follows:

a) After the intelligent IoT device passes the identity authentication, it encapsulates the collected data into JSON format and transmits it to edge device.

b) Edge device receives the data from perception layer and transmits the files whose size exceeds a certain threshold to cloud layer.

c) Cloud server adds large files to IPFS and gets the file hash value which needs to be passed back to edge device.

d) Edge servers add the hash value of large file to the original JSON format data to generate new data. Edge servers call the data storage contract and pass in the parameter (new data). After the transaction passes consensus algorithm, the new data is stored in the blockchain, and the transaction hash value (transaction ID) is obtained.

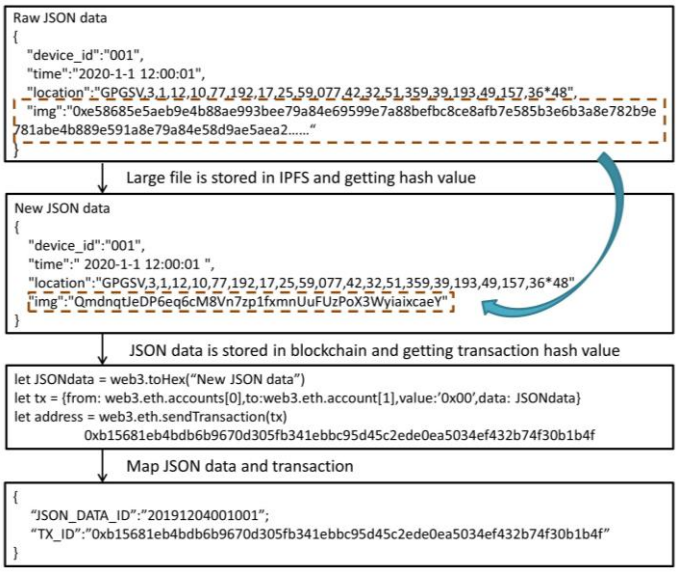

Fig. 6. Data Storage Work Flow

3) Data query

After end users complete authentication and obtain the data access right, the edge server can call data query contract. The function of data query contract is to obtain data according to transaction ID. The specific process of data query is as follows:

a) Edge server calls data query contract and pass in the parameter (transaction ID) in order to obtain file hash value.

b) Edge server sends the file hash value to cloud server.

c) Cloud server retrieves the specific file in IPFS through file hash value, verifies the file and downloads it to the edge server.

d) Edge server sends data to end user finally.

IV. Discussion

In this paper, we propose an edge computing system based on permissioned blockchain and adopt lightweight IoT messaging protocols. As a bridge between intelligent IoT devices and storage in cloud, edge computing system ensures the legal access of terminal devices and the security of data access. Compared with the existing edge computing systems, our scheme has more technical advantages.

A. Robustness

CoAP and MQTT are the communication protocols used among all layers of proposed system, which are widely used in the IoT scenarios with limited resources and restrained network environment where connection is broken frequently. Three different Quality of Service (QoS) levels of MQTT protocol guarantee the reliability of the message and the use of TCP ensures the stability of the connection. CoAP runs on unreliable UDP protocol but uses retransmission mechanism to make up for this shortcoming.

B. Security

In traditional IoT system, the identity authentication of IoT terminal devices depends on a trusted third party. This centralized authentication method is vulnerable to internal and external attacks, which leads to single point failure, data tampering, and other security problems. In proposed system, we come up with an identity authentication method of terminal device based on smart contract to prevent unregistered device accessing to edge layer.

C. Data Privacy Protection

The data collected by physical devices is not transmitted to data center for centralized storage. Instead, we adopt the strategy of storing hash values in blockchain ledger and storing files in the IPFS deployed in cloud to prevent illegal access to privacy data.

D. Traceability

IPFS storages data permanently and provides version traceability. Any small changes of a file can be checked by version. Not only data will not be lost, but also all details will be retained. Moreover, all operations of end devices and users are recorded in blockchain ledger in the form of transactions and cannot be changed. Therefore, proposed system can prevent data from being tampered with maliciously, locate the data source accurately, and identify users who request or modify data.

E. Cost

In the preparation and commit stage of traditional PBFT consensus algorithm, all consensus nodes need to interact with each other. When the total number of consensus nodes in network is 750, the number of communications that needed to complete a consensus process is 1123500, reaching the order of millions, which will greatly increase the consensus time and communication overhead. As for our proposed lightweight PBFT consensus algorithm scheme, theoretical proof and previous experiments show that it can reduce the number of communication times of three orders of magnitude, dramatically shorten the time-consuming of consensus process and improve the efficiency of consensus. In addition, the slice random distributed storage adopted in IPFS greatly reduces the bandwidth pressure of the servers, saves at least 60% of the bandwidth resources, and improves the transmission speed.

V. CONCLUSION

In this paper, we proposed a novel edge computing system based on permissioned blockchain network. We defined the system architecture and a new messaging model based on CoAP and MQTT. In order to apply PBFT consensus algorithm to IoT scenario, we propose an improved scheme of PBFT based on clustering algorithm. IPFS is utilized to improve the expandability of blockchain and ensure data security and traceability. In addition, we use a device authentication mechanism based on smart contract to guarantee the safe access of IoT devices.

This work realizes the organic integration of edge computing and blockchain, providing a new idea to address scalability, authentication, and data security challenges of IoT system. Future research directions aim at evaluating the actual performance of proposed system and improve the functions for various applications continuously.

ACKNOWLEDGMENT

The authors appreciate the financial support of BJAST Youth Scholar Program （YS201901）

REFERENCES

[1] Shabir A , Lei H and Do K, "Design and Implementation of Cloud-Centric Configuration Repository for DIY IoT Applications," in *Sensors*, vol. 18, no. 2, pp. 474, 2018.

[2] Zwolenski, Matt and L. Weatherill, "The Digital Universe Rich Data and the Increasing Value of the Internet of Things," in Australian Journal of Telecommunications & the Digital Economy, vol. 2, no. 3, 2014.

[3] Zhao Ziming, Liu Fang, Cai Zhiping and Xiao Nong, "Edge Computing:Platforms, Applications and Challenges," in Journal of Computer Research and Development, vol. 55, no. 2, pp. 327-337, 2018.

[4] W. Shi, J. Cao, Q. Zhang, Y. Li and L. Xu, "Edge Computing: Vision and Challenges," in IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637-646, Oct. 2016.

[5] Shi Weisong, Sun Hui, Cao Jie, Zhang Quan and Liu Wei, "Edge Computing——An Emerging Computing Model for the Internet of Everything Era," in *Journal of Computer Research and Development*, vol. 54, no. 5, pp. 907-924, 2017.

[6] ZHENG Fengbin, ZHU Dongwei, ZANG Wenqian, YANG Jinlin and ZHU Guanghui, "Review and Application Research on A New Computing Paradigm：Edge Computing," in *Journal of Frontiers of Computer Science and Technology*, vol. 44, no. 11, pp. 2011-2022, 2018.

[7] ZHUANG Xiao-jun, YANG Bo, WANG Xu, PENG Jin and China Mobile Research Institute, "Approach on mobile edge computing security," in Telecom Engineering Technics and Standardization, vol. 31, no. 12, pp. 38-43, 2018.

[8] D. Li, W. Peng, W. Deng and F. Gai, "A Blockchain-Based Authentication and Security Mechanism for IoT," *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, Hangzhou, 2018, pp. 1-6.

[9] N. Naik, P. Jenkins, P. Davies and D. Newell, "Native Web Communication Protocols and Their Effects on the Performance of Web Services and Systems," *2016 IEEE International Conference on Computer and Information Technology (CIT)*, Nadi, 2016, pp. 219-225.

[10] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," in *IEEE Access*, vol. 6, pp. 32979-33001, 2018.

[11] A. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," *2016 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, 2016, pp. 839-858.

[12] Yang Yuguang and Zhang Shuxin, "Review and Research for Consensus Mechanism of Block Chain," in *Journal of Information Security Research*, vol. 4, no. 4, pp. 369-379, 2018.

[13] YUAN Yong, NI Xiao-Chun, ZENG Shuai and WANG Fei-Yue, "Blockchain Consensus Algorithms: The State of the Art and Future Trends," in *Acta Automatica Sinica*, vol. 44, no. 11, pp. 2011-2022, 2018.

[14] LI Ceng and XU Ji-cheng, "A Decentrolized Identity Authentication Model," in *Journal of Eastern Liaoning University(Natural Science Edition)*, vol. 27, no. 1, pp. 62-72, 2020.

[15] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues and K. Ko, "Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues," in *IEEE Access*, vol. 6, pp. 1513-1524, 2018.

[16] R. Yang, F. R. Yu, P. Si, Z. Yang and Y. Zhang, "Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1508-1532, Secondquarter 2019.

[17] C. Li and L. Zhang, "A Blockchain Based New Secure Multi-Layer Network Model for Internet of Things," *2017 IEEE International Congress on Internet of Things (ICIOT)*, Honolulu, HI, 2017, pp. 33-41.

[18] J. Huang, P. Tsai and I. Liao, "Implementing publish/subscribe pattern for CoAP in fog computing environment," *2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, BC, 2017, pp. 198-203.

[19] M. Kovatsch, M. Lanter and Z. Shelby, "Californium: Scalable cloud services for the Internet of Things with CoAP," *2014 International Conference on the Internet of Things (IOT)*, Cambridge, MA, 2014, pp. 1-6.

[20] P. Bellavista and A. Zanni, "Towards better scalability for IoT-cloud interactions via combined exploitation of MQTT and CoAP," *2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI)*, Bologna, 2016, pp. 1-6.

[21] He Bai, Yue Jiang, Hui Yang and Geming Xia, "The Messaging Protocols Analysis of Integrating Blockchain and Edge Computing for IoT," 2019.

[22] S. Raval, *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology*. Sebastopol, CA, USA: O'Reilly Media, 2016.

[23] ZHANG Yanhua, YANG Zhaoxin, YANG Ruizhe, JIN Kai, LIN Bo and SI Pengbo, "Traceability System of Farm Produce Based on Blockchain," in *Technology Intelligence Engineering*, vol. 4, no. 3, pp. 4-13, 2020.

[24] R. Wang, W. Tsai, J. He, C. Liu, Q. Li and E. Deng, "A Video Surveillance System Based on Permissioned Blockchains and Edge Computing," *2019 IEEE International Conference on Big Data and Smart Computing (BigComp)*, Kyoto, Japan, 2019, pp. 1-6.

[25] Bruno Rodrigues, Thomas Bocek, Andri Lareida, David Hausheer, Sina Rafati and Burkhard Stiller, "A Blockchain-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts," *IFIP International Conference on Autonomous Infrastructure, Management, and Security*, Springer, Cham, 2017, pp. 16-29.

[26] L. Zhang, H. Li, L. Sun, Z. Shi and Y. He, "Poster: Towards Fully Distributed User Authentication with Blockchain," *2017 IEEE Symposium on Privacy-Aware Computing (PAC)*, Washington, DC, 2017, pp. 202-203.

[27] M. Zhaofeng, W. Xiaochang, D. K. Jain, H. Khan, G. Hongmin and W. Zhen, "A Blockchain-Based Trusted Data Management Scheme in Edge Computing," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2013-2021, March 2020.