Proceedings of 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN 2018)

Edge Computing and Caching based Blockchain IoT Network

Fangmin Xu, Fan Yang, Chenglin Zhao
Key Lab. of Universal Wireless Communications, MOE
Beijing University of Posts and Telecommunications,
No.10 Xitucheng Road, Beijing, China

Chao Fang
Faculty of Information Technology
Beijing University of Technology
Beijing, P.R. China

***Abstract*—With the development of internet of things (IoT) network in recent years, while the centralization data management brings longer delay while has more safety troubles. Moreover, once a single device is attacked, the system crashes. So, blockchain technique which could realize safety distributed data management is introduced. However, the consensus mechanism of blockchain consumes huge computation resources. And the storage of entire ledger also consumes huge storage resources of the blockchain nodes. Due to the limited capacity of IoT devices, the nodes cannot afford the computation resources to reach consensus and caching resources. This paper introduces an architecture of edge computing based blockchain network which makes use of the computation and caching capacity of edge server to help the IoT devices in reaching consensus and storing data.**

Keywords—internet of things, blockchain, edge computing, computation, caching

I. INTRODUCTION

Blockchain is an emerging technology with the features of decentralization, tamper-resistant which could guarantee the safety record of transactions [1]. First, blockchain can be distributed to various equipment which effectively avoid the problem of single node failure leads to entire network collapse. Moreover, blockchain is tamper-resistant. This means once the transaction is recorded in the ledger, it cannot be changed or deleted. Finally, each block contains the hash value of previous block which makes the records of blockchain ledger is traceability. By using blockchain techniques in IoT, the collected data can be stored safely. And each transaction are traceability. Moreover, the smart contract mechanism of blockchain makes transaction between IoT devices more intelligence and reliable.

Although blockchain brings many benefit to IoT network, it consumes huge computation and storage resources. However, blockchain devices cannot afford the resource consumption. So, this paper introduces an architecture of edge computing based blockchain network which makes use of the computation and caching capacity of edge server to help the blockchain devices in reaching consensus and storing data. Edge computing (EC) can help devices calculate and store blocks. The devices could only verify whether the result is correct and the edge server is credible.

II. RELATED WORK

Mobile edge computing has been introduced for data storage and decision making in IoT for a long time. Frameworks that offers secure and efficient edge computing for IoT applications are proposed in [2][3].

978-1-5386-4870-4/18/$31.00 ©2018 IEEE

To reach a consensus of all nodes and securely store the data in the system. Many researches focus on using blockchain to store data in IoT network. Many blockchain-based IoT system with secure storage and homomorphic is proposed in [4][5]. However, it assumes that all blockchain has enough calculation and storage resources. This limits the device type of the blockchain nodes [6].

By introducing edge computing based blockchain system to store data in IoT network, the system could store data safety with high throughput.

III. EDGE COMPUTING BASED BLOCKCHAIN NETWORK

As shown in Fig.1, system is consisted of four parts which includes IoT network, blockchain network, edge server and external network.

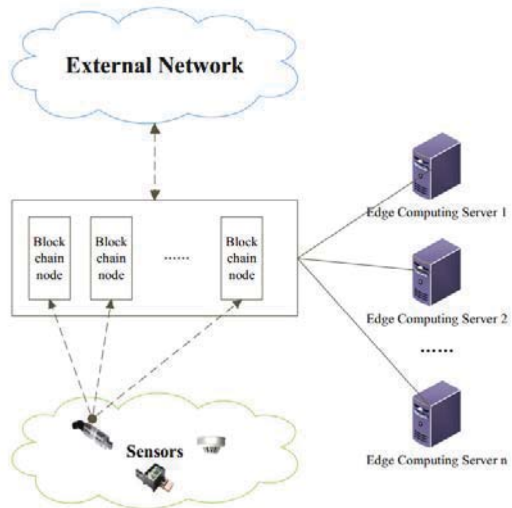

Fig. 1. Edge computing based blockchain network architecture

A. The architescture

IoT network is responsible for data collection and upload the data to nearest blockchain devices.

Blockchain network is based on P2P communication network. Each blockchain node includes consensus module, access module, identification module and inspection module as shown in Fig.2. The consensus module is responsible for reaching a consensus. In public blockchain network, consensus mechanism consumes huge resources. For example, proof of work (PoW) is always used as the consensus mechanism which consumes huge computation resources. The goal is to make all distrusted nodes reaching a consensus and keep consistent blockchain views. Access module responsible for judging the access rights and access

The project is supported by the Key Program of the National Natural Science Foundation of China (Grant No 61431008), Intelligent Manufacturing Integrated Standardization and New Model Application Project, Beijing Natural Science Foundation under Grant 4174081.

modes of external network visitors. It outputs data and generates access records. Identification module is responsible for broadcasting the unique identifier of the blockchain node on the blockchain platform, and stores the unique identifier of the blockchain node after the consensus is reached. Inspection module is responsible for detecting any malicious third party from tampering with the data.

Edge servers have high computing power, which is used to cooperate with the blockchain node in the difficult Hash value calculation solving, and return the calculation results to the blockchain node for verification. Edge server could also help the devices with storing data.

External network can access the data stored in blockchain as a third party. Different devices in external network could obtain different permissions which is controlled by access module in blockchain nodes.

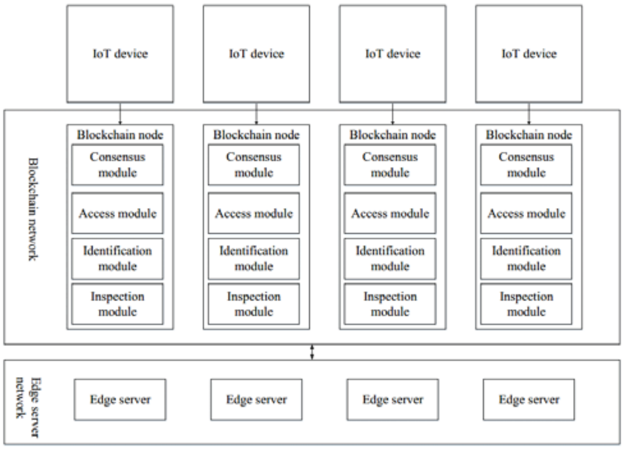

Fig. 2. Functionality architecture of the system

B. *Computation offloading*

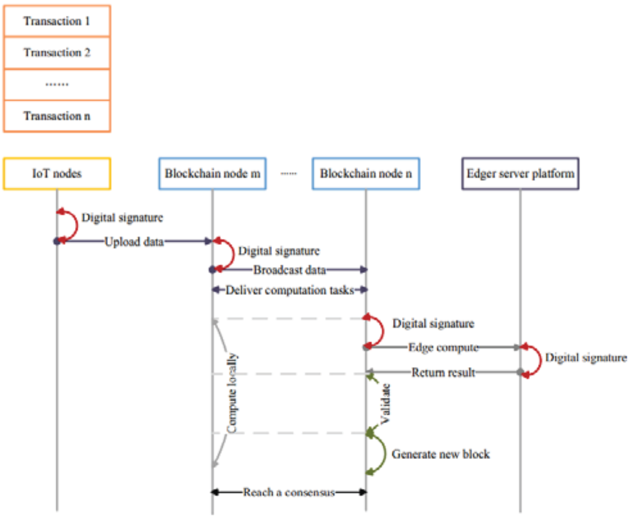

Fig. 3. Computation offloading process

The computation offloading process is shown in Fig.3. The IoT devices collect data and upload the data to nearest blockchain node m. Blockchain node *m* will broadcast the data to all P2P blockchain nodes. Then network delivers a computation task which means all nodes need to calculate a sha256 value. Blockchain nodes will compare the time consumption between local calculation and computation offloading which needs to consider the mission requirements, local computing capabilities, edge server capabilities, transmission delay and queueing delay at edge server side comprehensively. In Fig.3 blockchain node *m* decides to compute locally and blockchain *n* decides to offload the mission to edge server. In Fig.3 blockchain *n* offloads the mission to edge server after digital signature the mission. The edge server validates the signature and performs the calculation then returns the result to blockchain node *n*. Node *n* validates the result, if the result is correct then node *n* generates new block and broadcast to all nodes. The nodes received the new block, then validate the block and if it is legal then add the block to the blockchain.

C. *Caching offloading*

When the consensus is reached, the blockchain nodes add the new block to the end of blockchain. If the node have enough storage, it stores the blockchain in its own internal storage. If the node does not have enough internal storage, then it could offload whole blockchain to the edge server and only store relatively new blocks in the internal storage.

D. *Access data*

When external network devices need to acquire data or transactions from blockchain, devices access to the nearest blockchain node and the access module in the node will identify the rights of the devices and gives different access mode. There are two access mode: general mode and smart contract mode. If the query operation triggers the smart contract, then the program will execute automatically. And the access will be recorded in the blockchain.

IV. Conclusion

Due to the increasing amount of IoT devices deployed in the network, generous data are generated. To store the data and transaction between different devices safely, this paper introduced edge computing based blockchain network. The architecture could not only make consensus and store the data, but also could have high throughput by introducing edge computing.

References

[1] J. C. Cheng, N. Y. Lee, C. Chi and Y. H. Chen, "Blockchain and smart contract for digital certificate," *2018 IEEE International Conference on Applied System Invention (ICASI)*, Chiba, Japan, 2018, pp. 1046-1051.

[2] S. Almajali, H. B. Salameh, M. Ayyash and H. Elgala, "A framework for efficient and secured mobility of IoT devices in mobile edge computing," *2018 Third International Conference on Fog and Mobile Edge Computing (FMEC)*, Barcelona, 2018, pp. 58-62.

[3] S. Li and J. Huang, "Energy Efficient Resource Management and Task Scheduling for IoT Services in Edge Computing Paradigm," *2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC)*, Guangzhou, 2017, pp. 846-851.

[4] L. Zhou, L. Wang, Y. Sun and P. Lv, "BeeKeeper: A Blockchain-based IoT System with Secure Storage and Homomorphic Computation," in *IEEE Access.*

[5] M. Singh, A. Singh and S. Kim, "Blockchain: A game changer for securing IoT data," *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, Singapore, 2018, pp. 51-55.

[6] C. Fang, F. R. Yu, T. Huang, J. Liu, and Y. Liu, "A survey of green information-centric networking: research issues and challenges," Commun. Surveys Tuts., vol. 17, no. 3, pp. 1455–1472, 2015.