Proceedings of the Seventh International Conference on Research in Intelligent and Computing in Engineering pp. 141–144 DOI: 10.15439/2022R17 ISSN 2300-5963 ACSIS, Vol. 33

Proof-of-Miner-Clustering-Authentication Consensus Method of Blockchain for IoT Networks

1st Tam T. Huynh
Faculty of Information Technology
Posts and Telecommunications Institute of Technology Ho Chi Minh City,
Vietnam tamht@ptithcm.edu.vn

2st Chinh N. Huynh
Faculty of Information Technology
Ho Chi Minh City University of Technology and Education Ho Chi Minh City, Vietnam
chinhhn@fit.hcmute.edu.vn

3st Thanh H. Nguyen
Faculty of Information Technology
Posts and Telecommunications Institute of Technology
Ho Chi Minh City, Vietnam
thanhnh@ptithcm.edu.vn

***Abstract*—Using blockchain technology in the Internet of Things (IoT) security is a research trend in recent years. With large IoT networks, miners will have to verify a lot of transactions broadcast from IoT devices. This can cause a delay in saving valid transactions to the ledger. This paper proposes a proof-of-miner-clustering-authentication consensus method of blockchain for IoT networks. In the proposed method, miners in a blockchain network will be clustered, each miner in a cluster is responsible for verifying transactions from IoT devices in the area it manages. Mining of new blocks between clusters is done by the round robin method. Our consensus method can apply to private or consortium blockchain networks, helping to improve the transaction verification speed of miners.**

***Index Terms*—blockchain, IoT, consensus.**

I. Introduction

In today's rapidly developing digital technology era, the number and types of IoT devices being put into use are increasing day by day. The International Data Corporation forecasts the quantity of Internet-connected IoT devices reach 150 billion by 2025 [1]. Security for IoT networks are very important and urgent nowadays. With the current development trend of IoT, the use of a security platform based on blockchain for large IoT networks with high scalability needs is a suitable solution, because this technology has many advantages, such as decentralization, anonymity, and accountability [2-3].

In 2008, Satoshi Nakamoto introduced blockchain technology, which is a block-linked list [4]. Each block has a hash pointer that connects it to its parent block and stores the predecessor's hash value at a specific time. Genesis block is the name of the chain's initial block. A block structure includes a header which contains information management of the block, and a body containing valid transactions.

A blockchain network has two types of nodes: user nodes and miner nodes. Transactions can be carried out by User nodes, meanwhile, Miners hold the ledger that records a series of verified blocks. A consensus protocol is used in a blockchain network to synchronize ledger data between miners. Some consensus protocols include Proof-of-work (PoW), Proof-of-stake (PoS), Proof-of-activity (PoA) [5]. Blockchain is classified into three types: public blockchain, private blockchain, and consortium blockchain [6].

Regarding the management model of an IoT network, usually an IoT network is managed by one or several organizations. In the case of an IoT network managed by an organization, the organization can set up a private blockchain for the security platform. In case the IoT network is managed by several organizations, a consortium blockchain can be used for the security platform. Two important components in a blockchain network are miners and a consensus protocol. Miners need high computing performance and large enough storage capacity to verify transactions and store data for the entire network. The consensus mechanism is used in a blockchain network to synchronize data on the miners' ledger.

Normally, the data consensus process in a blockchain network is as follows: (1) when a node in a network performs a blockchain transaction, the transaction is broadcast to all network-connected miners; (2) These transactions will be saved in each miner's pool; (3) in each cycle of mining, a miner verifies and places valid transactions in a new block. The other miners will be informed about this new block, and this miner will also save this new block in its ledger; (4) after receiving this new block, the miners check the block's legitimacy, and if it is true, they add it to their ledger. Obviously, given the large size of IoT networks both in terms of the number of devices and geographic coverage, miners will receive and process a lot of transactions. This can cause delays in saving valid transactions to the blockchain ledger.

There have been many consensus methods applied to blockchain for IoT such as PoW, PoS, PoAh [10, 11, 16]. However, solutions using these consensus methods have not been mentioned to apply to large IoT networks. Therefore, this paper proposes a novel consensus approach based on the clustering of miners. The proposed method can be applied to large IoT networks both in terms of the number of devices and geographic coverage. In this method, miners in a private network or consortium blockchain will be grouped into multiple clusters, miners in each cluster will be responsible for verifying transactions from IoT devices in the area that the cluster manages. The proposed method helps to speed up the transaction verification and data consensus on the blockchain ledger.

The remainder of this paper is organized as follows. Section II reviews the related works. Section III describes the proposed method. Finally, our conclusion and future works are given in Section IV.

II. Related Works

Oscar Novo proposed a blockchain-based access control architecture for IoT. In this architecture, Management Hubs are used to manage IoT devices and act as a bridge between IoT devices and the blockchain network. The proposed architecture uses Ethereum for the private blockchain network [7]. Liu et al. [8] introduced a platform that ensures the integrity of IoT data stored on a cloud storage service, this secure platform uses the Ethereum blockchain. Panda et

al. [9] proposed an authentication platform for IoT devices that uses the Ethereum blockchain. Sheron et al. [10] proposed a secure platform that provides a communication method that ensures privacy and integrity in the IoT environment, which uses the PoW consensus protocol.

The authors in [11] introduced a secure communication platform for IoT networks. The platform is implemented in the consortium blockchain network and uses a combined consensus algorithm. Overall, this consensus algorithm is similar to the PoS consensus protocol. Currently, the PoW consensus mechanism on the Ethereum blockchain is being replaced by the PoS consensus protocol since it uses quite a lot of electrical energy and processing resources[12]. Li Yang et al. [13] proposed a distributed consensus algorithm for blockchains on multi-hop IoT networks. The authors in [14] introduced a model that makes the consensus approach more energy efficient, utilizes less memory, and less processing time. Manal Mohamed Alhejazi et al. [15] presented Weighted Majority Consensus Algorithm for IoT systems.

The general architecture of the blockchain network of the solutions surveyed above is that all miners are not clustered, so all transactions from IoT devices propagate to all miners in the network. Therefore, when the IoT network size increases in both the number of connected devices and the geographic coverage, miners will have to process a large number of transactions in the network. This can greatly affect the processing performance of miners and can cause delays in saving transactions on the blockchain ledger. Moreover, blockchain networks that use the PoW consensus protocol, it is costly in terms of electrical energy consumed by miners and is not suitable for private networks or blockchain consortiums.

III. THE PROPOSED CONSENSUS METHOD

A. System Model

Figure 1 illustrates the architecture of a blockchain network for IoT, consisting of three clusters. Each of clusters has two miners and IoT devices, clustering can be based on the geographical location of miners in the network. The number of clusters and miners in each cluster is determined by the size of the IoT network. Administrator is possible to add IoT devices to the clusters.

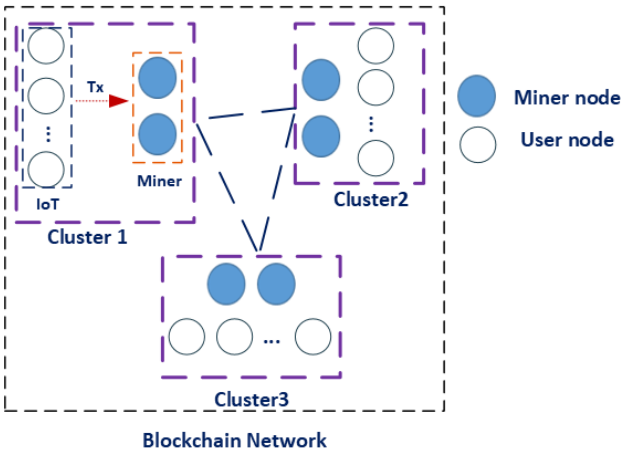

Fig. 1. The system model.

The system has two kinds of nodes:

- Miner Node: Miners in a cluster verify the transactions of IoT devices in that cluster, can create new blocks on the blockchain ledger.
- User Node: Each IoT device is a User Node in the blockchain network and can perform blockchain transactions on the network.

B. System Policies

The policies are implemented on miner nodes and user nodes as follows:

- Miner Node: Each miner maintains a list containing the communication addresses of other miners and a list of blockchain addresses of miners in the blockchain network. The administrator will configure this list on the miners.
- User Node: Each IoT device in a cluster knows the addresses of the miners in that cluster. When an IoT device in a cluster performs a transaction, the transaction is broadcast only to the miners in its cluster.

C. System Setup

In this work, it is denoted that $PCS(x,k)$ is a public-key cryptosystem with a message x and a key k. H is a cryptographic hash function. Symbol $||$ is an operation of string concatenation. Let n be the number of miners in the network, and m be the number of IoT devices.

Each node in the system is generated a key pair by a public key cryptographic algorithm. Specifically, $PK_{m[i]}$ and $SK_{m[i]}$ are the public key and the corresponding private keys of the i-th miner, $0 < i \leq n$; $PK_{d[j]}$ and $SK_{d[j]}$ are the public key and the corresponding private key of the j-th IoT device, respectively, $0 < j \leq m$. In the blockchain network, miners and IoT devices use their private keys to create digital signatures and their public key as their blockchain address. The administrator also generates a public blockchain transaction address that is shared by the whole system, denoted SYS_Add. We denote $L = (PK_{m[1]}, PK_{m[2]}, \ldots, PK_{m[n]})$ as a list of miners' blockchain address in the network.

D. Consensus method

The consensus method includes three steps as follows:

- Step 1: an IoT device $d[j]$ performs a blockchain transaction, this device uses its private key to create a digital signature on that transaction, then this transaction along with the digital signature will be broadcast to the miners in its cluster.

  (i) The structure of a transaction as follows: *Tx={"Sender":<Blockchain_Address_of_Sender>, "Receiver":< <Blockchain_Address_of_Receiver>, "Content":<Content_of_Transaction>}.*

  (ii) Generating digital signature:

  $$h \leftarrow H(Tx)$$

  $$Sig \leftarrow PCS(h, SK_{d[j]})$$

  (iii) Broadcasting $(Tx||Sig)$ to miners in its cluster.

- Step 2: At a mining round, a selected miner $m[i]$ in the cluster will verify the signature on the received

transactions (in its pool), if the digital signature is valid, the transaction will be considered valid. This miner puts valid transactions in a new block, then forms a digital signature on this new block and distributes it to other miners in the network along with the digital signature. Note that the number of transactions in a block is determined by the size of each transaction as well as the system policies for each specific application.

(i) Verifying Tx:

$$h \leftarrow PCS(Sig, PK_{d[j]})$$

Where $PK_{d[j]}$ is the sender address field of Tx

$$h' \leftarrow H(Tx)$$

$$True/False \leftarrow (h' == h)$$

(ii) Creating a new block denoted b.

(iii) Generating digital signature on b

$$h\_b \leftarrow H(b)$$

$$Sig\_b \leftarrow PCS(h\_b, SK_{m[i]})$$

(iv) Broadcasting $(b||Sig\_b)$ to other miners

- Step 3: After receiving a new block along with a digital signature, the miners verify: (1) verify digital signature; and (2) Verify the miner who advertises this new block is on the list of miners in the network. If these two conditions are met, this new block will be added to the miners' ledger.

(i) Verifying digital signature:

$$h\_p \leftarrow PCS(Sig\_b, PK_{m[i]})$$

$$h'\_p \leftarrow H(b)$$

$$True/False \leftarrow (h\_p == h'\_p)$$

(ii) Verifying $PK_{m[i]}$ in L:

$$True/False \leftarrow (PK_{m[i]} \in L)$$

The proposed consensus process is shown in Fig. 2.

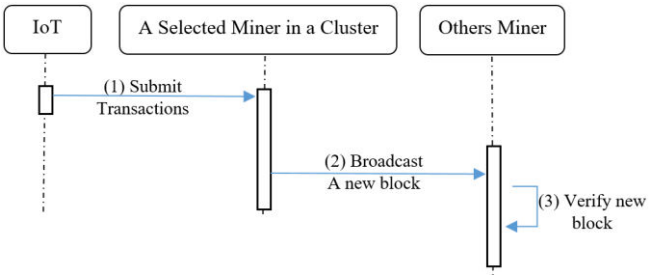

Fig. 2. The process of consensus method.

E. Mining round setup

As mentioned in Step 2 of the consensus method, at each mining round, a miner will be selected for a new block proposal. In this section, we will detail how to select miners at each cluster and when to start a mining round.

For the time to start a mining round: we assume that Δt is the time it takes for miners in a cluster to receive and verify a new block which broadcasts from a miner of the other cluster. we also assume that the computing power of each miner is the same. Proposing new blocks on the ledger will be done in the round robin method between clusters with the quantum time Δt. Specifically, the first block will be proposed by a miner in cluster 1. the second block will be done by a miner of cluster 2, the third block will be proposed by a miner in cluster 3, cluster 1 will propose the 4th block, and so on. New blocks will be proposed every Δt time. The round robin mining of clusters is shown in Figure 3.

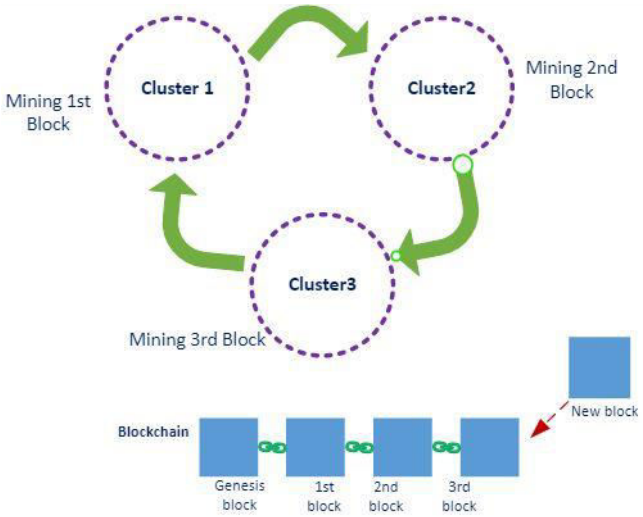

Fig. 3. The round robin mining of clusters.

The field "*Cluster_Number*" in the block header will be used to contain the cluster number that the block has mined, as shown in Figure 4.

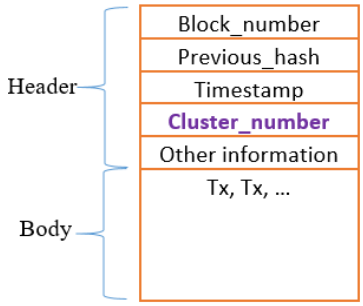

Fig. 4. The block structure.

For selecting a miner at each cluster: the administrator can use PoS consensus mechanism in the clusters, in which a fixed miner in each cluster will be selected to verify transactions and propose new blocks. In case something goes wrong with the selected miner, the administrator can transfer the mining role to another miner.

F. Discussion

Our consensus protocol is predicated on the authenticity of the event source. Specifically, IoT devices must sign on their transactions. Miners in the cluster verify the signature on that transactions; After mining a new block, the miner generates a signature on that block, then broadcast them to other miners in the network. The signature on the new block is used to verify the validation of the block.

Miners are divided into clusters by geographical area, each of which will manage the transactions of those central IoT devices. That improves mining speed in large IoT networks. However, all miners in the proposed blockchain architecture are honest miners. This means that it is very

difficult for miners to be compromised by attackers and they also do not commit any fraud in the blockchain network.

IV. Conclusion and Future Work

This paper proposes a new consensus method of blockchain for IoT networks, it is named Proof-of-Miner-Clustering-Authentication Consensus. In the blockchain network architecture for IoT, we group miners into clusters. Each miner cluster is responsible for verifying transactions from devices in that cluster. Mining of new blocks is performed by the round robin method between clusters. The proposed consensus method can be used in private or consortium blockchain for IoT networks.

In our future work, we will apply the proposed consensus method to certain applications evaluate them, and subsequently improve the method.

References

[1] A. Patrizio, "IDC: Expect 175 zettabytes of data worldwide by 2025," Network World, 2018.

[2] A. M. Antonopoulos, "Mastering Bitcoin: unlocking digital cryptocurrencies," O'Reilly Me-dia, Inc, 2014.

[3] Z. Zheng, S. Xie, H. N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," in International Journal of Web and Grid Services, 14(4), pp. 352-375, 2018.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system. Manubot," 2008.

[5] T. T. Huynh, T. D. Nguyen, and H. Tan, "A Survey on Security and Privacy Issues of Blockchain Technology," in 2019 International Conference on System Science and Engineering (ICSSE), IEEE, pp. 362-367, 2019.

[6] V. Buterin, "On Public and Private Blockchains. Ethereum Blog," 2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains.

[7] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," in IEEE internet of things journal, 5(2), pp. 1184-1195, 2018.

[8] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in 2017 IEEE International Conference on Web Services (ICWS), IEEE, pp. 468-475, 2017.

[9] S. S. Panda, U. Satapathy, B. K. Mohanta, D. Jena, and D. Gountia, "Blockchain Based Decentralized Authentication Framework for Resource Constrained IOT devices," in 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), IEEE, pp. 1-6, 2019.

[10] P. F. Sheron, K. P. Sridhar, S. Baskar, and P. M. Shakeel, "A decentralized scalable security framework for end-to-end authentication of future IoT communication," Transactions on Emerging Telecommunications Technologies, 31(12), e3815, 2020.

[11] M. I. Khan, and I. A. Lawal, "Sec-IoT: A framework for secured decentralised IoT using blockchain-based technology," in International Congress on Information and Communication Technology. Springer, Singapore, pp. 269-277, 2020.

[12] J. Li, N. Li, J. Peng, H. Cui, and Z. Wu, "Energy consumption of cryptocurrency Mining: A study of electricity consumption in Mining cryptocurrencies," Energy, 168, pp. 160-168, 2019.

[13] L. Yang, Y. Zou, M. Xu, Y. Xu, D. Yu, and X. Cheng, "Distributed consensus for blockchains in internet-of-things networks," Tsinghua Science and Technology, 27(5), pp. 817-831, 2022.

[14] S. Wadhwa, S. Rani, S. Verma, J. Shafi, and M. Wozniak, "Energy Efficient Consensus Approach of Blockchain for IoT Networks with Edge Computing," Sensors, 22(10), 3733, 2022.

[15] M. M. Alhejazi, and R. M. A. Mohammad, "Enhancing the blockchain voting process in IoT using a novel blockchain Weighted Majority Consensus Algorithm (WMCA)," Information Security Journal: A Global Perspective, 31(2), pp. 125-143, 2022.

[16] D. Puthal, S. P. Mohanty, P., Nanda, E. Kougianos, and G. Das, "Proof-of-authentication for scalable blockchain in resource-constrained distributed systems," in 2019 IEEE international conference on consumer electronics (ICCE), IEEE, pp. 1-5, 2019.