Science & Technology Development Journal, 25(1):2279-2287

Open Access Full Text Article

Research Article

A novel security framework based on blockchain for IoT networks

Huynh Thanh Tam[1,*], Nguyen Dinh Thuc[2], Dang Hai Van[3], Huynh Nguyen Chinh[4]

ABSTRACT

Internet of Things (IoT) devices are indispensable components of smart cities, smart homes, and industrial control systems. Using a blockchain (BC)-based security framework in IoT security is extremely necessary and a current research trend. However, most current BC-based decentralized security frameworks have not yet reached the optimal performance of miners in transactions verification and data consensus in the BC ledger. In this paper, we present a novel BC-based security framework for ensuring the correctness and reliability of the data in the BC ledger and optimizing miners' performance over an IoT network. We propose the process of verifying transactions and data consensus based on two assumptions about miners in a BC network: (1) all miners are trusted nodes, and (2) some miners are untrusted nodes but less than one-third of the total number of miners. The evaluation results show that the more miners join the network, the more verified transactions increase and the lower the average mining time for a new block for assumption 1. For assumption 2, transactions only need to be verified once even if an untrusted miner is selected to propose a new block at a mining round. The proposed framework is more effective than other decentralized frameworks in the process of verifying transactions and data consensus.

Key words: IoT, Blockchain, security, framework

[1]*Faculty of Information Technology Posts and Telecommunications Institute of Technology, Ho Chi Minh City, Vietnam*

[2]*Decentralized Crypto Lab, Vietnam National University of Ho Chi Minh City, Vietnam*

[3]*Faculty of Information Technology University of Science, Vietnam National University of Ho Chi Minh City, Vietnam*

[4]*Faculty of Information Technology Ho Chi Minh City University of Technology and Education, Vietnam*

Correspondence

Huynh Thanh Tam, Faculty of Information Technology Posts and Telecommunications Institute of Technology, Ho Chi Minh City, Vietnam

Email: tamht@ptithcm.edu.vn

History

- Received: 2021-11-06
- Accepted: 2022-03-04
- Published: 2022-03-31

DOI : 10.32508/stdj.v25i1.3855

Check for updates

INTRODUCTION

A security framework is a set of functions, technologies, and protocols that provides a secure foundation for the implementation of applications. Using a security framework improves the system's optimization and ensures the accuracy and reliability of the stored data. A framework for an IoT network does not depend on any types of IoT devices in the network and can easily integrate new modules without changing the IoT network architecture.

Currently, the security frameworks for IoT networks can be divided into two main groups: centralized frameworks and decentralized frameworks. In centralized frameworks, a central node is responsible for storing data and providing services to the network, and other nodes can send requests to this node. Some typical solutions of this type are introduced in [1–3]. However, these solutions have three limitations as follows [4,5]: (1) *Data security*: all data stored in the central system can be altered or removed by any people controlling the system; (2) *Availability*: all nodes cannot be able to access the services if the central system is stopped operation due to overload, denial-of-service or distributed denial-of-service attacks, or system errors; (3) *Management, configuration, and scalability:* when the number of IoT devices and resources increases dramatically, the tasks of administration, configuration, and scalability become more complex.

For decentralized frameworks, most solutions use BC technology as the main component in the systems due to its advantages such as *anonymity*, *transparency*, *decentralization*, and *auditability* [6–8]. Moreover, an IoT network is usually owned by an exclusive organization. Hence, the private BC model is a more suitable selection for improving security and reducing network delay compared to the public BC model. However, the current consensus protocols used in these frameworks are not yet optimized resources for miners. Particularly, there are two assumptions about miners in a private BC as follows: (1) all miners in a private BC network are trusted nodes. However, the speed verification for transactions remains unchanged when adding some miners to the network, and (2) The assumption that a BC network exists some untrusted miners but less than one-third of the total number of miners, in case a malicious miner is selected at a mining round, it absolutely can put some invalid transactions in a new block and then broadcasts that block to the network. Of course, this invalid block is dropped by other miners; however, the valid transactions in this block have to be reverified in a future mining round. Therefore, we proposed a BC-based security framework for IoT networks, which aims to guarantee the reliability of data in the BC ledger and improve miners' performance.

The objectives of the proposed framework are as follows:

Cite this article : Tam H T, Thuc N D, Van D H, Chinh H N. **A novel security framework based on blockchain for IoT networks**. *Sci. Tech. Dev. J.;* 25(1):2279-2287.

- For assumption 1: (1) Increase the number of verified transactions when the number of miners in the framework increases; (2) Reduce the mining time when increasing the number of miners in the framework; (3) Increase the number of verified transactions as the mining time of a block increases while the number of miners stays the same.
- For assumption 2: Transactions only need to be verified once.

The proposed framework includes two phases: the verification phase and the block making phase. We also consider two assumptions when all BC miners are trusted nodes and some miners are untrusted nodes. Our contribution in this paper can be summarized as follows: (1) We propose a novel security framework based on BC for IoT networks; (2) We compare the proposed framework with other decentralized frameworks with the two assumptions discussed above; (3) We evaluate our proposed framework in terms of the mining speed and the number of transactions verified within certain times.

Paper outline: Section II presents the related work of BC-based security frameworks for IoT. The preliminaries are given in Section III. The proposed security framework is described in Section IV. The evaluation is given in Section V. Finally, the paper is concluded in Section VI.

RELATED WORK

Currently, BC-based security frameworks for the IoT provide three main features: access control, authentication and communication, and data security.

Concerning access control, a framework called FairAccess was introduced by Ouaddah et al.[9] as a privacy-preserving access control system in the IoT, where smart contracts are used to enforce access control policies and to distribute access tokens to the BC. A requester can use a token issued by a resource owner to access a licensed resource. In addition, each resource owner can also perform a GrantAccess transaction to revoke or update permissions granted to a requester. However, the authors in[10] specified the limitations of FairAccess in the high time cost related to distributing authorization to requesters and the lack of integration of the policies with a relationship network. To overcome these limitations, researchers also proposed a solution called ControlChain, which uses four different BCs, named Context BC, Relationships BC, Rules BC, and Accountability BC, to establish relationships between objects and then assign attributes to these relationships.

Concerning authentication and secure communication, Panda et al.[11] proposed an authentication framework for IoT systems. In this proposal, the gateway nodes joined in the BC network are an interface between IoT devices and the Ethereum BC network. Moreover, those nodes are also responsible for controlling connections and translating messages between IoT devices and users. A user can send his/her permission ticket emitted by a smart contract to the gateway to access a certain IoT device. In another work[12], the authors built a decentralized and scalable security framework to provide a secure communication mechanism for users and applications in an IoT environment. The tree-based hash method is responsible for verifying and authenticating messages exchanged between devices, while the BC ledger is used to store and distribute data securely. Similarly, Muhidul Islam Khan et al.[13] introduced a framework for secured communication in a decentralized IoT network. In this framework, a sending node has to sign a contract created by a selected miner node to transfer data to another node. They used a hybrid consensus algorithm consisting of binary and average consensus mechanisms for miner selection in the BC network.

Concerning IoT data security, the BC-based framework addressed in[14] allows both data owners and customers to verify data integrity for IoT data stored in the semitrusted cloud. In this approach, each data block is identified by a hash value of its content before uploading it to a cloud service provider. The encrypted hash value and the corresponding data block ID are written in a smart contract. In[15], the authors described a BC-based framework for IoT data trade, in which the processes of device management, data exchange between producers and consumers, and service quality assessment are performed by smart contracts.

The decentralized frameworks discussed above have some important contributions to the IoT domain. However, most of these frameworks focus on providing security services for IoT without mentioning the optimization issue in consensus. Particularly, the authors in[9,15] do not specify a particular consensus protocol in their BC network. The frameworks[11,14] use the proof-of-work (PoW) consensus protocol of the Ethereum BC platform to guarantee the reliability and accuracy of data stored in the BC ledger. Therefore, the mining process requires considerable electricity consumption and computational power for miners[16,17]. In[13], the hybrid consensus will operate like Proof-of-Stake (PoS) when the top miners maintain stable operation, and a selected miner has to take an extra step for sending contracts to the sending nodes for signing. In[7], the authors compare consensus algorithms and indicate that the PBFT, Tendermint, and DPOS protocols are suitable for consortium BCs or private BCs. He Yi et al.[18] also propose using Tendermint for a private BC. Deepak Puthal et al.[19] proposed a consensus algorithm named Proof-of-Authentication (PoAh) for a lightweight BC for IoT.

PRELIMINARIES

Blockchain

A BC can be viewed as a linked list of blocks of transactions, and each block refers to its parent block via a hash pointer. The first block of the chain is called the genesis block, which has no parent block, so the value of the hash pointer is initialized by the constructor of the BC network. The structure of each block includes two main components: the block header contains management information of the block and chain, such as Version, Previous block hash, Timestamp, Merkle root, and Nonce, and the block body holds a list of transactions[6], as shown in Figure 1.

The number of transactions in each block depends on the size of each transaction and block. However, a BC network will not work efficiently when blocks contain large data because the data synchronization time on the ledger will be very slow due to the network latency, which consumes considerable computational power of miners[20,21]. For Bitcoin electronic currency, each transaction has an average size of 250 bytes, and the maximum block size is set at 1 megabyte. The average block size of the last 100 blocks of Ethereum, measured by the authors in[22], is 2.9 kilobytes. There are two types of nodes on a BC network:

- *User node (or Normal node)*: The nodes only conduct transactions.

- *Miner node*: The nodes are responsible for verifying transactions, creating new blocks, and holding the ledger. A miner node can also perform transactions as normal nodes.

Each node of a BC network is initialized to a public/private key pair where the private key is used to create the signature on transactions while the public key is used to verify the digital signature. In general, there are three types of BC networks: public BC, private BC, and consortium BC[23].

Consensus Protocols

BC is a decentralized system in which nodes communicate directly with each other through a peer-to-peer network. Therefore, to synchronize data in the ledger of miners, one of the consensus protocols must be implemented in a BC system. Some consensus protocols are as follows:

- Proof-of-Work (PoW)[24]: The PoW consensus algorithm requires miners to find a nonce value such that the hash value of the nonce combined with the rest of the new block must satisfy a given difficulty. The process of adding a new block in the chain is called mining.

$$H(Nonce||New\ block) \leq \ Target\ value$$

where H is a cryptographic hash function and the symbol || denotes the concatenation of two strings

- *Proof-of-Stake* (PoS)[25,26]: A miner owning a certain amount of the network's value will have been the opportunity for mining. Depending on the particular applications, the "stake" value will be indicated.

- *Proof-of-Activity* (PoA)[27]: PoA is a hybrid protocol between PoS and PoW, where each miner tries to generate an empty block header satisfying a given difficulty requirement of PoS and then switching to PoS. This block needs to be signed by a certain number of stakeholders to be a valid block.

- *Proof -of-Authentication* (PoAh)[19]: The basic idea of the PoAh algorithm is that a normal node combines transactions in a new block. Then, the node signs on the new block before transmitting it to the network, and a trusted node verifies the received block and the signature of the sending node. After successful authentication, the trusted node broadcasts the validated block together with its PoAh identification to the network. Other nodes verify the PoAh identification to add the new block in their local chain.

- *Delegated proof of stake* (DPOS)[28]: Each node on the network is responsible for voting its trusted miner in each mining round, and a miner owning more BC stakes will have a higher possibility of being voted from other nodes for mining new blocks. If a miner fails to verify all transactions in the specified time, the mining task will be performed by the subsequent miner.

- *Practical Byzantine Fault Tolerance* (PBFT)[29]: The PBFT consists of three phases: Preprepared, Prepared, and Commit. In Preprepared, a selected miner combines transactions in a block and then broadcasts that block to other miners. In preparation, other miners issue their votes if the received block is valid. In the commit phase, each miner broadcasts their commitment on that block to other miners if they have received over 2/3 of votes for that block. Nodes will accept a new block if it receives more than 2/3 of commitments.

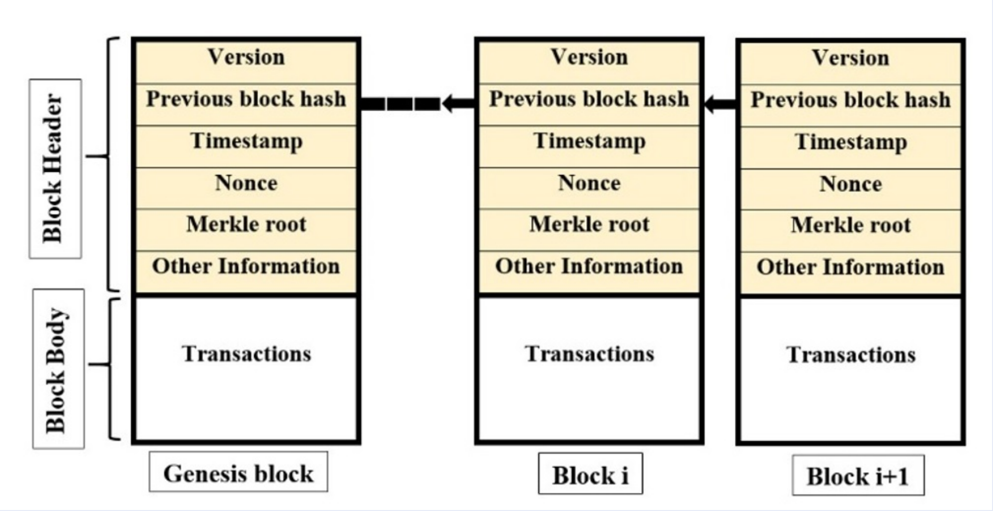

Figure 1: An example of blockchain.

- *Tendermint*[30]: Tendermint is a variant of PBFT consensus, which is composed of three phases: Prevote, Precommit, and Commit. In general, these steps are similar to PBFT; however, each protocol uses different techniques for each phase, and validators are locked their coins when participating in the Prevote process. The general characteristic of these consensus protocols is that a selected miner is responsible for verifying transactions and putting the valid transactions into a new block before proposing that block to the network; other nodes verify validation for the proposed block. Therefore, when increasing the number of miners in the network, the speed of confirming transactions does not change. In some cases, all miners used in a private BC network are trusted nodes. Hence, it is necessary to design a new security framework to maximize the performance of trusted miners.

PROPOSED FRAMEWORK

Let $M = \{m_1, m_2, ..., m_n\}$ be the set of n miner nodes in a BC network; each miner is responsible for verifying transactions and creating new blocks. Normally, these nodes have a high performance, such as servers or workstations, and own a private key and a corresponding public key in which the public key is considered a node identification or a wallet address on the BC network, while the private key is used to sign on transactions/blocks. All miner nodes must participate in the process of verifying transactions, and one of them is randomly selected for proposing a new block for each mining round. The waiting list $WL = \{tx_1, tx_2, ..., tx_m\}$ is the set of unconfirmed transactions received from IoT devices, which is considered a public transaction pool for miners. Furthermore, the verification list $VL = \{tx_1^*, tx_2^*, ..., tx_k^*\}$ is the set of verified transactions, and the values of m and k fluctuate from time to time. Let l be the maximum number of transactions in each block.

Each IoT device is a node on the BC network and has a key pair similar to a miner node, which can perform transactions. The architecture of the proposed framework is shown in Figure 2. The rules are applied for the VL and WL, including (1) Unverified transactions are saved to WL; (2) Only miners can verify transactions in the WL; (3) If a transaction is confirmed successfully, it will be moved from the WL to the VL otherwise dropped; (4) After adding a new block to the chain successfully, the corresponding transactions in the VL are removed by a system application.

We consider two assumptions about miners on a private BC network as follows:

- ***Assumption 1***: All miners are trusted nodes. This means that these nodes cannot be compromised by hackers and do not perform any cheating operation on the BC network.
- ***Assumption 2***: Some of the miners, called untrusted nodes or dishonest nodes, do not guarantee reliability. This can be compromised by attackers through the vulnerabilities of their operating systems or installed applications. However, the number of dishonest nodes is less than one-third of the total number of miners on the network.

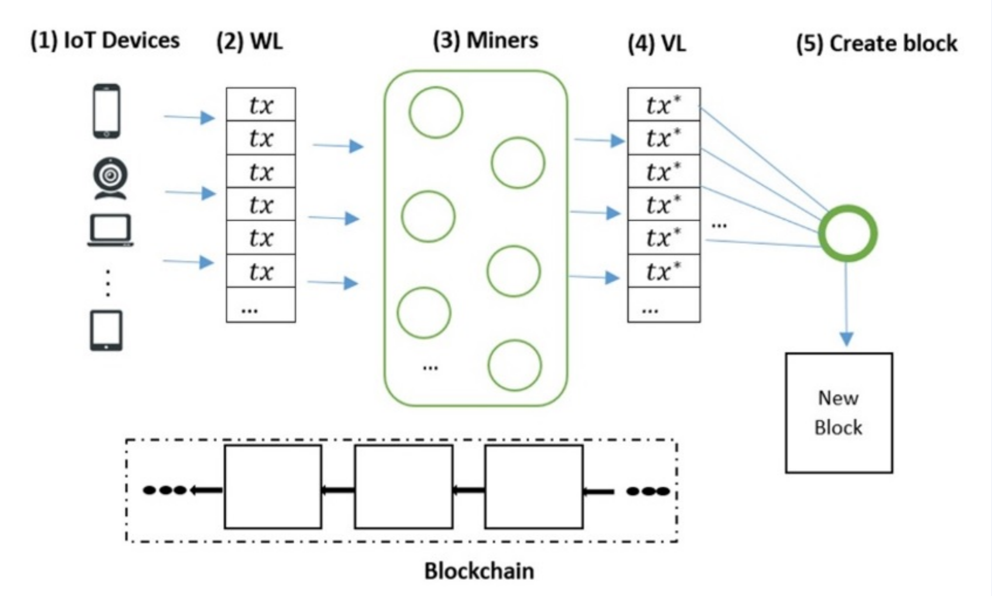

Figure 2: The architecture of the proposed framework.

The processes of creating and synchronizing data on the ledger of the proposed framework consist of two phases as follows:

- **Phase 1:** The verification phase

When an IoT device makes a transaction tx_i which is broadcasted to the BC network and is stored in the tail of the WL. The process of verifying transactions in the WL depends on the two assumptions.

+ *For Assumption 1:* Since all miners are completely trusted, tx_i only needs to be verified by one miner in the network, for instance, m_j. If tx_i is a valid transaction, it will be added to the tail of VL; otherwise, it will be dropped.

+ *For Assumption 2:* The tx_i needs to be verified by at least two-thirds of the miners to be added to the VL.

- **Phase 2:** Block-making phase

The basic idea is that a selected miner puts the head transactions of the VL into a new block and then signs and transmits that block to other miners for verification. The block is added to the chain if it satisfies the requirements of the particular assumptions. The detailed steps of this phase are as follows:

Step 1: The goal of this step is to select a miner for creating and broadcasting a new block to the network.

+ *For Assumption 1:* Since the miners are all honest, the administrator can select a fixed miner node m_i and can also change m_i by another node as needed.

+ *For Assumption 2:* A miner is randomly selected for each mining round: $m_i \leftarrow M$, where $1 \leq i \leq n$.

Step 2: The m_i takes l transactions in the VL into a new block, where the value l depends on the size of each transaction and the maximum allowed size of each block. Then, m_i generates a digital signature on the new block.

Step 3: The m_i broadcasts the new block and signature to the other miners. In addition, m_i also adds that block to its local chain.

Step 4: After receiving a new block, other miners verify the validation of the block proposed by the m_i.

+ *For Assumption 1:* Other miners verify the signature of m_i; if the signature is valid, the block is added to their chain.

+ *For Assumption 2:* Including the two following substeps

(i) Other miners verify the signature of the m_i. If the verification is successful, the miners go to the next substep; otherwise, the miners drop that block and go to *Step 1*.

(ii) Other miners check whether the transactions in the new block are the same as the transactions in the VL. If it is true, the block is added to their chain; otherwise, the miners drop that block and go to *Step 1*.

EVALUATION

In this section, we evaluate the proposed framework in the two assumptions in terms of the mining time of a block containing l transactions and the number of verified transactions in a certain time. The current decentralized security frameworks for IoT are mainly focused on providing particular features such as access control, authentication, secure communication, and data security. However, the mechanisms of verifying transactions, creating blocks, and synchronizing data in the ledger depend entirely on consensus protocols. Therefore, we compare the proposed framework to other consensus protocols that can be used in the frameworks mentioned in the related work section.

We assume that all miners have the same computational performance. Let t_1 be the verification time per transaction of a miner, t_2 be the time of generating a digital signature/vote/certificate of a miner for a block, and t_3 be the time of verifying a signature/vote/certificate of a miner. The time of transferring a block/vote/certificate/transaction to a destination (such as the VL or a miner) is t_4, and t_5 be the time of randomly selecting a miner at each mining round.

The proposed framework in assumption 1

In phase 1, each transaction is verified by only one of the n miners; therefore, the verification time of l transactions is $\frac{l}{n}t_1$, and the time for transferring l transactions verified by the n miners to the VL is $\frac{l}{n}t_4$. In phase 2, the time of the first operation is ignored because a miner is fixed for creating blocks; hence, the total time of this phase includes the time at steps 2, 3, and 4, that is, $t_2+t_3+t_4$. The total time of generating a new block of our framework, denoted by T, is considered the average mining time of the system, which is as follows:

$$T = \frac{l}{n}t_1 + t_2 + t_3 + \left(\frac{l}{n} + 1\right)t_4 \qquad (1)$$

Consider the time of generating a new block of other frameworks using consensus protocols such as PoW, PoS, PoA, PoAh, PBFT, and Tendermint. The common characteristic of these consensus protocols is that a selected miner is responsible for proposing a new block, and other nodes must verify this proposed block. With assumption 1, all miners are trusted nodes and have to publish their public key to the BC network. A selected miner has to sign on a new block before distributing that block to other miners. The general algorithm of these consensus protocols, denoted by A1, is illustrated in Table 1.

To verify l transactions in *Step 1(1)*, m_i spends $lt_1 time$. The times of creating a signature and broadcasting the new block at *Step 1(2)* and *Step 1(3)* are t_2 and t_4, respectively. The time for verifying a signature at Step 2 is t_3. The total average mining time of the A1, denoted by T', is calculated as follows:

$$T' = lt_1 + t_2 + t_3 + t_4 \qquad (2)$$

Let t_1 = 1, t_2 = 1, t_3 = 1, t_4 = 1, and l = 40. Figure 2 shows the average mining times of A1 and the proposed framework. From this figure, it is shown that the mining time of the proposed framework is much lower than.A1. Specifically, the average mining time of A1 T'= 43 when the number of miners n = 10 remains unchanged when increasing the number of miners from 10 to 50, whereas the average mining time of the proposed framework T = 11 when n = 10, and for n = 50, then T = 4.6. This means that the more miners that join the network, the lower the average mining time.

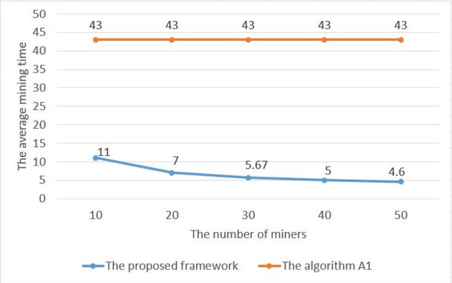

Figure 3: The comparison result between the two algorithms.

Another experimental analysis is performed in terms of adjusting the parameters n and l in formula (1) of the proposed framework, as shown in Figure 4. As shown in the figure, it is clear that with the same number of miner nodes, the average mining time increases proportionally with the number of transactions in a block. In addition, when the number of miners increases, the average mining time is reduced. Particularly, when the same value n = 10, with the number of transactions in each block l = 10, then the average mining time T = 5; for l = 20, then T = 7; for l = 30, then T = 9; and with l = 40, then T = 11. When increasing the number of miners n = 50, for l = 10 then T = 3.4, for l = 20 then T = 3.8, for l = 30 then T = 4.2, and with l = 40 T = 4.6.

Figure 5 shows that if both solutions are configured with the same average mining time and the number of miners is 20 (n = 20), the total verified transactions of the proposed framework are also significantly higher than the A1. When the average mining time is 5, the numbers of processed transactions of A1 and the proposed framework are 5 and 20, respectively. However,

Table 1: The algorithm

	Algorithm A1
	Input: l transactions in the pool, a selected miner m_i, and other miners. **Output**: a new block in the BC ledger.
Step 1	(1) m_i verifies l transactions and puts them into a new block. (2) m_i generates a signature on this block. (3) m_i broadcasts that block to other miners as well as adds that block to its local chain.
Step 2	Other miners verify the signature on the received block, if the signature is valid, the block will be added to the chain.

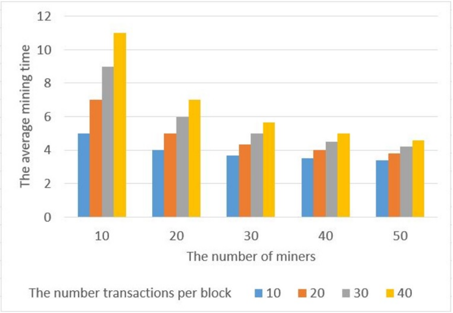

Figure 4: The average mining time of the proposed framework.

when T is set to 25, the number of processed transactions of A1 increases slightly to 22, while the proposed framework handles up to 220 transactions.

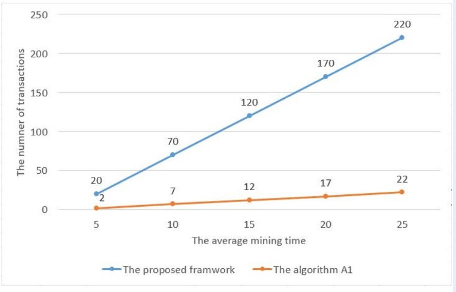

Figure 5: Comparison of the number of verified transactions of both solutions.

The number of verified transactions of the proposed framework increases proportionally with the verification time and the number of miners on the network, as shown in Figure 6. In the same mining time, the system with more miners has more verified transactions than other systems. Specifically, considering the average mining time T = 5, when the number of miners in the network n = 5, the total number of verified transactions from these miners l = 5; when n = 10, then l = 10, and n = 15 corresponds to l = 15. Consider T = 40; for n = 5, then l ≈ 93 transactions; for n = 10, then l = 185; and for n = 15, l ≈ 278.

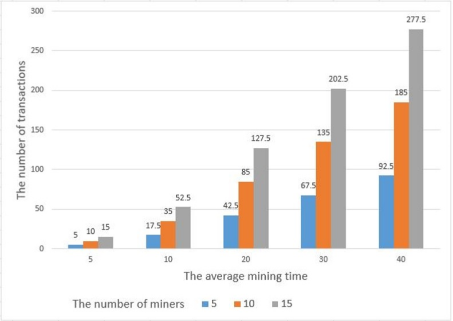

Figure 6: The number of verified transactions of the proposed solution.

Our evaluation results show that using the proposed security framework in this assumption is well suited for private BC networks, which will be highly effective in the process of transactions verification and data consensus on the BC ledger. However, all miners in the private BC network must be completely trusted, which means that they are hardly compromised by any attackers and do not commit any fraud in the BC network.

The proposed framework in assumption 2

Each transaction must be verified by at least two-thirds of all miners, which means that a valid transaction will be issued a certificate by a trusted miner. If a transaction has reached two-thirds of certificates, it will be immediately moved to the VL by a monitor application without further verification; otherwise, it will be removed from the WL. In the case of a network with many untrusted miners but less than one-third of the total number of miners, each transaction has to be verified by all miners. This work is similar to other consensus protocols when considering that all miners are the same as a miner, as shown in Figure 7.

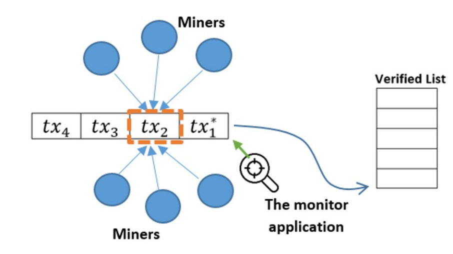

Figure 7: The transaction verification process in phase 1.

In this assumption, we compare the proposed framework to the PBFT and Tendermint protocols. Tendermint is based on PBFT consensus, and both of these consensuses operate based on the assumption that less than one-third of the miners are untrusted nodes. We describe the general three steps of these two protocols, called A2, as shown in Table 2.

In general, both the A2 and the proposed framework have the same security level when all transactions have to be verified by at least two-thirds of miners. In case the selected miner is honest, the verification time for transactions is not much different in both solutions. However, the proposed framework is better than the A2 in the case the selected miner is untrusted. More precisely, when the selected miner is compromised by hackers in a mining round, the hackers can broadcast a new block containing some invalid transactions. Of course, this new block will be removed by other miners in both solutions. However, for, A2, the valid transactions in the dropped block have to be reverified in the next mining round. Meanwhile, in the proposed framework, miners do not need to reverify these transactions because those transactions are still stored in VL until a block containing them has been successfully verified.

The proposed framework in this assumption can be used for consortium BC networks, in which untrusted miners must be less than one-third of the total number of miners in the networks.

CONCLUSION

This paper proposes a framework based on BC for the IoT. The proposed framework provides the reliability of data in the BC ledger and optimizes computational powers for miners in two assumptions about miners on the private BC network. With the assumption that miners are trusted nodes, the proposed framework operates more efficiently than other consensus protocols. In addition, in the case of existing untrusted miners with less than a third of the total number of miners, the proposed framework is better than the PBFT and Tendermint algorithms. The proposed framework is an effective and feasible solution for IoT networks.

ACKNOWLEDGMENTS

This research is funded by Vietnam National University of Ho Chi Minh City (VNU-HCMC) under grant number HTHT2021-18-02.

REFERENCES

1. Banerjee A, et al. Centralized framework for controlling heterogeneous appliances in a smart home environment. In 2018 International Conference on Information and Computer Technologies (ICICT), 2018, pp. 78-82;Available from: https://doi.org/10.1109/INFOCT.2018.8356844.
2. Bouij-Pasquier I, et al. A security framework for internet of things. In International Conference on Cryptology and Network Security, 2017, pp. 19-31; ;Available from: https://link.springer.com/chapter/10.1007/978-3-319-26823-1_2.
3. Liu X, et al. A security framework for the internet of things in the future internet architecture. Future Internet, 2017, 9(3), 27; ;Available from: https://doi.org/10.3390/fi9030027.
4. Zhang C, et al. Privacy and security for online social networks: challenges and opportunities. IEEE network, 2010, 24(4), pp. 13-18;Available from: https://doi.org/10.1109/MNET.2010.5510913.
5. Xu R, et al. Blendcac: A blockchain-enabled decentralized capability-based access control for Iots. In 2018 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), 2018, pp. 1027-1034;Available from: https://doi.org/10.3390/computers7030039.
6. Antonopoulos AM. Mastering Bitcoin: unlocking digital cryptocurrencies. O'Reilly Media, Inc, 2014;.
7. Zheng Z, et al. Blockchain challenges and opportunities: A survey. In International Journal of Web and Grid Services, 2018, pp. 352-375;Available from: https://doi.org/10.1504/IJWGS.2018.10016848.
8. Conti M, et al. A survey on security and privacy issues of bitcoin. IEEE Communications Surveys & Tutorials, 2018, pp. 3416-3452;Available from: https://doi.org/10.1109/COMST.2018.2842460.
9. Ouaddah A, et al. Toward a novel privacy-preserving access control model based on blockchain technology in IoT. In Europe and MENA cooperation advances in information and communication technologies, 2017, pp. 523-533;Available from: https://doi.org/10.1007/978-3-319-46568-5_53.
10. Pinno OJA, et al. Controlchain: Blockchain as a central enabler for access control authorizations in the iot. In GLOBECOM 2017-2017 IEEE Global Communications Conference, 2017, pp. 1-6;Available from: https://doi.org/10.1109/GLOCOM.2017.8254521.
11. Panda SS, et al. A Blockchain Based Decendcasttralized Authentication Framework for Resource Constrained IOT devices. In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp. 1-6;Available from: https://doi.org/10.1109/ICCCNT45670.2019.8944637.
12. Sheron PF, et al. A decentralized scalable security framework for end-to-end authentication of future IoT communication. Transactions on Emerging Telecommunications Technologies 31.12 (2020): e3815;Available from: https://doi.org/10.1002/ett.3815.
13. Khan MI, Lawal I. Sec-IoT: A framework for secured decentralized IoT using blockchain-based technology;.

Table 2: The algorithm

Algorithm A2	
	Input: l transactions in the pool and miners **Output**: a new block in the BC ledger
Step 1	Randomly select one miner at each mining round (e.g. m_i) m_i verifies puts l valid transactions into a new block. m_i creates a vote on this block. m_i broadcasts this block along with a vote on the proposed block to other miners on the BC network.
Step 2	Each miner has to perform the following works after receiving a new block and vote from m_i: Verifying transactions in this block. If all transactions are valid, the miner generates its vote for that block. Broadcasting the vote to other miners. When a miner has received more than 2/3 of votes. It will create a certificate for that block and broadcast it to other miners.
Step 3	Miners verify received certificates. If the miner node has received over 2/3 of valid certificates on the proposed block, the miner will add the block to the chain

14. Liu B, et al. Blockchain based data integrity service framework for IoT data. In 2017 IEEE International Conference on Web Services (ICWS), 2017, pp. 468-475;Available from: https://doi.org/10.1109/ICWS.2017.54.
15. Singh PK, et al. Designing a Blockchain Based Framework for IoT Data Trade. In International Conference on Innovations for Community Services, 2020, pp. 295-308;Available from: https://doi.org/10.1007/978-3-030-37484-6_17.
16. Li J, et al. Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies. Energy, 2019, 168, pp. 160-168;Available from: https://doi.org/10.1016/j.energy.2018.11.046.
17. Bach LM, et al. Comparative analysis of blockchain consensus algorithms. In 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018, pp. 1545-1550;Available from: https://doi.org/10.23919/MIPRO.2018.8400278.
18. Yi H, et al. Research on a suitable blockchain for IoT platform. In Recent Developments in Intelligent Computing, Communication and Devices, 2019, pp. 1063-1072;Available from: https://doi.org/10.1007/978-981-10-8944-2_123.
19. Puthal D, et al. Proof-of-authentication for scalable blockchain in resource-constrained distributed systems. In 2019 IEEE International Conference on Consumer Electronics (ICCE), 2019, pp. 1-5;Available from: https://doi.org/10.1109/ICCE.2019.8662009.
20. Dennis R, et al. A temporal blockchain: a formal analysis. In 2016 International Conference on Collaboration Technologies and Systems (CTS), 2016, pp. 430-437;Available from: https://doi.org/10.1109/CTS.2016.0082.
21. Göbel J, Krzesinski AE. Increased block size and Bitcoin blockchain dynamics. In 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), 2017, pp. 1-6;Available from: https://doi.org/10.1109/ATNAC.2017.8215367.
22. Gencer AE, et al. Decentralization in bitcoin and ethereum networks. In International Conference on Financial Cryptography and Data Security, 2018, pp. 439-457;Available from: https://doi.org/10.1007/978-3-662-58387-6_24.
23. Buterin V. On public and private blockchains. Ethereum blog, 2015;Available from: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.
24. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system, 2018;.
25. King S & Nadal S. Ppcoin: Peer-to-peer cryptocurrency with proof-of-stake. self-published paper, 2012;.
26. Zheng Z, et al. Blockchain challenges and opportunities: A survey. In International Journal of Web and Grid Services, 2018, pp. 352-375;Available from: https://doi.org/10.1504/IJWGS.2018.10016848.
27. Bentov I, et al. Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract], y. ACM SIGMETRICS Performance Evaluation Review, 2014, 42 (3) (pp. 34-37);Available from: https://doi.org/10.1145/2695533.2695545.
28. Larimer D. Delegated proof-of-stake (DPOS). Bitshare whitepaper, 2014;.
29. Sukhwani H, et al. Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric). In 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), 2017, pp. 253-255;Available from: http://dx.doi.org/10.1109/SRDS.2017.36.
30. Kwon J. Tendermint: Consensus without Mining, 2014;.

VNUHCM PRESS
25 years of scholarly publishing
1997-2022

Tạp chí Phát triển Khoa học và Công nghệ
Đại học Quốc gia Tp. Hồ Chí Minh

ISSN 1859-0128
Sci. Tech. Dev. J.
Issue 1, Vol 22, 2019
Science and Technology Development Journal
The official journal of Viet Nam National University Ho Chi Minh City, Viet Nam
Since 1998
Indexed & Abstracted by:
Google Scholar, OCLC
Worldcat, Dimension, Scilit
www.scienceandtechnology.com.vn

Tạp chí Phát triển Khoa học và Công nghệ
ISSN: 1859-0128
Hình thức xuất bản: In và trực tuyến
Hình thức truy cập: Truy cập mở (Open Access)
Ngôn ngữ bài báo: Tiếng Anh
Tỉ lệ chấp nhận đăng 2021: 72%
Phí xuất bản: Miễn phí
Thời gian phản biện: 43 ngày
Lập chỉ mục (Indexed): Google Scholar, Scilit

SCAN ME

ISSN 2588-106X
Sci. Tech. Dev. J.-Nat. Sci.
Issue 1, Vol 3, 2019
Science and Technology Development Journal
NATURAL SCIENCE
A sub-journal of Science and Technology Development Journal
http://stdjns.scienceandtechnology.com.vn

Tạp chí Phát triển Khoa học và Công nghệ - Khoa học Tự nhiên
ISSN: 2588-106X
Hình thức xuất bản: In & trực tuyến
Hình thức truy cập: Truy cập mở
Ngôn ngữ bài báo: Tiếng Việt
Tỉ lệ chấp nhận đăng 2021: 75%
Phí xuất bản: Miễn phí
Thời gian phản biện: 30-45 ngày
Lập chỉ mục (Indexed): Google Scholar, Scilit

SCAN ME

ISSN 2615-9872
Science and Technology Development Journal
ENGINEERING & TECHNOLOGY
A sub-journal of Science and Technology Development Journal
BK
http://stdjet.scienceandtechnology.com.vn

Tạp chí Phát triển Khoa học và Công nghệ - Kĩ thuật và Công nghệ
ISSN: 2615-9872
Hình thức xuất bản: In & trực tuyến
Hình thức truy cập: Truy cập mở
Ngôn ngữ bài báo: Tiếng Việt
Tỉ lệ chấp nhận đăng 2021: 61%
Phí xuất bản: Miễn phí
Thời gian phản biện: 50 ngày
Lập chỉ mục (Indexed): Google Scholar, Scilit

SCAN ME

ISSN: 2588-1051
Sci. Tech. Dev. J.-Eco. Law Manag.
Issue 1, Vol 3, 2019
Science and Technology Development Journal
ECONOMICS-LAW AND MANAGEMENT
A sub-journal of Science and Technology Development Journal
UEL
http://stdjelm.scienceandtechnology.com.vn

Tạp chí Phát triển Khoa học và Công nghệ - Kinh tế-Luật và Quản lý
ISSN: 2588-1051
Hình thức xuất bản: In & trực tuyến
Hình thức truy cập: Truy cập mở
Ngôn ngữ bài báo: Tiếng Việt
Tỉ lệ chấp nhận đăng 2021: 65%
Phí xuất bản: Miễn phí
Thời gian phản biện: 45 ngày
Lập chỉ mục (Indexed): Google Scholar, Scilit

SCAN ME

ISSN 2588-1043
Sci. Tech. Dev. J.-Soc. Sci. Human.
Issue 1, Vol 3, 2019
Science and Technology Development Journal
SOCIAL SCIENCES & HUMANITIES
A sub journal of Science and Technology Development Journal
http://stdjssh.scienceandtechnology.com.vn

Tạp chí Phát triển Khoa học và Công nghệ - Khoa học Xã hội và Nhân văn
ISSN: 2588-1043
Hình thức xuất bản: In & trực tuyến
Hình thức truy cập: Truy cập mở
Ngôn ngữ bài báo: Tiếng Việt
Tỉ lệ chấp nhận đăng 2021: 62%
Phí xuất bản: Miễn thu phí đối với tác giả là CBVC của ĐHKHXHNV, ĐHQG-HCM; Tác giả khác: 500.000 VNĐ/bài
Thời gian phản biện: 75 ngày
Lập chỉ mục (Indexed): Google Scholar, Scilit

SCAN ME

ISSN 2588-1078
Sci. Tech. Dev. J.-Sci. Earth Environ.
Issue 1, Vol 3, 2019
Science and Technology Development Journal
SCIENCE OF THE EARTH & ENVIRONMENT
A sub-journal of Science and Technology Development Journal

Tạp chí Phát triển Khoa học và Công nghệ - Khoa học Trái đất và Môi trường
ISSN: **2588-1078**
Hình thức xuất bản: In & trực tuyến
Hình thức truy cập: Truy cập mở
Ngôn ngữ bài báo: Tiếng Việt và tiếng Anh
Tỉ lệ chấp nhận đăng 2021: 87%
Phí xuất bản: liên hệ tòa soạn
Thời gian phản biện: 45 ngày
Lập chỉ mục (Indexed): Google Scholar, Scilit

SCAN ME

ISSN 2734-9446
Science and Technology Development Journal
HEALTH SCIENCES
A sub-journal of Science and Technology Development Journal
http://stdjhs.scienceandtechnology.com.vn

Tạp chí Phát triển Khoa học và Công nghệ - Khoa học Sức khỏe
ISSN: 2734-9446
Hình thức xuất bản: In & trực tuyến
Hình thức truy cập: Truy cập mở
Ngôn ngữ bài báo: Tiếng Việt
Tỉ lệ chấp nhận đăng 2021: 70%
Phí xuất bản: Miễn phí
Thời gian phản biện: 30 ngày
Lập chỉ mục (Indexed): Google Scholar, Scilit

SCAN ME

Tạp chí Phát triển Khoa học và Công nghệ, Đại học Quốc gia Tp.HCM
25 năm xuất bản học thuật (1997-2022)
Tòa soạn: Nhà điều hành Đại học Quốc gia Tp.HCM, P. Linh Trung, TP. Thủ Đức, TP. HCM
Email: stdj@vnuhcm.edu.vn; tcptkhcn@vnuhcm.edu.vn; Website: *http://www.scienceandtechnology.com.vn*