A Scalable Nested Blockchain Framework with Dynamic Node Selection Approach for IoT

Xiaofeng He
Beijing University of Posts and Telecommunications
Beijing, China
xiaofenghe@bupt.edu.cn

Yuchao Zhang
Beijing University of Posts and Telecommunications
Beijing, China
yczhang@bupt.edu.cn

Xiaotian Wang
Beijing University of Posts and Telecommunications
Beijing, China
wangxiaotian@bupt.edu.cn

***Abstract*—A high level of scalability is needed to support the large-scale Internet-of-Things (IoT) networks. To address the issue of distributed trust in different IoT devices, blockchain technology can be effectively used to safely manage IoT data due to its ability to provide transactions traceability and security. However, massive real-time IoT application data has brought huge challenges to the scalability of the integration framework of blockchain and IoT. This paper proposes a nested-chain architecture, which consists of one main chain and multiple sub chains to address the aforementioned challenges. The main chain stores identity credential used for distributed identity (DID) management, while the sub chain stores the IoT data. A notary module that involves access nodes from both chains is designed for cross-chain transactions. In addition, considering the transaction information, node characteristics, and network status, we further introduce a node selection algorithm based on Graph Convolutional Network (GCN), which can effectively reduce the cost of cross-chain communications. We implement and evaluate a prototype of our framework on the Hyperledger Fabric platform to demonstrate its feasibility and superiority. The analyzed results have shown that our proposed framework outperforms traditional schemes, by reducing system latency up to 23.2% and increasing system throughput up to 12.5%.**

***Index Terms*—IoT, Blockchain, Scalability, Machine Learning**

I. Introduction

The emergence of blockchain technology brings practical solutions to overcome security issues in the Internet-of-Things (IoT). But with the rapid development of 5G and other communication technologies, the demand for scalable IoT systems with high performance has grown significantly due to the huge amounts of IoT data and the resource constraints of IoT devices [1].

Current blockchain frameworks are unsuitable to be applied in large-scale IoT networks because when many nodes within the system generate massive real-time data, the frameworks cannot support high transaction throughput while still maintaining low latency [2]. This has become an essential issue in the use of blockchain for different IoT scenarios. To make it possible, we must deal with the following two fundamental challenges. The first one is **scalability limitation**. As each full node in the blockchain needs to store a complete copy of the blocks, it could easily exhaust the local disk storage of IoT devices when expanding to large-scale networks with high-frequency transactions. The increasing scale of the network consumes more network bandwidth and computation resources which leads to a rapid increase in communication overhead [3]. The second one is **interoperation problem**. Interoperation allows heterogeneous blockchains to interact and make synchronously cross-chain transactions. Cross-chain communication requires a stable and low-latency connection with each other to send, receive and validate new blocks timely. Existing solutions may realize verified and secure interoperation at the cost of inefficiency which causes a remarkable decline in system performance [4]. In short, the scalability bottleneck and interoperation issues of current blockchain frameworks make them impracticable in IoT.

In this paper, we propose a new multi-chain architecture that addresses bottlenecks and shortcomings of scalability in current blockchain frameworks. To overcome the two challenges above, we present the following two novel designs. 1). **Nested-chain Framework**. To resolve the scalability issue, we propose a nested blockchain architecture, which consists of one main chain and multiple sub chains. The sub chains interact with IoT devices to receive and store local IoT data and the main chain is responsible for collecting essential metadata of identity that is used for decentralized digital identity storage and authentication of clients. The interoperation between the main chain and the sub chain involves verification of the identity. 2). **Cross-chain Notary Module**. To address the communication limitation, we design a notary module that is used for cross-chain communication and transaction authentication between the main chain and the sub chain. Access nodes are elected from each chain when cross-chain communication is requested, and they are then involved in the notary module for interoperation. Since nodes in the sub chain are deployed in distributed geographical locations, it is challenging to maintain stable states and high computational power. If an inefficient node is selected to be an access node, the latency of the cross-chain transaction will increase which results in system performance degradation. Thus, we further propose a node selection algorithm using an improved

This work was supported in part by the Key Project of Beijing Natural Science Fisoundation under M21030, the National Natural Science Foundation of China (NSFC) under Grant 62172054 and 62072047, and the National Key R&D Program of China under Grant 2019YFB1802603. Yuchao Zhang is the corresponding author.

978-1-6654-4331-9/21/$31.00 ©2022 IEEE

Graph Convolutional Network (GCN) model. To evaluate the performance of the proposed framework, we implement a prototype of the nested-chain system on the Hyperledger Fabric blockchain platform. We provide experimental results and evaluate the framework in WAN deployments which means the nodes are uniformly selected from different regions. The experiment results show that the nested-chain system achieves the lowest latency, highest throughput, and minimum system performance degradation with different input settings in cross-chain communication compared to existing methods.

Our contributions can be summarized as follows:

- We propose and implement a novel nested multi-chain framework with high scalability and performance. A notary module is designed for achieving interoperation.
- We propose a node selection algorithm based on the Graph Convolutional Network (GCN) which can realize high-efficient and stable cross-chain communication.
- We conduct a series of experiments on the proposed framework and then provide a detailed analysis showing that the proposed solution performs better than current approaches.

The remainder of this paper is organized as follows. The related work is described in Section II. In Section III, we present the system model and the node selection algorithm. Comparative experiments and analysis are presented in Section IV. Finally, the paper is concluded in Section V.

II. RELATED WORK

In terms of multi blockchain structure, scalability and cross-chain interoperability are quite related research topics, so in this section, we introduce some state-of-the-art solutions related to these topics.

A. Existing Multi-chain Frameworks

Unlike previous blockchain implementations which have focused on providing a single chain of varying degrees of generality over potential applications, multi-chain architecture normally involves multiple layered heterogeneous blockchains to address the issue of extensibility and scalability. Polkadot [5] proposed an influential multi-chain framework, to provide a scalable and interoperable framework for multiple chains with pooled security through gathering the security power of all these chains together in a shared security system. Some works [6]–[8] have made improvements to the traditional multi-chain architecture to resolve the issue of low efficiency with low transaction throughput. Despite the significant benefits of existing multi-chain based approaches, such us high-efficient interopration and privacy preservation, many issues remain unaddressed. For example, [9] proposed a framework to address the scalability limitations of blockchain using a scalable lightweight multi-chain structure, which reduces the average processing time of each cross-chain transaction. However, it employs a P2P overlay network for blockchain management which could easily cause single point of failure node and the number of concurrently served clients are limited. [10] designed a novel hierarchical multi expressive blockchain that provides the autonomous management of the trusted application data and an inherent forensics mechanism tailored for granular auditing. This approach reduces the transaction validation frequency without losing the immutability benefits. But it is still unable to satisfy the requirements for interoperability of independently managed trust authorities. The solutions mentioned above may be effective in relieving the scalability issue, however, high increased costs for addressing massive real-time data make them impracticable to be applied in a large-scale IoT network.

B. Cross-chain communication

Since consortium blockchain is a permissioned chain which makes it unable to directly make transactions between chains, interoperation is needed to achieve cross-chain communication [4]. According to the state of the arts, recent works on making blockchain interoperable mainly use relay technology or notary mechanism. However, these solutions are restricted in some aspects. Relay technology is to construct a common chain or relay structure between two chains to validate and store account status and transaction status. For example, Cosmos [11], and Polkadot [5] solve interoperation issue by using Cosmos Hub or Polkadot Relay Chain, allowing interconnection between heterogeneous blockchain networks. However, the above two solutions may lead to poor security guarantee and fail to consider the dynamic status of nodes that are selected to build the relay chain for transaction, which is not conducive to the efficient execution of the system. BTC Relay [12] is considered to be the first side-chain, which realizes the cross-chain access of data between Ethereum and Bitcoin by focusing exclusively on one type of interconnection via smart contract. But it only supports cross-chain access from Ethereum to Bitcoin, and Bitcoin cannot read information in the Ethereum at the same time which means it could only transact in a parent-child mode [13]. The Notary mechanism [14] uses a third party to undertake the information interaction between two chains which removes the trust validation required by the transaction participants. This method is more flexible and secure since the system security is guaranteed when a few nodes are attacked or various errors occur. However, it may involve unauthenticated node with misbehavior, which is not conducive to the efficient execution of the system since the identity verification during cross-chain communication is crucial for interoperation.

III. SYSTEM DESIGN

In this section, we will first introduce the framework of the proposed nested multi-chain architecture, and then present the access node selection algorithm.

A. Overview of Nested-chain architecture

The proposed solution is a multi blockchain architecture including one main chain and multiple sub chains to solve the scalability issue. The overall structure of the nested-chain is shown in Figure 1. The bottom layer is a wide diversity of IoT devices that are connected to different sub chains

through gateways. Considering the limited computing power and storage capacity of IoT devices, they are not implemented as blockchain nodes in our framework. Instead, a gateway is used to connect IoT devices with blockchain networks, which acts as an agent to receive enrolments/data from the local cluster of IoT devices and transmit it to the blockchain network by invoking the smart contract. The blockchain network, which is the most critical part of this project, consists of a main chain, multiple sub chains, and notary modules.

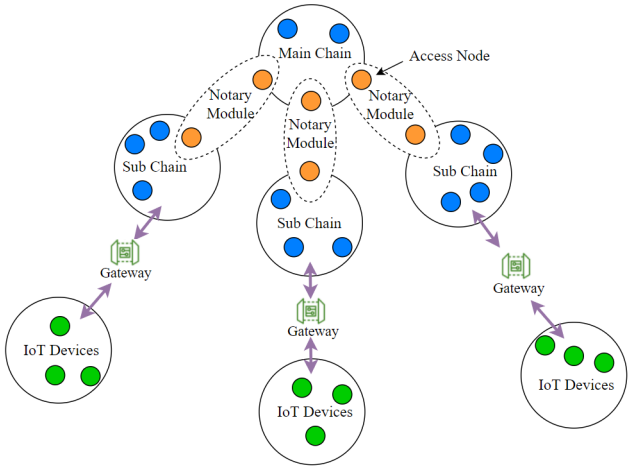


Fig. 1: The nested-chain architecture

1) Main chain: Decentralized identifiers (DID) [15] is a type of decentralized verifiable digital identifier. The main chain is designed to be a decentralized identity management system used for storing DID authentication information and identity verification during cross-chain communication. To avoid creating a central authority for validation, identities should be independently verifiable by a third party which means the decoupling of devices' identities from the blockchain they are within. Thus, the main chain maintains identity records of the sub chain nodes in a distributed ledge which can be shared by the pool of sub chain nodes through consensus to ensure the reliability of cross-chain interoperation. For the storage process, the IoT devices first pack the public key and private key into a registration request and send it to the CA. After receiving the request, the CA uses a random number associated with the identity as the identity link to build a digital identity certificate for the device ID. The digital identity includes a public key, timestamp, validity period, and identity link. A digital identity certificate issuance transaction is conducted between the CA and the main chain. The main chain processes the transaction, packs it into a new block and broadcasts it to the blockchain network.

2) Sub Chain and Notary Module: Each sub chain is responsible for collecting and storing the generated data from IoT devices. The identity data exchange between the main chain and the sub chain is achieved through cross-chain transactions. However, most current blockchain frameworks for IoT do not support high-efficient interoperability. To maintain stable and low-latency connection during cross-chain communication, a notary module is proposed to verify and authenticate blockchain transactions and ensures trust between inter-operating blockchain network. It is a mini blockchain that only contains intermediaries called access nodes. Access nodes are high-efficient nodes selected from the main chain and the sub chain.

To ensure the security of cross-chain communication, it is necessary to verify whether the access node is reliable before sending the identity information of both parties. This scheme realizes the reliability verification of the access nodes through a pre-signature mechanism [16], and authenticates the IoT device through the main signature to realize a highly secure identity authentication. The digital certificate is stored in the form of the Merkle Patricia tree (MPT) [4], which is an improved tree structure that combines the advantages of the Merkel tree and the Prefix tree. The IoT device first verifies whether the key value formed by the query path of the digital certificate in MPT is equal to the hash value of the node public key, and then calculates the MPT root value according to the path hash value of the node. Compare the calculated root with the MPT root value contained in the newly released block, the node identity certificate is valid if they are consistent. Figure 2 illustrates the process of DID management in the main chain.

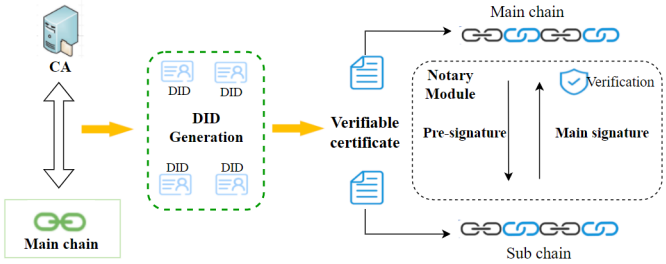


Fig. 2: The DID for cross-chain notary module

The overall workflow of the framework is as follows: The sub chain first requests for a DID and a key pair from the main chain. The DID is associated with the public key and the globally unique identifier for the chain. After the DID and public key are broadcasted, the main chain can provide a set of complete infrastructure for DID generation. When data is uploaded by the IoT device, the gateway will first authenticate the identity and pre-process the raw IoT data. If the IoT device has not been registered on the sub chain, the gateway will interact with CA in the sub chain to register an identity for the device. Then to update the hash of the processed data to the main chain, a transaction request is sent to the notary module. Access nodes from both chains are needed to construct the notary module. In the main chain, the access node is a known node for a specific sub chain. In the sub chain, a ledger query within the chain is executed and the latency is compared with a threshold to decide whether to replace the current access node or not. After the determination of access nodes, cross-chain communication proceeds. The read/write transactions are executed sequentially by the access nodes and are packaged into blocks. The nodes in the notary module will add this block to the blockchain ledger after verifying the transactions. The

client of the sub chain can retrieve the corresponding data and encrypt it using the public key. Then the encrypted data is transmitted to the client of the main chain where the data can be decrypted and a hash value is generated. This hash of the data will be checked to check the integrity and consistency of the data which ensures that the data is neither leaked nor subject to tampering.

B. Node Selection Algorithm

GCN applies the convolution operators to extract spatial features of the topological graph and is proved to be effective in node classification [17]. Since large-scale network with plenty of IoT nodes in distributed geographical positions requires high-efficient interoperation which means the optimal access nodes ought to be selected. Considering both node characteristics and interaction between neighboring nodes, this paper proposes an improved GCN model for the high accuracy of node classification. Three aspects of information are integrated to construct a directed transaction graph with edge information as model input, and an improved GCN architecture is designed for classifying nodes in the sub chain. The overall process is shown in Figure 3.

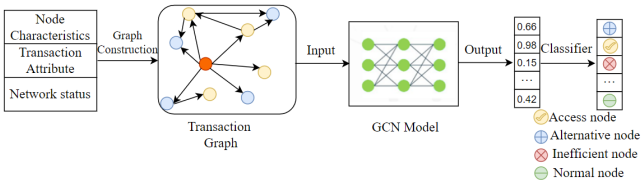


Fig. 3: The node perception algorithm

Graph construction: The transaction graph is constructed by using the characteristic attributes of nodes in the blockchain and the transaction information between nodes. The following four kinds of metrics are represented to construct a graph as model input:

- Node characteristics: The characteristic attribute of the k-th node is expressed as $\vec{v_k} = [f_1, f_2, s_1, s_2]$,
- Adjacent matrix: Since in the transaction graph, different types of edge represent various transactions such as asset transfer, ledger query, and chaincode invoke. Here a set $\{A_1, A_2 \cdots A_r\}$ is used to describe r transaction types of adjacent matrix.
- Transaction delay t_{ij}^r: Except for the node and edge, more information is exploited for accurate classification of nodes. It represents the average transaction delay level from node i to node j of transaction type r which is calculated by averaging the delay and making quantization according to the maximum and minimum of delay.
- Network delay l_{ij}^r: It represents the average network environment delay level from node i to node j of transaction type r which is calculated by averaging the ping value during the transaction.

Graph learning: Based on the transaction graph above, the layer-wise propagation can be treated as a special case of the forward updating process as this formulation:

$$h_i^{(l+1)} = \sigma\left(\sum_{r\in R}\sum_{j\in N_i^r} \frac{\text{Sigmoid}\left(\alpha t_{ij}^r + \beta l_{ij}^r\right)}{c_{i,r}} W_r^{(l)} h_j^{(l)}\right) \tag{1}$$

Where $h_i^{(l)}$ is the hidden state of node v_i in the l-th layer of the neural network. α, β is the weight of transaction delay and network delay. We can adjust the weight according to the environment of the blockchain network, if the network condition is very stable and fast, we could enhance the transaction delay weight and decrease the network delay weight for improving model learning, and vice versa. $\sigma$is activation function. $c_{i,r} = |N_i^r|$ is the normalization coefficient. $|N_i^r|$ is the set of neighboring nodes of v_i for transaction type r. $W_r^{(l)}$ is the weight matrix for the l-th neural network layer belonging to the transaction type r. It is the model parameter needed to be learned from training. The product of the weight matrix and node hidden state can be seen as a process of line transformation of node feature, and for every transaction type, the network shares the weight matrix. The gradient of $W_r^{(l)}$ is calculated from loss, and $W_r^{(l)}$ is updated from the gradient. From the formulation, we can see that the model aggregates different nodes according to different transaction types, it considers not only the connection between nodes but also the relationship type of the transaction.

Node Classification: The model calculates the output and through the softmax classifier, we finally get the classification probability of each node, the vector $\vec{v_k}$ includes the probabilities of classifying the node v_i into t categories, respectively. The maximum probability of the type is the classification result of the node. The access node is chosen to be involved in the notary module for interoperation and the overview of node classification process is shown in Figure 4.

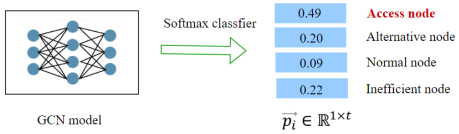
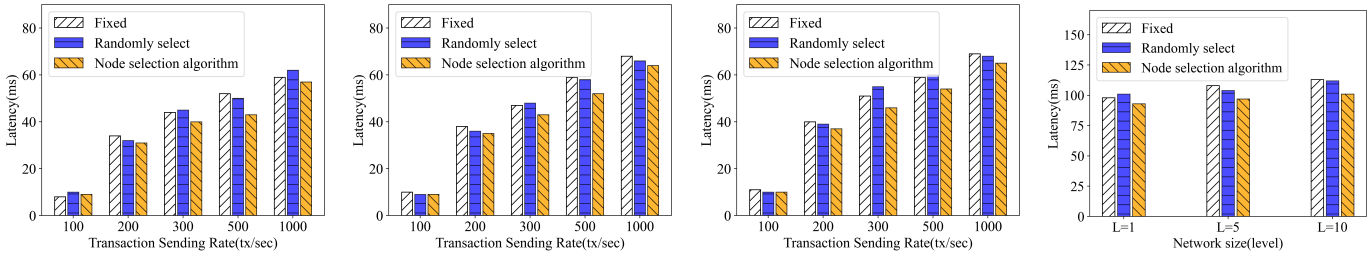


Fig. 4: Classification of sub chain nodes

IV. Results and Discussion

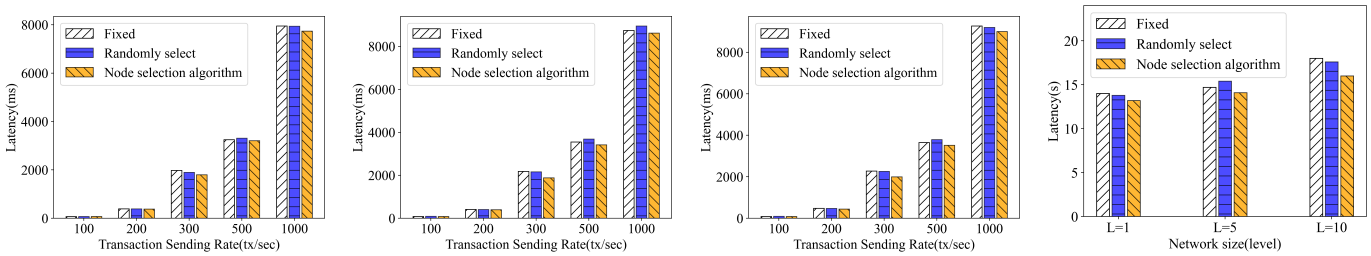
We implemented a prototype of the nested blockchain framework in Hyperledger Fabric v2.4 and the nodes are deployed on five 3.60GHz Intel(R) Xeon(R) 12, Linux Servers (Ubuntu 20.04) with 16GB RAM Memory. Performance for executing transactions between the main chain and the sub chain was tested. Hyperledger Caliper is an official tool that sends different rates of transactions and tests the throughput and latency of writing or reading. Reports produced by Caliper include transaction latency and system throughput which is measured by transactions per second (tps).

We implement a read/write smart contract for the Fabric network and use the read/write operations for testing the latency and throughput. We use L to represent the network size



(a) Latency for reading with L=1 (b) Latency for reading with L=5 (c) Latency for reading with L=10 (d) Latency comparison with different network sizes

Fig. 5: Latency for reading of different cross-chain schemes.



(a) Latency for writing with L=1 (b) Latency for writing with L=5 (c) Latency for writing with L=10 (d) Latency comparison with different network sizes

Fig. 6: Latency for writing of different cross-chain schemes.

for testing different scale networks. The experiments compare the following three different access node selection methods in the nested blockchain system:

1) A fixed access node is used and maintained during all transactions.

2) Randomly select an access node from the sub chain nodes for every transaction.

3) To use the node selection algorithm for selection.

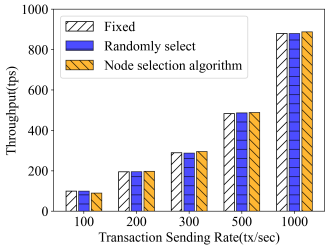
We conduct a series of experiments to evaluate the latency and throughput of the above three methods. The comparisons of latency and throughput in different network sizes are also presented with 2000 transactions sent to the system per second.

A. *Latency*

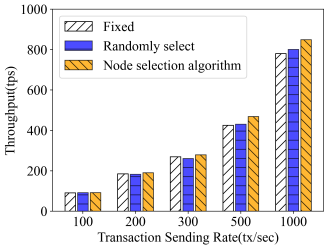
For latency, Figure 5 and 6 report the latency of different access nodes selection methods. The latency for reading operation is relatively lower than writing since the overhead is more caused by the complex consensus execution, encryption, and database interaction, which also results in the rapid increase of latency in writing. There is no absolute superiority in the first two methods. The first one uses a fixed access node which means the latency will be greatly affected when the chosen node has an unstable state. The second one randomly chooses the access node which is also unable to maintain a high level of system performance and the process of replacing the access node takes time. The node selection algorithm ensures the access node is efficient when executing the cross-chain transaction and only make a replacement when it becomes inefficient. The performance of our algorithm is consistently better than the other methods in different transaction sending rates according to the figures. The latency difference for reading operations is higher than that for writing operations due to the congestion caused by the rapid growth in the number of cross-chain transactions waiting in the execution and validation queues. We observe that the increase of the latency is small in both reading and writing when the network scale increases.

B. *Throughput*

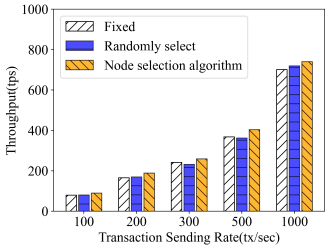
For throughput, Figure 7 and 8 demonstrate the throughput of different access nodes selection methods. The peak throughput is enhanced by using the node selection algorithm but the improvement is less than that in latency. This finding is expected as the current throughput is sufficiently high in the nested-chain architecture which means it is near saturation. On the whole, with the increase in transaction sending rate, the throughput presents a trend that gradually rises and then stabilizes. The experimental results in the figure also show that the difference is slight when the sending rate is low, but with a higher sending rate, system using the node selection algorithm provides more throughput improvements in reading or writing operations since with high efficient access nodes, the probability of transaction failure is lower. Increasing the number of nodes normally significantly degrades throughput, this is because the transaction sequencing, consensus execution, and encryption overhead increase with the increase in the number of nodes. We find that in our nested-chain network, throughput in reading is more robust to the degradation and the performance reduction is within an acceptable range with the scale expansion.



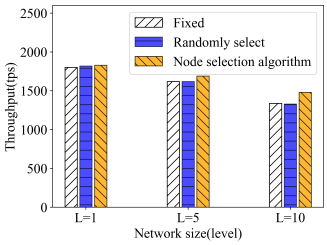
(a) Throughput for reading with L=1



(b) Throughput for reading with L=5

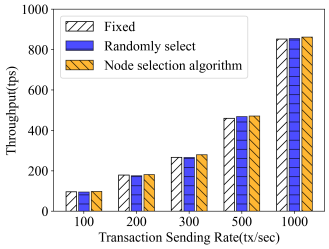


(c) Throughput for reading with L=10

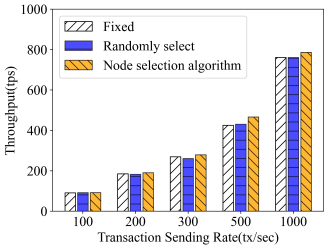


(d) Throughput comparison with different network sizes

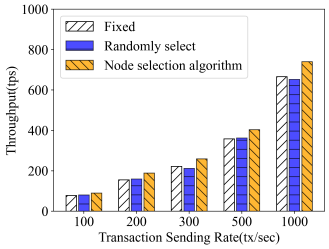
Fig. 7: Throughput for reading of different cross-chain schemes.



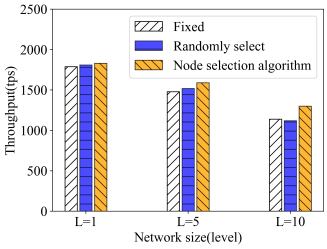
(a) Throughput for writing with L=1



(b) Throughput for writing with L=5



(c) Throughput for writing with L=10



(d) Throughput comparison with different network sizes

Fig. 8: Throughput for writing of different cross-chain schemes.

V. Conclusion

In this paper, a nested blockchain framework for IoT is proposed using a multi-chain architecture, which can ensure the legitimacy of device identity and validity of the cross-chain transaction. A node selection algorithm based on graph learning is designed to select high-performance nodes for low-latency cross-chain communication. The experimental results show that the proposed framework achieves a high level of scalability while maintaining high performance. Compared with the fixed or random access node selection methods, it can enhance the system performance by 23.2% in latency and 12.5% in throughput averagely.

References

[1] A. Gupta, R. Christie, and R. Manjula, "Scalability in internet of things: features, techniques and research challenges," *Int. J. Comput. Intell. Res*, vol. 13, no. 7, pp. 1617–1627, 2017.

[2] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and iot integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, 2018.

[3] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey," *Ieee Access*, vol. 8, pp. 16 440–16 455, 2020.

[4] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," *ACM Computing Surveys (CSUR)*, vol. 54, no. 8, pp. 1–41, 2021.

[5] J. Burdges, A. Cevallos, P. Czaban, R. Habermeier, S. Hosseini, F. Lama, H. K. Alper, X. Luo, F. Shirazi, A. Stewart *et al.*, "Overview of polkadot and its design considerations," *arXiv preprint arXiv:2005.13456*, 2020.

[6] Y. Abuidris, C. Wang, and W. Yang, "Collaborative multi-chain architecture for data transmission across homogeneous blockchain," in *2022 International Conference on Innovations and Development of Information Technologies and Robotics (IDITR)*. IEEE, 2022, pp. 105–110.

[7] C. Pop, M. Antal, T. Cioara, I. Anghel, D. Sera, I. Salomie, G. Raveduto, D. Ziu, V. Croce, and M. Bertoncini, "Blockchain-based scalable and tamper-evident solution for registering energy data," *Sensors*, vol. 19, no. 14, p. 3033, 2019.

[8] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, and M. A. Imran, "A scalable multi-layer pbft consensus for blockchain," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 5, pp. 1146–1160, 2020.

[9] L. Hirtan, P. Krawiec, C. Dobre, and J. M. Batalla, "Blockchain-based approach for e-health data access management with privacy protection," in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. IEEE, 2019, pp. 1–7.

[10] V. Malamas, P. Kotzanikolaou, T. K. Dasaklis, and M. Burmester, "A hierarchical multi blockchain for fine grained access to medical data," *Ieee Access*, vol. 8, pp. 134 393–134 412, 2020.

[11] L. Piccolboni, P. Mantovani, G. D. Guglielmo, and L. P. Carloni, "Cosmos: Coordination of high-level synthesis and memory optimization for hardware accelerators," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 16, no. 5s, pp. 1–22, 2017.

[12] N. Kannengießer, M. Pfister, M. Greulich, S. Lins, and A. Sunyaev, "Bridges between islands: Cross-chain technology for distributed ledger technology," 2020.

[13] H. Wang, Y. Cen, and X. Li, "Blockchain router: A cross-chain communication protocol," in *Proceedings of the 6th international conference on informatics, environment, energy and applications*, 2017, pp. 94–97.

[14] K. Qin and A. Gervais, "An overview of blockchain scalability, interoperability and sustainability," *Hochschule Luzern Imperial College London Liquidity Network*, 2018.

[15] D. Reed, M. Sporny, D. Longley, C. Allen, R. Grant, M. Sabadello, and J. Holt, "Decentralized identifiers (dids) v1. 0," *Draft Community Group Report*, 2020.

[16] J. V. Carcello and C. Li, "Costs and benefits of requiring an engagement partner signature: Recent experience in the united kingdom," *The Accounting Review*, vol. 88, no. 5, pp. 1511–1546, 2013.

[17] T. N. Kipf and M. Welling, "Semi-supervised classification with graph convolutional networks," *arXiv preprint arXiv:1609.02907*, 2016.