International Journal of Web Engineering and Technology

ISSN online: 1741-9212 - ISSN print: 1476-1289
https://www.inderscience.com/ijwet

Cross-chain data exchange and information security protection management in blockchain

Qiong Li, Lei Wang

DOI: 10.1504/IJWET.2025.10067668

Article History:

Received:	25 January 2024
Last revised:	25 July 2024
Accepted:	21 September 2024
Published online:	02 April 2025

Cross-chain data exchange and information security protection management in blockchain

Qiong Li*

School of Management Engineering,
Xuzhou University of Technology,
Xuzhou, 221018, China
Email: liqiong331@163.com
*Corresponding author

Lei Wang

Information Center Yi-Shu-Si River Basin Administrator Bureau,
Xuzhou, 221018, China
Email: wlhpu963@onionmail.org

Abstract: To enhance the security and privacy of cross-chain data exchange, a data exchange and security management protocol based on blockchain is proposed. It utilises a cross-chain channel matching model, employing communication protocols between relay chains and licensed blockchains. A communication protocol based on payment script hashes is designed. Experimental verification demonstrated that the peer matched consensus mechanism of this model has advantages in energy efficiency, decentralisation, and scalability. The proposed communication protocol completed calculations within 3 ms with 10 participants, using a maximum communication overhead of 6 KB. The cross-chain data protection protocol reduced the average exchange time by 9.08% at different problem nodes, achieving a 79% protection effect. Results indicate that the proposed model achieves data information protection during cross-chain exchange, while the communication exchange protocol enhances information security through decentralisation. The data security management protocol reinforces privacy and security in cross-chain exchange processes.

Keywords: internet of things; IoT; blockchain; cross-chain technology; CCT; data information security; consensus mechanism; communication protocol.

Reference to this paper should be made as follows: Li, Q. and Wang, L. (2025) 'Cross-chain data exchange and information security protection management in blockchain', *Int. J. Web Engineering and Technology*, Vol. 20, No. 1, pp.22–42.

Biographical notes: Qiong Li obtained her PhD in Management Science and Engineering from HHU, Nanjing, China in 2022. Presently, she is working as a Lecturer in the Department of Management Science and Engineering, Xuzhou Institute of Technology, Xuzhou. She has published articles in more than ten international reputed peer reviewed journals and conferences proceedings. Her areas of interest include information management and blockchain application.

Lei Wang received his Master's degree in Computer Science and Technology from CUMT, Xuzhou, China in 2008. Presently, he is working as a Professor in the Information Center Yi-Shu-Si River Basin Administrator Bureau, Xuzhou,

China. He has published articles in more than ten international reputed peer reviewed journals and conferences proceedings. His areas of interest are water conservancy informatisation and computer application.

1 Introduction

With the continuous progress of blockchain technology, its characteristics such as decentralisation and tamper resistance have made its role increasingly important in the internet of things (IoT) (Liu, 2021; Aryavalli and Kumar, 2023). The ecological diversity of blockchain has to some extent promoted the flourishing development of blockchain technology, but it has also triggered data and information security. With the complexity and diversification of application scenarios, how to effectively ensure the information security of data exchange while breaking the limitation of 'information silos' has become an urgent problem to be solved (Fotiou et al., 2021; Trofymenko et al., 2021). Cross-chain technology (CCT) can achieve data exchange between blockchains, providing support for data exchange between multi-party blockchains in the IoT (Wei et al., 2023; Yi et al., 2022). However, existing cross-chain technologies often rely on decentralised intermediaries or intelligent protocols, which limit data exchange between heterogeneous chains and cannot guarantee the privacy of data information. Single chain structures are related closed. It is difficult to achieve mutual trust without active interaction with the outside world. Data and information services are limited to each single chain information silo, which greatly hinders the exchange and utilisation of data and information (Bhattacharya et al., 2022). Therefore, the study proposes a data exchange and information security protection management protocol on the basis of CCT in terms of security and privacy of data cross-chain exchange in the IoT, aiming at solving the poor efficiency of data exchange between IoT blockchains built on the basis of licensed blockchain. Firstly, a cross-chain channel matching (CCM) model is constructed based on anchor-relay chain (ARC) and licensed inter-blockchain connection communication protocols (LIBCCP). On this basis, a data exchange and information security protection management protocol with a pre-adapter signature algorithm protocol is further designed.

The data exchange and information security protection management protocol proposed in this study based on CCT combines the relay chain protocol with the Fabric channel concept organically. Moreover, it meets the demand for cross-chain exchange of IoT data in a trusted environment, and strengthens the data cross-chain data exchange by the blockchain characteristics of peer matched channel (PMC). Non-codifiability and security are strengthened by the blockchain feature of PMC. The protocol has feasibility and reliability in cross-chain data exchange in IoT, which has positive significance for the security protection of IoT sensitive data.

The overall framework of the study can be divided into four parts. The first part summarises the achievements and shortcomings of cross-chain data exchange and data information security protection in blockchain both domestically and internationally. The second part constructs a CCM model based on ARC. On this basis, a data exchange and information security protection management protocol is designed. The third part conducts experimental analysis on the data exchange and information security protection

management protocol. The fourth part summarises the research findings and points out the direction for further research.

2 Related works

With the rapid development of blockchain technology, the demand for data exchange between chains is constantly increasing. CCT has emerged in response. CCT aims to connect and integrate these blockchains, forming an interconnected global blockchain network. Domestic and foreign experts have conducted various studies on CCT. Shao et al. (2021) proposed a cross-chain communication mechanism based on identity encryption. The direct cross-chain communication protocols between proxy nodes were designed to solve the difficulty of cross platform blockchain communication. The interoperability and value exchange between different independent blockchain systems limited the blockchain expansion. Therefore, Xiong et al. (2022) proposed a cross-chain interaction model based on notary groups. The data information exchange between different blockchains was achieved through the notary public election mechanism. Jiang et al. (2022) conducted in-depth research on issues such as data integrity verification for cross-chain interaction. From the perspective of chain by chain governance, a decentralised cross-chain data integrity verification protocol was proposed. By incorporating audit summaries into the blockchain transaction structure, the storage burden during the audit process was reduced. Herlihy et al. (2022) proposed a cross-chain transaction concept on how to merge multiple steps into a single atomic operation and how to synchronise concurrent access to data. Based on the proposed synchronous communication foundation, the fully decentralised protocol and semi-synchronous communication protocol were implemented, thus achieving autonomous and trust transactions between blockchains. Dehury et al. (2022) proposed a clustered edge intelligence protocol based on blockchain in order to improve the event diary security of network edge devices. Edge device activity and environmental data are protected from the source device to the cloud server, making the security of edge devices. Al Shahrani et al. (2024) proposed a zero-trust architecture based on blockchain extensions for the limited hardware and software capabilities of IoT devices. The blockchain component provided an immutable database for user storage. Potential malicious user activities were analysed and identified to verify credibility, thereby enhancing the system's resistance to attacks in smart city environments.

The blockchain cross-chain communication protocol is a key interoperability technology in blockchain technology. It is applied to connect and integrate different blockchains, forming an interconnected global blockchain network. Significant research progress has been made in communication protocols both domestically and internationally. Yin et al. (2023) proposed an interoperable communication protocol to address the slow and costly processing of each cross-chain transaction between two or more blockchains. By implementing a two-stage lock/unlock process in an atomic manner, each cross-chain transaction was processed more quickly and inexpensively, resulting in reduced storage and bandwidth overhead in small-scale clients. He et al. (2021) proposed a multi chain charging model to improve the storage and query efficiency of reputation solutions based on blockchain in charging piles. The proposed cross-chain trusted smart contract enhanced the authenticity, real-time performance, and inter chain write/exclude of cross-chain information. The existing cross blockchain asset

transfer protocols overlook the loss during the asset transfer process. Therefore, Sober et al. (2023) developed a cross blockchain asset transfer protocol. The cost and transmission duration of asset transfer protocols were reduced. Abdullah et al. (2022) proposed a framework for deploying discovery services on lightweight nodes registered on blockchain networks, addressing the differences in platform, consensus mechanism, and governance compared with existing systems. Furthermore, it achieved the record integrity of cross-chain transactions between the pending state and the target blockchain confirmation.

From the above, scholars at home and abroad have conducted various studies on blockchain CCT and cross-chain communication protocols. Although some cross-chain data issues have been resolved, most of the results can only be applied to specific token blockchain networks, mainly focused on token or asset data transmission. Under the complexity and diversity of application scenarios, how to ensure the information security of data exchange and break the limitation of 'information islands' is an urgent problem. Existing CCT usually relies on decentralised intermediaries or smart protocols, which limits data exchange between heterogeneous chains. With the continuous development and application of the blockchain ecosystem, the current cross-chain data exchange and information security protection still have the problem of insufficient security. Therefore, a cross-chain data exchange and information security protection management protocol in blockchain is proposed. A cross-chain exchange protocol is innovatively designed to enhance the security protection and management of data information exchange. Through the cross-chain data exchange and information security protection management strategy, it solves the limitations of the existing CCT on the data exchange between heterogeneous chains, improves the information security of data exchange, and breaks the 'information silo'. In addition, to further illustrate the validity of the methodology proposed by the study, it is compared with the existing methods, as shown in Table 1.

Table 1 Comparison of the methodology proposed by the study with other methods in the literature

Research purpose	*Research methodology*	*Limitations*	*Reference*
In order to solve the security authentication problem in IoT environment and the cross-chain communication problem of blockchain platforms	Identity-based cryptographic blockchain communication mechanism for the IoT	Primarily used for token or asset data transmission	Shao et al. (2021)
To realise interoperability and value exchange between different independent blockchain systems	Cross-chain interaction model based on notary group, notary election mechanism, and guaranteed reserved restriction notary mechanism	Depended on the energy efficiency of the notary, with low security efficiency	Xiong et al. (2022)
To ensure data integrity during cross-chain interactions	Decentralised cross-chain data integrity verification protocol	Only integrity verification studies were conducted, not exploring the security of cross-chain data transfers in depth	Jiang et al. (2022)

Table 1 Comparison of the methodology proposed by the study with other methods in the literature (continued)

Research purpose	*Research methodology*	*Limitations*	*Reference*
To enable synchronous access to data	Cross-chain transaction concepts for fully decentralised protocols and semi-synchronous communication protocols on the basis of synchronous communication	Used for specific token blockchain networks	Herlihy et al. (2022)
To improve the event diary security of network edge devices	Cluster edge intelligence protocol on the basis of blockchain	Limitations only for edge device activities from original device to cloud services	Dehury et al. (2022)
To improve the ability of IoT devices to resist attacks	Zero-trust architecture based on blockchain extension	Used for specific token blockchain networks	Al Shahrani et al. (2024)
To improve the ability of cross-chain data exchange and security protection in the blockchain	IoT blockchain data exchange and information security protection management protocol based on CCT, ACR, LIBCCP, and pre-adapter signature algorithm	-	This study

3 Data exchange and information security protection management protocol based on CCM model

A CCT-based IoT blockchain data exchange and information security management protocol is designed for cross-chain data exchange and security protection in blockchain. Firstly, a cross blockchain channel matching CCM model is constructed based on ACR and LIBCCP. On this basis, a data exchange protocol for the pre-adapter signature algorithm is further designed. Finally, a data exchange and information security protection management plan is designed.

3.1 Construction of CCM model based on ARC and LIBCCP

To achieve data exchange across multiple license chains, a cross blockchain channel matching model CCM is constructed. CCM can achieve data information exchange across multiple license chains. Meanwhile, it can also provide security records that prohibit tampering with cross-chain data. It mainly consists of license participation chain, ARC, LIBCCP, and PMC, as shown in Figure 1.

In Figure 1, the license participation chain refers to the license blockchain of many IoT networks that are about to become cross-chain connections. It is built and managed by one or more organisations or institutions. The anchor master node on each chain connects multiple permission chains. Nodes on the chain are authorised and managed by

organisations or institutions. As the core and hub of the CCM model, ARC must pass through all license participation chains to connect with other license chains that have already accepted the LIBCCP protocol. Only anchor master nodes on the chain that have been approved by ARC can generate mapping nodes in ARC, which contain and synchronise on chain information from the original blockchain. The LIBCCP protocol stipulates as follows. When the licensed participation chain is anchored to ARC, the organisers of the licensed participation chain shall pay a fee to ARC as a security deposit for the information authenticity provided by the participation chain and subsequent data exchange. The LIBCCP protocol also defines a Peer Matched (PM) mechanism for managing and matching nodes that have been granted access permission to participate in the chain. The PM consensus mechanism is shown in Figure 2.

Figure 1 CCM model structure (see online version for colours)

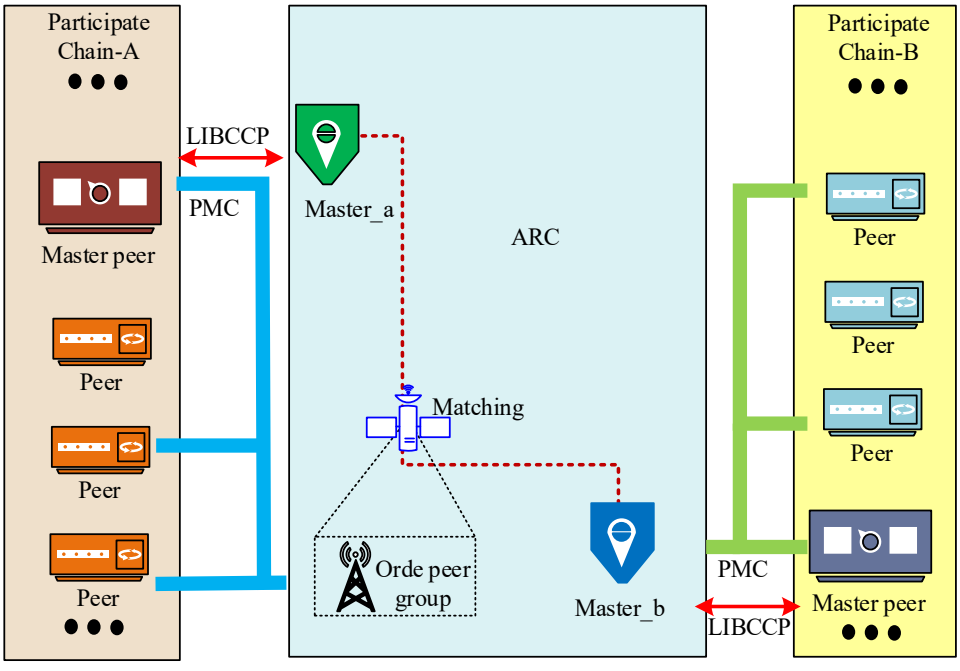
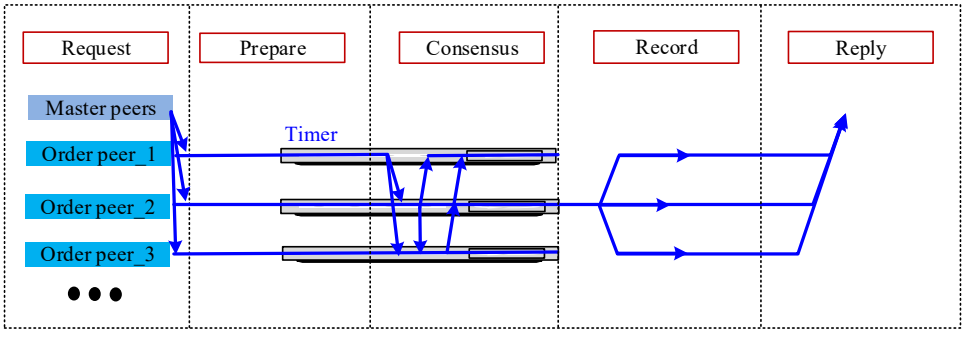


Figure 2 PM consensus mechanism core process (see online version for colours)



The PM consensus mechanism mainly includes five stages: submission, preparation, consensus, broadcast recording, and feedback. In the submission stage, the mapping node is responsible for transferring the basic information of the nodes on the chain to the leader node cluster for selection. In the preparation phase, each leader node in the leader node cluster will randomly select 51% of the valid normal points in their respective licensed participation chains for channel configuration, while timing the consensus phase. Consensus can only be reached when the broadcast information exceeds the maximum fault-tolerant nodes. The PM consensus mechanism can provide fault-tolerant for faulty and malicious nodes (Zhang et al., 2022; Wang and Wang, 2021). When all nodes send their own node authentication information and node public key to the anchor master nodes on their respective chains, the mapping nodes generated by the master nodes on the ARC further obtain information and synchronise, while accepting information review from the leader nodes. Therefore, the information review can be divided into three situations, as shown in equation (1).

$$\begin{cases} Q = f_i & f \neq 0, m = 0 \\ Q = m_i & f = 0, m \neq 0 \\ Q = f_i + m_i & f \neq 0, m \neq 0 \end{cases} \tag{1}$$

In equation (1), Q represents all problem nodes. f represents the faulty node. m represents the malicious node. i represents the consensus node involved. When all problem nodes are faulty nodes, like $Q = f_i$, if there are more effective normal nodes participating in the formula node set than faulty nodes, the nodes that can participate in the consensus process is displayed in equation (2).

$$g = \begin{cases} n_i, & y - f \geq 1 \\ n_i - f_i, & y - f < 1 \end{cases} \tag{2}$$

In equation (2), g represents the node that can participate in consensus. n represents the node participating in consensus. y represents the normal number of nodes. In this case, the maximum fault-tolerant node supported by the PM consensus mechanism is shown in equation (3) (Zhang et al., 2024).

$$x = \frac{(y + f - 1)}{2} \tag{3}$$

In equation (3), x represents the maximum number of fault-tolerant nodes supported. If the number of faulty nodes exceeds half of the nodes participating in the consensus, the consensus will be terminated and the corresponding deposit of the license chain will be deducted. At the same time, the license chain will be urged to rectify the nodes. When the problem node consists of faulty and malicious nodes, like $Q = f_i + m_i$, n_i nodes participate in the consensus only, if the number of y exceeds Q by 1 node. Based on the above, the maximum fault-tolerant nodes that the PM consensus mechanism can support is derived, as shown in equation (4) (Feng et al., 2023).

$$x_{\max} = \frac{(Q + y) + f + m - 1}{4} \tag{4}$$

Figure 3 PMC structure (see online version for colours)

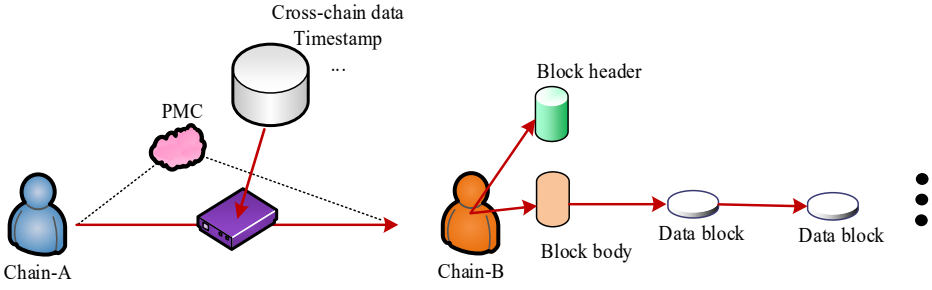
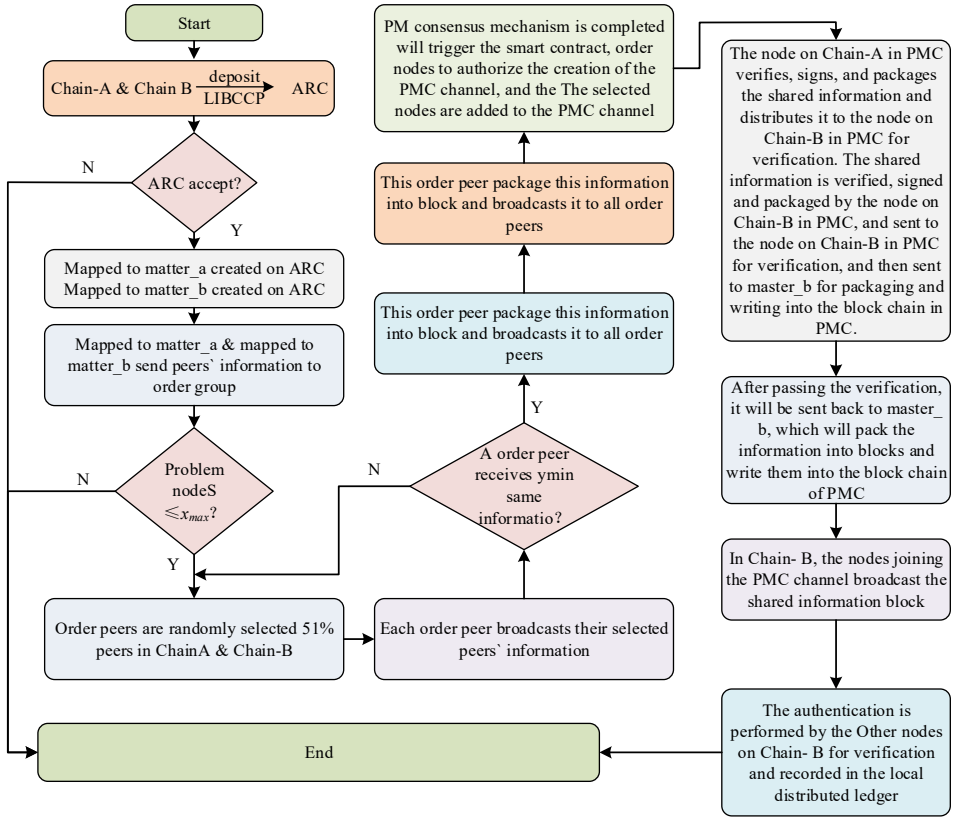


Figure 4 Data exchange process across-chain for the CCM model (see online version for colours)



In equation (4), $x_{\max}$ represents the maximum number of fault-tolerant nodes that the PM consensus mechanism can support. Under the maximum fault-tolerant nodes, the valid normal nodes owned by the permission chain in the PM consensus mechanism are shown in equation (5) (Yang et al., 2022).

$$y_{\min} = \frac{3\left[(Q+y+f+m)+1\right]}{4} \tag{5}$$

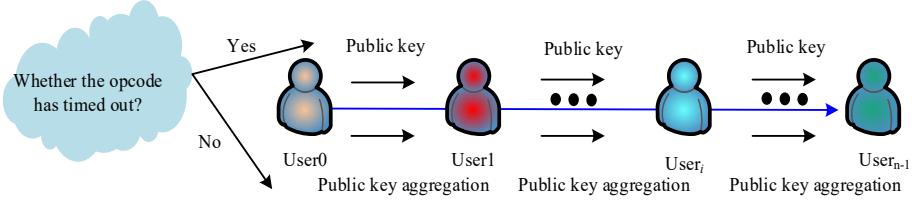
In equation (5), y_{min} represents the minimum number of valid normal nodes under the maximum number of fault-tolerant nodes. After the PM consensus mechanism passes through the core process, the leader node will be authorised to create a PMC between randomly selected participating chain nodes through a smart contract. These nodes will be added to the PMC. The PMC is displayed in Figure 3.

When exchanging data, these data are consensus data in license chain A and have been recorded in blocks. After randomly selecting 51% of normal nodes from chain A within PMC and verifying with the local ledger, the private key signature of the nodes is obtained. The master node is responsible for packaging cross-chain data and broadcasting it within PMC to nodes in chain B for verification. After verification, the master node feedback to chain B is encapsulated and packaged. Then it is linked and broadcasted for recording. In chain B, 51% of nodes within PMC are added. After consensus, cross-chain data is broadcasted to other nodes on chain B. Other nodes then go through the core process of the PM consensus mechanism. The feedback stage obtains the node list and public key of chain A from the leader node to verify the block. According to the above four modules, the running process of the CCM model is shown in Figure 4.

3.2 Data exchange and information security protection management protocol based on CCM model

Based on the CCM model, a cross-chain exchange protocol based on Pay-to-Script-Hash (P2SH) is further designed to optimise the cross-chain exchange. P2SH scripts can be used to specify the identity or payment conditions of participants. It can also generate corresponding payment addresses (Wang et al., 2021; Lee et al., 2021). The main process is shown in Figure 5.

Figure 5 P2SH process (see online version for colours)



Firstly, the first executor of the protocol is User0. The script corresponding to this user contains two public keys. The first executor can negotiate with User1 to generate an adapter signature. The script corresponding to User1 consists of three common parameters that can be negotiated with User2 to obtain a signed valid signature. The scripts corresponding to User$_i$ and the fourth party, User$_{n-1}$, each contain two common parameter combinations. However, traditional adapters cannot achieve orderly protocol execution and continuous online for participants (Attkan et al., 2023; Rosser et al., 2021). Therefore, a pre-adapter signature algorithm based on schnook digital signature is proposed. The Pre-Adapter Signature Algorithm (PASA) is combined with the Multi-Party Adapter Signature Algorithm (MPASA) to construct a secret transmission channel for multiple participants. After the scene setting and preparation stage, in the initialisation stage of MPASA, each participant calculates and broadcasts their respective signature shares. The specific calculation is shown in equation (6).

$$s_i = r_i + c \cdot a_i \cdot p_i \tag{6}$$

In equation (6), s_i represents the signature. r_i represents randomly selected parameters. c represents the global challenge information. a_i represents the public key aggregation parameter. p_i represents the private key. The proposed signature algorithm incorporates secret information during the initialisation phase. Therefore, the initialisation information is shown in equation (7).

$$R = \prod_{i=0}^{n-1} R_i \cdot T \tag{7}$$

In equation (7), R represents the initialisation information. R_i represents the initialisation information corresponding to the participant. T represents the witness information. For the received signature shares, each participant needs to verify their correctness. The verification method is shown in equation (8).

$$g^{si} = R_i \cdot P_i^{c \cdot ai} \tag{8}$$

In equation (8), g^{si} refers to the generator of the signature. P refers to the public key. The correctness verification of adapter signatures for all participants is shown in equation (9).

$$g^{s_{apt}} = \prod_{i=0}^{n-1} \left(R_i \cdot P_i^{a_i \cdot c} \right) = \frac{R \cdot \tilde{P}^c}{T} \tag{9}$$

In equation (9), s_{apt} represents the adapter signature generated after negotiation, corresponding to the secret information. $\tilde{P}$ represents the aggregated public key. Therefore, further algorithm scenario setting and preparation stages are carried out in PASA. Signature parameters and participant signature shares are calculated in the initialisation stage of PASA, as shown in equation (10).

$$\begin{cases} s_h = r_h + c \cdot a_h \cdot p_h \\ a_i = H_{agg}\left(L, T_i\right) \\ \tilde{P} = P_h^{a_h} \cdot P_{h+1}^{a_{h+1}} \cdot \prod_{i=0}^{h-1} T_i^{a_i} \\ R = R_h \cdot R_{h+1} \cdot T_h \cdot \prod_{i=0}^{h-1} T_i \\ c = H_{sig}(\tilde{P}, R, I) \end{cases} \tag{10}$$

In equation (10), h represents the number of participants. I represents a message. H_{agg} and H_{sig} represent hash functions, which are used to calculate aggregation keys and signatures, respectively. L represents an aggregated set of public keys. Based on the received signature shares, all participants can calculate the pre-adapter signature, as shown in equation (11) (Buser et al., 2023).

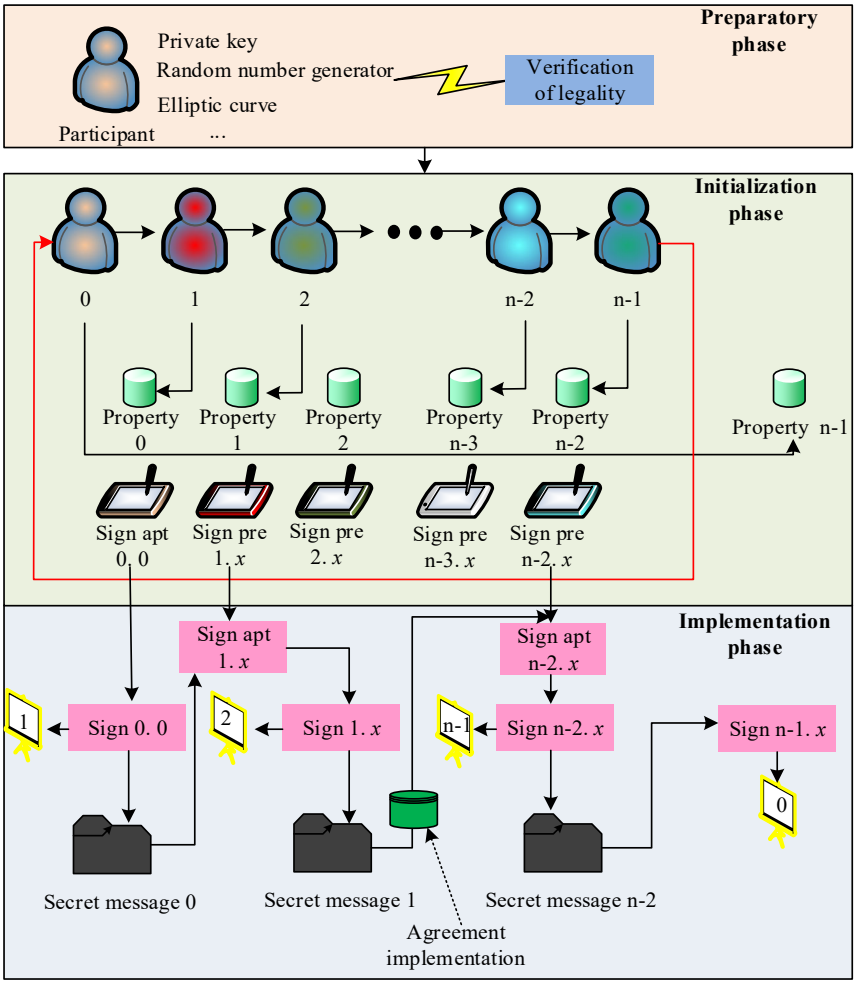
$$s_{pre} = s_h + s_{h+1} \tag{11}$$

In equation (11), s_{pre} represents the signature of the pre-adapter. During the PASA execution phase, all participants can use a secret value list to calculate signature shares

during the initialisation phase. Therefore, the secret information is used as both a public key and a random value at this stage. Then the signature of the adapter is calculated. Therefore, the signature shares during the execution phase is shown in equation (12).

$$s_i = t_i + c \cdot a_i \cdot t_i = (1 + c \cdot a_i) \cdot t_i \tag{12}$$

Figure 6 Protocol initialisation and execution process (see online version for colours)



Based on the signature share, the adapter signature can be further obtained, as shown in equation (13).

$$s_{apt} = s_{pre} + \sum_{i=0}^{h-1} s_i \tag{13}$$

In equation (13), s_{apt} represents the adapter signature during the execution phase. Based on the above calculations, assuming that additional secret information in PASA has been disclosed before the execution phase, the secret information can be dynamically disclosed as the protocol is executed. After collecting enough secret information, the signature of the pre-adapter is further converted into an adapter signature. The execution process of cross-chain exchange protocol is shown in Figure 6.

In Figure 6, during the preparation phase, the protocol ranks participants based on the flow of transaction funds. Participants find the relationship between themselves and various scripts based on P2SH, and complete the secret parameter selection and the common parameter verification. During the initialisation phase, participants generate scripts based on public information and locked funds into P2SH addresses, negotiating the generation order of adapter signatures and pre-adapter signatures in sequence. In addition, the arrows between the participating parties indicate the direction of agreement execution, which is opposite to the flow of funds. During the execution phase, each participant dynamically generates a complete signature by collecting secret information from other participants, and transfers the locked funds in the target P2SH address to complete cross-chain data exchange.

4 Experimental verification of data exchange and information security protection management protocol based on CCM model

To improve the effectiveness of cross-chain secure data exchange and information security protection in the IoT, performance analysis and comparison are conducted on the proposed CCM model. On this basis, the effectiveness of the data exchange and information security protection management protocol proposed in the study is further verified.

4.1 Validation and analysis of CCM Model based on ARC and LIBCCP

The CCM model is subjected to performance testing, mainly testing its request response time. It is compared with current mainstream formula mechanisms. Hyperledger Fabric is used as a license chain for experimentation. On multiple virtual machines, two identical Fabric networks are deployed as validation environments for the experiment. The response time recorded within different concurrency levels is shown in Figure 7.

From Figures 7(a) and 7(b), the response time of the CCM model to read and write to the license chain varied with different concurrency levels. When the concurrency did not exceed 20, the read and response time showed a decreasing trend. The read time was controlled within 300 ms. The read and write time of the CCM model increased correspondingly with the increasing concurrency. The overall write response time tended to stabilise. This may be due to the fact that under the PM consensus mechanism, the read and response time of CCM is affected by the amount of system concurrency. Therefore, the performance of the PM consensus mechanism designed in the CCM model is further compared. The comparison results are shown in Figure 8.

Figure 7 Recorded response time for CCM model with different concurrency levels, (a) CCM models record response times at lower concurrency levels (b) CCM models record response times at higher concurrency levels (see online version for colours)

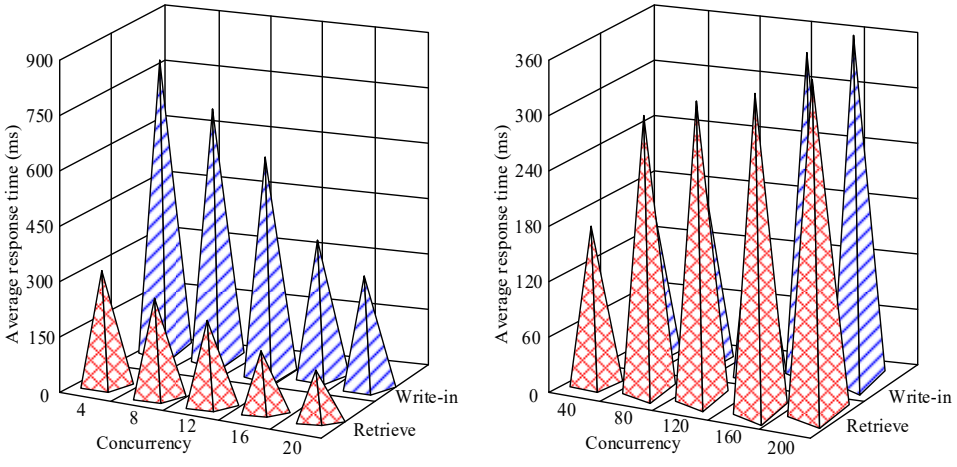


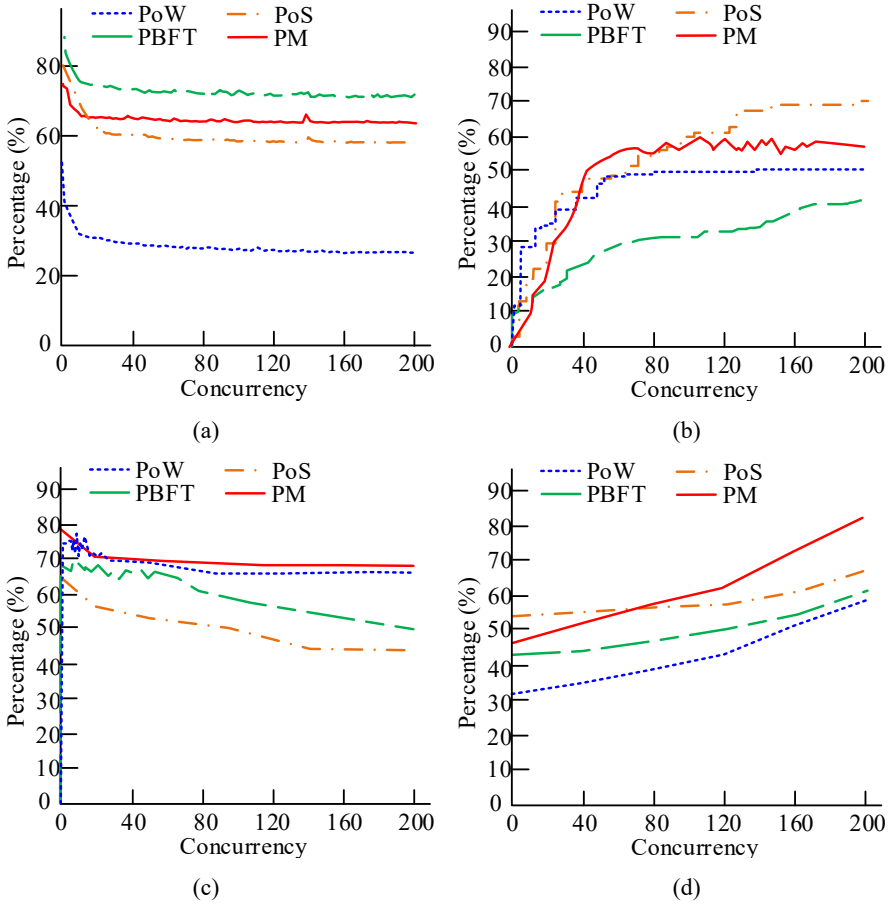
Figure 8(a) shows the energy efficiency comparison of four consensus mechanisms. The PM consensus proposed in the study was significantly better than the proof of work (PoW) mechanism and proof of stake (PoS) mechanism. Practical byzantine fault tolerance (PBFT) consensus mechanism, like PM mechanism, is able to accurately manage the inputs of the nodes. Therefore, it is better in energy efficiency. From the comparison of decentralisation in Figure 8(b), the PM consensus mechanism increased its decentralisation magnitude with the increase of concurrency. When the concurrency reached 200, its decentralisation increased by 44.44% compared with PBFT. Figure 8(c) shows the security of four consensus mechanisms. The security of the four consensus mechanisms decreased to varying degrees with increasing concurrency. From Figure 8(d), the scalability of the four consensus mechanisms increased to varying degrees with the increase of concurrency. Overall, PBET and PM determine bookkeeping rights by verifying a certain number of identical signatures within a limited number of nodes. The PM application scenario involves fewer nodes than PBET, so it consumes relatively fewer resources. PM also has the feature of verifying the same signature information to determine the bookkeeping right, so it is able to carry more transaction volume in the consensus information. Consequently, the PM consensus mechanism of the CCM model proposed in the study can effectively save resource consumption and increase bearable transaction volume in cross-chain mutual trust among multiple license chains. Meanwhile, it can also ensure the security of the cross-chain data exchange process.

4.2 Verification and analysis of cross-chain data exchange protocol based on CCM model

Based on the open-source Schnorr digital signature library, experimental verification is conducted on the proposed cross-chain data exchange protocol. Firstly, the pre-adapter signature algorithm based on Schnorr is instantiated in the Secp256k1 elliptic curve. The protocol running process is tested by simulating the overall process of the cross-chain

protocol. The cost analysis of different participants when the protocol runs smoothly is shown in Figure 9.

Figure 8 Comparison of consensus mechanisms, (a) energy efficiency comparison (b) decentralisation comparison (c) safety comparison (d) scalability comparison (see online version for colours)



From Figure 9, the computational cost of participants 2–8 steadily increased with the number of exchanges. At the beginning of the execution phase, protocol participants with lower execution orders are required to calculate the corresponding secret information and dynamically generated adapter signatures of all previous participants. The time required to generate a key pair was the lowest among all expenses. This is because the key pair belongs to public information in the protocol. The computational workload of all participants is equal, so its cost is the least. When one or more participants are offline, the latter participant needs to utilise more secret values to generate a valid adapter signature. Meanwhile, the network communication cost of different participants is further analysed. Figure 10 displays the results.

Figure 9 Computational overhead of each participant when the protocol is running in its entirety (see online version for colours)

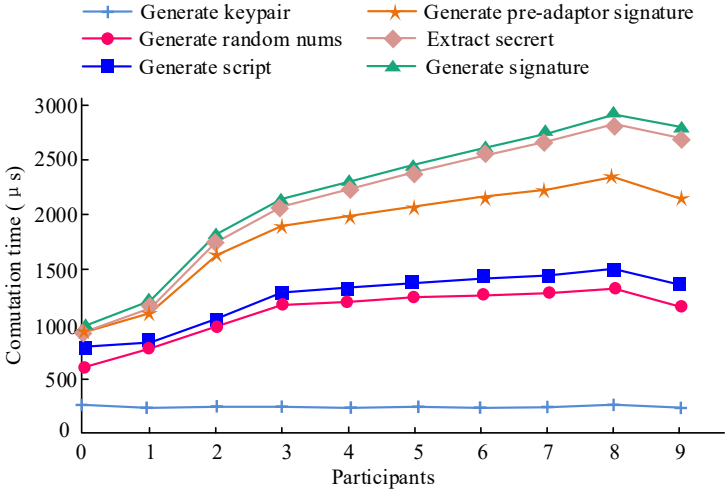
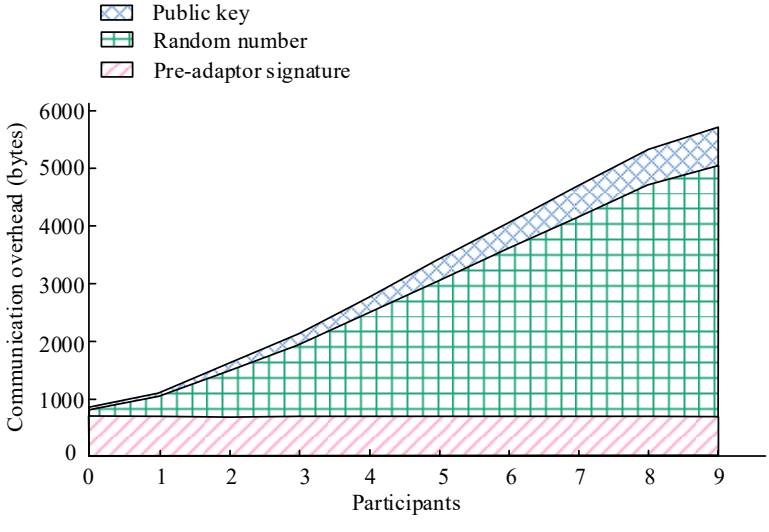


Figure 10 Communication overhead for each user in the protocol initialisation phase (see online version for colours)



From Figure 10, if the order of participants was lower, the required communication overhead was higher, showing a linear increase overall. This is because the participants at the back need to collect more information broadcasted by the previous participants to calculate the secret information hidden in the adaptive signature. However, the P2SH script pre-defined the composition of all common parameters. Therefore, participants can generate all scripts related to the protocol locally. The public key communication overhead of all participants in the proposed protocol was the same. This indicates that corresponding scripts can be generated without broadcasting between all parties involved.

To a certain extent, it ensures the security of data exchange. Meanwhile, it also saves the communication bandwidth consumption.

4.3 Verification and analysis of data exchange and information security protection management protocol based on CCM model

To further verify the effectiveness of the proposed data exchange and information security protection management protocol, it is compared with the commonly used protocols, including notary public mechanism (NPM), trunking program (TP), and sidechain program (SP). The cross-chain data exchange efficiency of the four protocols in different problem nodes is shown in Figure 11.

Figure 11 Comparison of data exchange efficiency in different problem node scenarios, (a) the case where the malicious node is 0 (b) the case where the faulty node is 0 (c) the case where the problem node contains faulty and malicious nodes (see online version for colours)

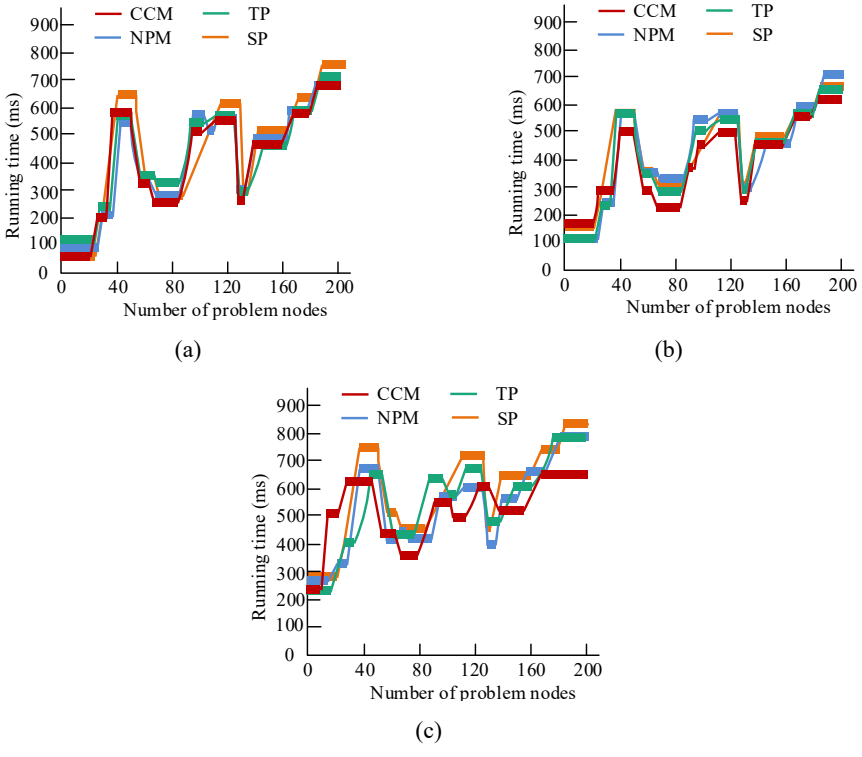
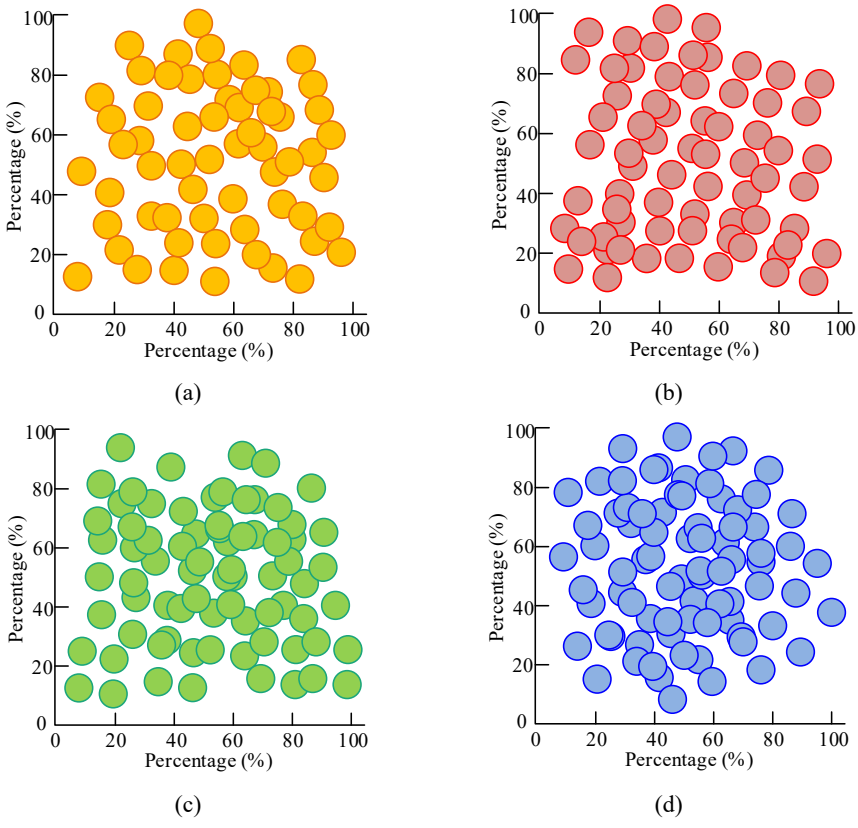


Figure 11(a) shows the exchange efficiency when the malicious node is equal to 0. The running time of the four solutions increased with the increase of the problem nodes. Figure 11(b) shows the cross-chain exchange efficiency when the faulty node is equal to 0. The proposed protocol in the study consumed less time than the other three protocols. When the problem nodes were 200, the CCM protocol reduced by an average of 8.87%. From Figure 11(c), when faulty and malicious nodes in the problem node were not zero, the four protocols required more time to complete cross-chain data exchange. Overall, the

proposed solution required less time at problem nodes. This indicates that it has better security in cross-chain data exchange and more effective information security protection management. Meanwhile, the proposed solution requires a more stable time. In addition, the cross-chain data protection effects of the four protocols are further compared. Figure 12 displays the results.

Figure 12 Comparison of the effectiveness of cross-chain data protection, (a) cross-chain data protection efficiency of NPM (b) cross-chain data protection efficiency of TP (c) cross-chain data protection efficiency of SP (d) cross-chain data protection efficiency of CCM (see online version for colours)



The cross-chain data protection effects of NPM, TP, SP, and CCM protocols are shown in Figures 12(a), 12(b), 12(c), and 12(d), respectively. The protection effect of NPM was about 63%, the TP was about 68%, and the SP was about 72%. The protection effect of the proposed plan was about 79%. NPM achieves cross-chain data exchange by introducing a third-party 'intermediary' that is jointly trusted by both parties in the blockchain to act as a notary public. Therefore, it requires more cross chain exchange time, with poor data protection effectiveness. The TP protocol utilises relay chains as intermediate hubs. Therefore, it requires less time than the other two protocols, but its protection effect is better than NPM. SP is based on anchoring tokens on the main chain. It overly relies on the main chain, but its data protection effect is more ideal than NPM

and TP. Finally, the study further compared the time complexity of the four methods as shown in Table 2.

Table 2 Comparison of time complexity of different methods

Method	*Operational phase (s)*				
	1	*2*	*3*	*4*	*5*
NPM	0.62	0.97	0.94	1.05	1.15
TP	1.01	1.13	1.16	1.48	1.13
SP	1.24	1.34	1.40	1.53	1.24
CCM	0.47	0.95	0.94	1.04	0.97

From Table 2, it can be seen that the time complexity of TP and SP is higher under different operation phases and their operations take more time. The overall time complexity of the research proposed method is 4.37 s, which is 24.66% less than the other three methods on average. This indicates that the time complexity of the method proposed in the study is significantly lower and has less overhead on time. Overall, the cross-chain data exchange and information security protection management protocol proposed in the study has better security and superior protection effect on the cross-chain process of data information.

5 Discussion

The study proposes a blockchain-based cross-chain data exchange and information security protection management protocol, aiming at solving the security problems existing in the current cross-chain data exchange process. By constructing a CCM model based on anchored relay chain (ARC) and licensed inter-chain connection communication protocol (LIBCCP), a cross-chain exchange communication protocol based on payment script hashing (P2SH) is designed. Experimental validation shows that the proposed model has advantages in energy saving, decentralisation and scalability, and can significantly improve the efficiency and security of data exchange. In terms of energy saving and efficiency, PM resource consumption is significantly lower than PoW and PoS, which may be due to the optimisation algorithm of the PM mechanism in dealing with the node consensus process reduces unnecessary computation and communication overheads. The degree of decentralisation of the PM consensus mechanism increases with the increase of concurrency. This indicates that the mechanism is able to effectively handle data exchange in a multi-node environment while maintaining the decentralised nature of the system. By comparing with NPM, TP and SP, the CCM model performs better in terms of data exchange efficiency and protection in different problematic node scenarios. This proves the advantages of the proposed protocol in terms of security and data protection.

However, ensuring the security and efficiency of cross-chain data exchange is a major challenge during the experiments. In addition, designing a protocol that can work seamlessly across multiple network environments and different blockchain platforms is also a technical challenge. In contrast, the study proposes the CCM model and P2SH communication protocol, which not only improves the security of cross-chain data exchange, but also reduces the transaction cost and time delay, which is of great

significance in promoting the application of blockchain technology in IoT and other scenarios. The protocol proposed by the research outperforms existing work in terms of security, efficiency and scalability, providing a more reliable solution for cross-chain data exchange.

Subsequent research will extend the proposed approach in terms of large-scale deployment, compatibility, security enhancement, and performance optimisation. The proposed protocol will be tested and deployed in a larger scale network environment to verify the performance and stability of the proposed method in real applications. By exploring compatibility with more existing blockchain platforms to enable wider cross-chain data exchange. It is expected to further enhance the security, efficiency and practicality of cross-chain data exchange and promote the application of blockchain technology in more fields.

6 Conclusions

A cross-chain data exchange and information security protection management protocol in blockchain was proposed to address the low security in the current cross-chain data exchange process. Firstly, a CCM model was constructed based on ARC and LIBCCP to improve the security of cross-chain data exchange. A cross-chain exchange communication protocol based on P2SH was designed. Experimental validation showed that the PM consensus mechanism in the CCM model could effectively save resource consumption and bearable transaction volume. The proposed communication consensus protocol could complete initialisation and execution phase calculations within 3 ms with 10 participants. The maximum communication cost for participants was 6 KB. The cross-chain data protection protocol proposed in the study required less exchange time at different problem nodes. When the problem node was a faulty node or a malicious node, the average cross-chain data exchange time reduced by 8.87%. The proposed solution had a cross-chain data protection effect of 79%, which was superior to NMP, TP, and SP. The results indicate that the CCM model based on ARC and LIBCCP proposed in the study can securely encrypt data information during cross-chain exchange. The data security protection management protocol can effectively enhance privacy and security during cross-chain exchange processes. However, the proposed solution has not been demonstrated on a large scale. No further research has been conducted on cross-chain exchange between license chains. In the future, data cross-chain exchange will be further analysed to ensure cross-chain security.

References

Abdullah, S., Arshad, J. and Alsadi, M. (2022) ‘Chain-net: An internet-inspired framework for interoperable blockchains’, *Distributed Ledger Technologies: Research and Practice*, Vol. 1, No. 2, pp.1–20.

Al Shahrani, A.M., Rizwan, A., Sánchez-Chero, M., Cornejo, L.L.C. and Shabaz, M. (2024) ‘Blockchain-enabled federated learning for prevention of power terminals threats in IoT environment using edge zero-trust model’, *The Journal of Supercomputing*, Vol. 80, No. 6, pp.7849–7875.

Aryavalli, S.N.G. and Kumar, G.H. (2023) 'Futuristic vigilance: empowering chipko movement with cyber-savvy IoT to safeguard forests', *Archives of Advanced Engineering Science*, Vol. 1, No. 8, pp.1–16.

Attkan, A., Ranga, V. and Ahlawat, P. (2023) 'A rubik's cube cryptosystem-based authentication and session key generation model driven in blockchain environment for IoT security', *ACM Transactions on Internet of Things*, Vol. 4, No. 2, pp.1–39.

Bhattacharya, S., Victor, N., Chengoden, R., Ramalingam, M., Selvi, G.C., Maddikunta, P.K.R. and Gadekallu, T.R. (2022) 'Blockchain for internet of underwater things: State-of-the-art, applications, challenges, and future directions', *Sustainability*, Vol. 14, No. 23, p.15659.

Buser, M., Dowsley, R., Esgin, M., Gritti, C., Kasra Kermanshahi, S., Kuchta, V. and Yu, J. (2023) 'A survey on exotic signatures for post-quantum blockchain: Challenges and research directions', *ACM Computing Surveys*, Vol. 55, No. 12, pp.1–32.

Dehury, C.K., Srirama, S.N., Donta, P.K. and Dustdar, S. (2022) 'Securing clustered edge intelligence with blockchain', *IEEE Consumer Electronics Magazine*, Vol. 13, No. 1, pp.22–29.

Feng, C., Xu, Z., Zhu, X., Klaine, P.V. and Zhang, L. (2023) 'Wireless distributed consensus in vehicle to vehicle networks for autonomous driving', *IEEE Transactions on Vehicular Technology*, Vol. 72, No. 6, pp.8061–8073.

Fotiou, N., Pittaras, I., Siris, V.A., Polyzos, G.C. and Anton, P. (2021) 'A privacy-preserving statistics marketplace using local differential privacy and blockchain: an application to smart-grid measurements sharing', *Blockchain Research*, Vol. 1, No. 4, pp.347–357.

He, Y., Zhang, C., Wu, B., Yang, Y., Xiao, K. and Li, H. (2021) 'A cross-chain trusted reputation scheme for a shared charging platform based on blockchain', *IEEE Internet of Things Journal*, Vol. 9, No. 11, pp.7989–8000.

Herlihy, M., Liskov, B. and Shrira, L. (2022) 'Cross-chain deals and adversarial commerce', *The VLDB Journal*, Vol. 31, No. 6, pp.1291–1309.

Jiang, J., Zhang, Y., Zhu, Y., Dong, X., Wang, L. and Xiang, Y. (2022) 'DCIV: decentralized cross-chain data integrity verification with blockchain', *Journal of King Saud University-Computer and Information Sciences*, Vol. 34, No. 10, pp.7988–7999.

Lee, J.H., Kim, M.J. and Hur, J. (2021) 'Multi-layer bitcoin clustering through off-chain data of darkweb', *Journal of the Korea Institute of Information Security & Cryptology*, Vol. 31, No. 4, pp.715–729.

Liu, Z. (2021) 'Literature review of supply chain finance based on blockchain perspective', *Open Journal of Business and Management*, Vol. 9, No. 1, pp.419–429.

Rosser, J.J.B., Nitsche, L., Yee, G. and Alam, H. (2021) 'The evolution of surgical virtual education and telementoring: one surgeon's journey', *Journal of Surgical Oncology*, Vol. 124, No. 2, pp.162–173.

Shao, S., Chen, F., Xiao, X., Gu, W., Lu, Y., Wang, S. and Mei, F. (2021) 'IBE-BCIOT: an IBE based cross-chain communication mechanism of blockchain in IoT', *World Wide Web*, Vol. 24, No. 5, pp.1665–1690.

Sober, M., Sigwart, M., Frauenthaler, P., Spanring, C., Kobelt, M. and Schulte, S. (2023) 'Decentralized cross-blockchain asset transfers with transfer confirmation', *Cluster Computing*, Vol. 26, No. 4, pp.2129–2146.

Trofymenko, O.G., Yaroslav, D., Loginova, N., Prokop, Y.V. and Zadereyko, A. (2021) Cybersecurity issues of medical computer systems', *Ukrainian Information Security Research Journal*, Vol. 23, No. 1, pp.30–39.

Wang, X., Wang, C., Zhou, K. and Cheng, H. (2021) 'Ess: an efficient storage scheme for improving the scalability of bitcoin network', *IEEE Transactions on Network and Service Management*, Vol. 19, No. 2, pp.1191–1202.

Wang, Y. and Wang, M. (2021) 'Influence dimension and control path of fault-tolerant mechanism: exploratory research based on grounded theory', *Journal of Northeastern University (Social Science)*, Vol. 23, No. 5, pp.39–47.

Wei, H., Qionglu, Z., Wei, O.U. and Wenbao, H. (2023) 'Survey on blockchain-based cross-domain authentication for internet of things terminals', *Computer Science and Exploration*, Vol. 17, No. 9, pp.1995–2014.

Xiong, A., Liu, G., Zhu, Q., Jing, A. and Loke, S.W. (2022) 'A notary group-based cross-chain mechanism', *Digital Communications and Networks*, Vol. 8, No. 6, pp.1059–1067.

Yang, H., Yang, Z., Xiang, S., Zhao, H. and Ackom, E. (2022) 'A double-chain blockchain with economic attributes and network constraints of prosumer transactions', *IEEE Transactions on Industrial Informatics*, Vol. 19, No. 3, pp.2351–2362.

Yi, L., Sun, Y., Duan, L., Ma, H., Wang, B. and Han, Z. (2022) 'Ccubi: a cross-chain based premium competition scheme with privacy preservation for usage-based insurance', *International Journal of Intelligent Systems*, Vol. 37, No. 12, pp.1152–1154.

Yin, L., Xu, J. and Zhang, Z. (2023) 'Interopera: an efficient cross-chain trading protocol', *The Computer Journal*, Vol. 66, No. 7, pp.1609–1621.

Zhang, G., Pan, F., Mao, Y., Tijanic, S., Dangana, M., Motepalli, S. and Jacobsen, H.A. (2024) 'Reaching consensus in the byzantine empire: a comprehensive review of BFT consensus algorithms', *ACM Computing Surveys*, Vol. 56, No. 5, pp.1–41.

Zhang, Z., Guo, B., Zhu, L., Shen, Y., Qin, C. and Li, C. (2022) 'A public blockchain consensus mechanism for fault-tolerant distributed computing in Leo satellite communications', *China Communications*, Vol. 19, No. 7, pp.110–123.

Abbreviated list

Abbreviations	*Full name*
IoT	Internet of things
CCT	Cross-chain technology
CCM	Cross-chain channel matching
ARC	Anchor-relay chain
LIBCCP	Licensed inter-blockchain connection communication protocols
PMC	Peer matched channel
PM	Peer matched
P2SH	Pay-to-script-hash
PASA	Pre-adapter signature algorithm
MPASA	Multi-party adapter signature algorithm
PoW	Proof of work
PoS	Proof of stake
PBFT	Practical byzantine fault tolerance
NPM	Notary public mechanism
TP	Trunking program
SP	Side chain program