International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18 (2026) pp. 1-18

https://doi.org/10.70917/ijcisim-2026-0391
Article

Blockchain-based data protection scheme and cybersecurity framework for housing finance trading platforms

Fang Yang [1,*]

[1] School of Computer Engineering, Shanxi Vocational University of Engineering Science and Technology, Jinzhong, Shanxi, 030619, China
* Correspondence author: jshryf2021@163.com

Abstract: Currently housing finance transaction platforms face challenges of data protection and cybersecurity. Blockchain technology, with its decentralization, non-tampering and high transparency, has become an effective tool for securing transaction data. In this paper, a blockchain-based data protection scheme for housing finance transaction platform is designed, which combines the shared energy storage system and realizes the cyber security protection of the transaction platform by optimizing the PBFT consensus mechanism. Methodologically, distributed file storage technology (IPFS) and smart contracts are adopted to ensure data encryption, storage and transaction transparency. Experimental results show that the proposed scheme excels in smart contract execution time, with a maximum execution time of 0.8ms, and achieves a significant increase in TPS when the concurrent volume of transactions reaches 1,200, and the throughput of the dual-chain architecture is increased by 28% compared to the traditional single-chain architecture. In addition, the system with ITPBFT consensus mechanism reduces the communication overhead by 46.19% compared to the traditional PBFT, and the consensus delay is also significantly reduced, with an efficiency improvement of 53.61%. The study shows that the proposed optimization scheme can enhance the efficiency and reliability of data transactions while improving the security of the system.

Keywords: blockchain, housing finance, smart contract, shared energy storage, PBFT, data protection

1. Introduction

As an important part of China's economic system, the stable and healthy development of the housing market is of vital significance to the smooth operation of the national economy, the protection of social livelihood and the security of the financial system [1-3]. In recent years, with the accelerated digital transformation of the housing industry, housing finance transaction platforms face a series of network data security threats, and the security of housing transaction data has become increasingly prominent [4-5]. In order to ensure the security of users' private information and funds, housing finance transaction platforms must adopt a series of effective data security protection measures [6-7].

Traditional security means have become increasingly difficult to cope with diverse and complex security threats, and the innovative development of security technology is a pressing task [8]. And blockchain technology, as a new type of security assurance tool, has become an important security strategy for information security [9-10]. Blockchain is a secure public database, which can connect transactions or records into a block in chronological order, which in turn constitutes an ordered chain [11-13]. Blockchain technology ensures that records are immutable, transparent, anonymous and distributed [14]. This is because once the data in one of the blocks is tampered with by an attacker, they will find that the hash value of the current block does not match the hash value of the previous block,

and all the blocks following the altered block will also be invalidated, the entire blockchain will be invalidated, and the data will not be able to pass the verification [15-18]. Therefore, blockchain becomes an ideal way to secure digital transactions [19]. And in the field of data security of housing finance transaction platforms, blockchain technology can be applied to data storage, data sharing, and data tracking to ensure data integrity, data transparency, and data security [20-22].

With the rapid development of information technology, blockchain, as a decentralized and tamper-proof technology, has gradually penetrated the financial field, especially the housing finance industry. In traditional housing finance transactions, data protection and security of transactions have always been a common concern for users and platforms. Since housing finance transactions involve a large amount of sensitive information, including user identities, transaction amounts, etc., any data leakage or tampering may have a great impact on the financial market. Therefore, designing a solution that ensures data security and improves transaction efficiency has become an urgent need for current technology development. Currently, the application of blockchain technology in data protection has received widespread attention. Its decentralized nature enables blockchain to avoid single point of failure, and its non-tamperability provides an extremely high level of trust for transactions. However, the performance of blockchain, especially its efficiency in processing large numbers of transactions, remains an urgent challenge. Existing blockchain systems usually suffer from bottlenecks in consensus mechanisms, transaction validation, and data storage, leading to their poor performance in highly concurrent situations. This study will provide an in-depth discussion of blockchain technology in multiple dimensions, including security, efficiency, and scalability. By combining blockchain and shared energy storage system, we propose a novel transaction protection framework, especially optimized on the basis of PBFT consensus mechanism. We adopt the ITPBFT algorithm to improve the efficiency and security of the consensus process by introducing node reputation evaluation and hierarchical mechanism. In addition, IPFS file storage technology is combined in the system to ensure the tamperability and efficient storage of transaction records, which provides more security for housing finance transactions.

2. Design of a blockchain-based secure transaction program for housing finance

In this chapter, based on blockchain technology, the design of shared energy storage secure transaction scheme design for housing finance transaction platform is designed, and the consensus mechanism of data structure on blockchain is optimized, so as to realize the data protection and cybersecurity of housing finance transaction platform.

2.1. Blockchain technology

2.1.1. Accounts and Keys

The digital wallet implemented based on blockchain technology is a secure, convenient and decentralized digital asset management tool with broad application prospects and potential. And the account in a blockchain wallet represents the identity information of each participant for the transactions associated with the account, thus enabling users to access data or resources. Therefore, accounts have an integral role in the transaction process and require keys for their maintenance. Each account is defined by a pair of keys, i.e., a private key and a public key, which are used to encrypt and decrypt data and secure the account. In this case, the private key is a randomly generated string of data, similar to a bank card's PIN, which is unique. The public key, on the other hand, is a private key generated by a cryptographic algorithm, similar to the account number of a bank card. The wallet address on the blockchain is generated by the public key and is the address where the digital currency is received and sent, and is an identifier for the system to interact with. In the blockchain, private keys can generate public keys and addresses, public keys can derive addresses, and all wallet addresses generated by different users are different.

Taking Bitcoin as an example, the detailed process of generating a public key from a private key and a wallet address from a public key is as follows:

(1) First ensure a sufficiently secure source of randomness by utilizing a random function to generate a random number of 256bit length as a legitimate private key $PrivKey$:

$$PrivKey = Random_{256}(seed) \tag{1}$$

(2) Use elliptic curve encryption algorithm [23] to compute the uncompressed public key $PubKey$ of 512bit length corresponding to private key $PubKey$:

$$PubKey = Secp256k1(PrivKey) \tag{2}$$

(3) Then the hash calculation of SHA-256 and RIPEMD-160 is successively performed on the uncompressed public key $PubKey$ to get the 160bit length compressed public key $PubKey'$, and spliced with the Bitcoin blockchain's mainnet version number 0x00 before it to get the public key $PubKey''$:

$$PubKey' = RIPEMD160(SHA256(PubKey)) \tag{3}$$

$$PubKey'' = 0x00 + PubKey' \tag{4}$$

(4) The spliced public key $PubKey''$ is then subjected to two SHA-256 computations to obtain the new public key $PubKey_1''$:

$$PubKey_1'' = SHA256(SHA256(PubKey'')) \tag{5}$$

(5) Then take the first 4 bytes of the public key $PubKey_1''$ as the checksum $check$ and splice it after the public key $PubKey''$ with the version number computed in step (3) to get the public key $PubKey_2''$:

$$check = Calculate_{4Byte}(PubKey_1'') \tag{6}$$

$$PubKey_2'' = PubKey'' + check \tag{7}$$

(6) Finally, the public key $PubKey_2''$ computed in step (5) is Base58 encoded to obtain the final wallet address $Adress$:

$$Adress = Base58(PubKey_2'') \tag{8}$$

2.1.2. Digital crypto tokens

Digital crypto token is a digital crypto asset based on blockchain technology and using cryptography to protect its transactions and issuance, which is decentralized, highly secure, transparent and traceable. Digital crypto tokens use cryptography and a decentralized network to maintain a reliable database and provide greater security for the execution of the transaction process. Digital crypto tokens can be categorized into two types: homogeneous and non-homogeneous tokens.

Homogeneous tokens are tokens that can be copied, exchanged without differences, infinitely divided and reproduced with the same code and identifier, such as Bitcoin and Ether. Homogeneous tokens, also known as decentralized currencies, feature a value structure of simple tokens, risk management capabilities, and fair and transparent transactions. It can effectively guarantee the value of the currency and create a secure and transparent trading environment for different currency models.

Non-homogeneous tokens (NFT) are irreplaceable, each of its tokens is unique, scarce, and cannot be copied, replaced, or divided.NFT is essentially a credible digital entitlement certificate with uniqueness characteristics in the blockchain network, a kind of data object that can be recorded and processed on the blockchain with multi-dimensional and complex attributes to make it a credible credential of authenticity and uniqueness for data assets.

2.1.3. Consensus mechanisms

In a blockchain network, individual nodes communicate and collaborate with each other through specific algorithms and protocols to maintain a reliable and consistent ledger. Due to the decentralized nature of blockchain, no single node can control the entire network, so a mechanism is needed to coordinate the behavior of each node to verify the validity of the transaction and reach a consensus to ensure the security and reliability of the entire network. There are a variety of blockchain consensus mechanisms, of which the most typical are three consensus mechanisms: proof-of-work (PoW) [24], proof-of-stake (PoS) [25], and Byzantine fault-tolerant (PBFT) [26].

In this paper, PBFT consensus mechanism is chosen to design a secure transaction scheme for shared energy storage. Different from PoW and PoS and other economic model-based consensus mechanisms, this mechanism solves the consensus problem with an algorithmic model, which is often applied to coalition chains, and can reach consensus in a few nodes' evil scenarios. Under the PBFT

mechanism, the introduction of redundancy and the voting mechanism ensures that the system still maintains normal operation and reaches a consensus in the presence of node crashes, message loss, or malicious behaviors. And the computational complexity of the algorithm is greatly reduced to polynomial level, which improves the efficiency of the algorithm. Meanwhile, PBFT is suitable for asynchronous environments and can effectively deal with the problems of message loss, delay, repeated propagation and disorder in asynchronous environments.

2.1.4. Smart Contracts

Smart contracts currently refer to digital protocols deployed on the blockchain that can be automatically executed, as well as computer programs that can be automatically executed in accordance with the terms of a predefined contract, with the aim of providing, verifying and enforcing the contract. Its working principle is: through the compiler and virtual execution environment, the smart contract with well-written business logic is deployed on the blockchain, in which the contract content sets up and encapsulates a number of predefined states, transition rules, trigger conditions and execution logic, and when the instruction is received, the smart contract is triggered, and automatically judged by the state machine, the computer system automatically executes the functional logic in the form of a transaction by the node through the consensus mechanism. After verification and packing into the block, the execution result is finally recorded in the chain.

2.1.5. Cross-chain mechanisms

(1) Notary mechanism

The notary mechanism is a cross-chain technology with more applications and easy to implement in data asset cross-chain transaction projects. This technology is based on one or more trusted third parties listening to events on different chains automatically or on request, and verifying the transaction events through preset consensus algorithms to ensure that these events are executed and eventually responded to in time, and according to the number of notary publics, it is divided into: single-signature notary public mechanism, multi-signature notary public mechanism and distributed multi-signature notary public mechanism.

(2) Hash lock

Hash locking is a cross-chain transaction method using hash function and smart contract, the technology by the transaction data for hash calculation, each of the assets held by the lock, when and only when the original value of the correct hash value obtained in the required time, you can unlock an equal amount of assets on the target chain, realizing the exchange of assets between different blockchains.

The detailed steps for the realization of hash locking technology are as follows:

1) The initiator of the transaction chooses a random number r and transcodes it with a hash function to obtain the hash value h.

2) The initiator sends the hash value h to the receiver for subsequent asset locking.

3) The initiator will take the hash value h as a parameter and call the smart contract to realize the asset locking on the chain, meanwhile, set the locking time t_1, and promise the receiver: within the stipulated time t_1, return the original value r of the hash value, and then you can get the assets of the initiator.

4) The receiver obtains the hash value h, calls the smart contract to realize the asset locking on the chain, and at the same time sets the locking time t_2, and promises the initiator: within the specified time t_2, sends the original value of the hash value r, and then can obtain the assets of the receiver side.

5) In the end, both parties to the transaction obtain the original value r within the specified time, unlock the assets on the two chains, and complete the cross-chain transaction.

(3) Sidechain/Relay Mechanism

Sidechain and relay cross-chain technologies are two technical solutions to achieve interoperability between different blockchains, with each implementation having its own focus. Sidechain technology aims to create a logical sub-chain that keeps information in sync with the main blockchain, realizing the function of on-demand asset transfer between the two chains. The technology is a relatively independent technical solution, which can independently define the rules and mechanisms of asset transfer, and can also choose different blockchain parameters and consensus algorithms. Sidechain technology can realize cross-chain transfer and exchange of assets and improve interoperability and scalability between blockchains. Relay chain is a more centralized cross-chain technology solution,

which can not only support a variety of different blockchain protocols and asset types, but also realize the transfer and exchange of assets between different blockchains. The advantage of relay chain is that it is more centralized and can realize more complex cross-chain interactions and operations.

(4) Distributed private key control

The principle of distributed private key control is to carry out distributed management of the ownership of assets on the blockchain and the right to use them. Distributed private key control manages private keys through distributed nodes, maps user assets to the blockchain that complies with cross-chain protocols, and deploys new smart contracts to create new cryptocurrency assets based on the relevant information of cross-chain transactions. The execution of distributed private key control technology is divided into two main steps:

1) Digital asset management: the key corresponding to the asset is split and processed, and the subkey is managed by the system node, followed by transferring the asset to the specified storage address for locking, and there are and only enough nodes sharing the subkey to recover the key corresponding to the asset, so that the asset can be unlocked and released.

2) Bookkeeping: After the transfer of assets is completed, the smart contract is triggered to update the accounts of distributed nodes in real time. This cross-chain technology benefits from the distributed fragmented storage of private keys, which makes cross-chain transactions highly secure, decentralized and scalable, and supports the transfer and exchange of assets between different blockchains.

To illustrate with an example of user A exchanging n bitcoins (BTC) with user B's m ethereum (ETH) assets, the operation process is as follows:

Step1: User A, located in the original Bitcoin chain, sends a cross-chain operation request to the cross-chain system.

Step2: The system generates the key pair $(Pub_A, Priv_A)$, where the public key Pub_A serves as the address of one of user A's asset transactions in the Bitcoin system $Addr_A$, while the private key $Priv_A$ is split into k copies and distributed to the cross-chain system of Each node participant, and each reference keeps only 1 of the fragmented keys.

Step3: The cross-chain system sends $Addr_A$, i.e., the public key $Priv_A$, to user A.

Step4: User A deposits n BTC into the transaction address $Addr_A$.

Step5: The cross-chain system verifies the transactions in $Addr_A$, and locks the assets therein if there is no error.

Step6: Similarly, user B sends a cross-chain operation request to the cross-chain system.

Step7: Similarly, the system generates a key pair $(Pub_B, Priv_B)$, and the public key Pub_B is used as the address of one of user B's asset transactions in the Ether system $Addr_B$, whereas the private key $Priv_B$ is split into k parts and distributed to each node participant in the cross-chain system. to each node participant in the cross-chain system to save the fragmentation key.

Step8: Similarly, the cross-chain system sends $Addr_B$, i.e., the public key Pub_B, to user B.

Step9: User B deposits m ETH into the transaction address $Addr_B$ and locks the asset after verifying that the transaction is correct.

Step10: Through the distributed private key management algorithm, the cross-chain system recovers the private keys $Priv_A$ and $Priv_B$ of user A and user B respectively through the key management participant, and then sends $Priv_A$ to user B, and sends $Priv_B$ to user A, thus user A can get m ETH, while user B will get n BTC, realizing the cross-chain transaction of assets.

Comparing the four mainstream cross-chain mechanisms, it can be seen that distributed private key control technology does not rely on centralized third-party media, adopts key sharing algorithms instead of the traditional asset cancellation/activation transfer method, and also supports the issuance and circulation of tokens based on smart contracts, which has strong security, atomicity and scalability. Therefore, this study decides to adopt distributed private key control technology to realize the construction of cross-chain transaction system.

2.2. Program design based on a shared energy storage security trading system

This study implements the data protection scheme and cybersecurity framework design for housing finance trading platforms by designing a blockchain-based secure trading system for shared energy storage.

2.2.1. System program architecture

The system covers five parts: application layer, business layer, file storage layer, smart contract and blockchain layer, as well as three entities: user node, owner node, and energy storage power station node. The application layer is the interaction entrance between users or owners and the system, where user or owner nodes can complete operations such as uploading transaction information, uploading and querying file indexes, and amount transactions. The business layer is centered on cryptographic encryption and decryption algorithms. When the user or owner node submits important transaction records, the system encrypts them before storing them to ensure data security. When nodes on both sides of the transaction retrieve the file, the system carries out decryption processing. The file storage layer is integrated into the distributed interplanetary file system (IPFS). Owner nodes encrypt the transaction information before submitting it and upload it to IPFS to ensure safe storage, tamper-proof, and also highly secretive and arbitrable to safeguard the integrity and credibility of the transaction records. The system sets up automatic operations, such as identity verification, amount transactions, etc., which are automatically executed under the premise of decentralization with the help of smart contract module. Blockchain layer, users share order record index information in IPFS, introduce IPFS to store encrypted order records, and upload retrieved information to the blockchain through smart contracts to realize distributed storage, reduce overhead and improve efficiency. The system program architecture is shown in Figure 1.

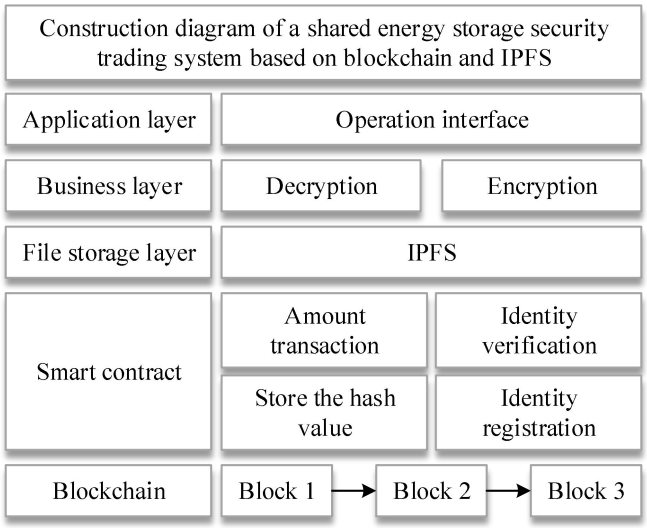


Figure 1. System construction diagram

2.2.2. System processing flow

During the transaction process, the user node encrypts the transaction information including the user's private information such as address, type of energy storage and demand using the public key of the owner node and then sends the encrypted information with the account address to the owner node. The owner node decrypts the transaction information, integrates it into an order and encrypts it again, stores it in IPFS, and sends the encrypted order index information generated by IPFS to the user. The user confirms the order and completes the payment operation through the system transaction interface. After the payment is completed, the owner node verifies the correctness of the user's payment amount through the blockchain and authorizes the energy storage plant to deliver the energy storage in accordance with the amount of electricity recorded in the transaction information. After the energy storage is delivered, the user node needs to authenticate itself through the system interface to obtain the authority to modify the energy storage status. Finally, the smart contract automatically completes the owner's withdrawal operation according to the energy storage status. The system processing flowchart is shown in Figure 2.

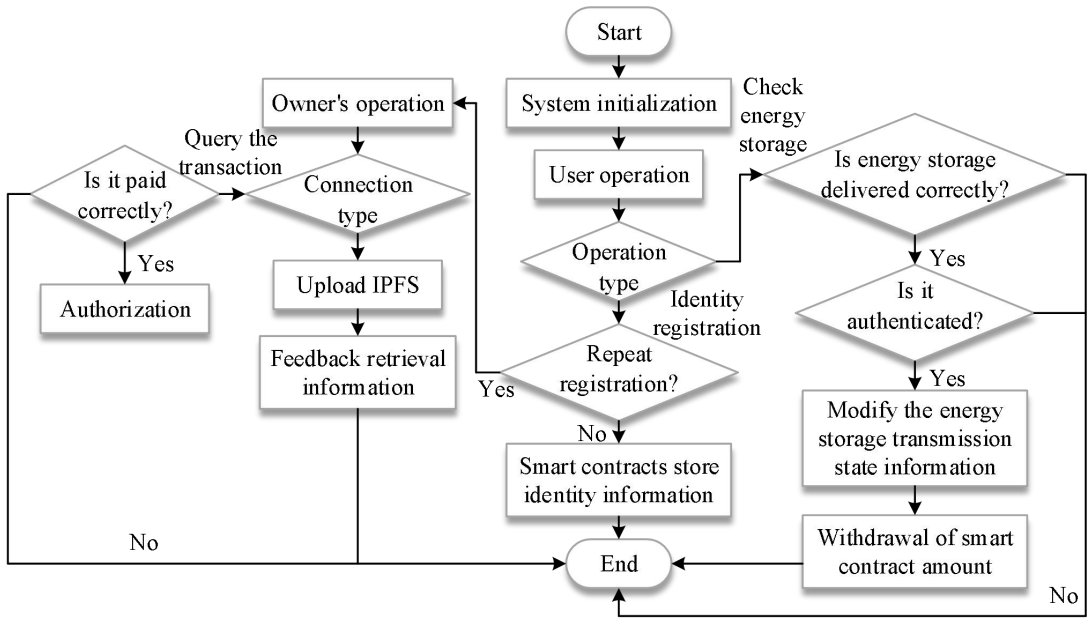


Figure 2. System processing flowchart

2.3. Optimization scheme of consensus mechanism based on on-chain data structure

In order to further ensure the effectiveness of the system, as well as the security of the network and data of the housing finance trading platform, this section proposes an optimization scheme for the PBFT consensus mechanism, ITPBFT, on the basis of the on-chain data structure, combined with the P2P reputation model [27].

2.3.1. Consensus mechanism optimization scheme

The overall process of ITPBFT program is a three-phase cycle of "assessment-monitoring-implementation", which includes the steps of credibility assessment, node level differentiation, timeout monitoring, credibility updating, restoration and rewards/punishments, etc. The system flow of ITPBFT program is shown in Figure 3. The system flow of ITPBFT program is shown in Figure 3.

The details of the three phases of the ITPBFT scheme are as follows:

1) Evaluation phase. The evaluation phase includes a total of two aspects, namely, reputation evaluation and node level differentiation. The scheme evaluates each node within the blockchain system according to its consensus behavior through the P2P reputation evaluation model, and then differentiates the nodes into different levels based on the evaluation results of the system.

2) Monitoring phase. The monitoring phase is mainly for system consensus timeout monitoring, if the system consensus timeout fails, it will be replaced to the next view and a new consensus master node will be selected.

3) Implementation phase. The implementation phase mainly includes several aspects of reputation updating, restoration and rewards and penalties. The system introduces a real-time reputation update system, which realizes real-time update of node reputation according to the node's behavior in each round of consensus. At the same time, the system introduces the node reputation incentive system, which is divided into the reputation restoration system and the reputation reward and punishment system to ensure the initiative of the nodes in the consensus, and prevent the high-reputation nodes from behaving lazily or the low-reputation nodes from behaving negatively in a continuous manner.

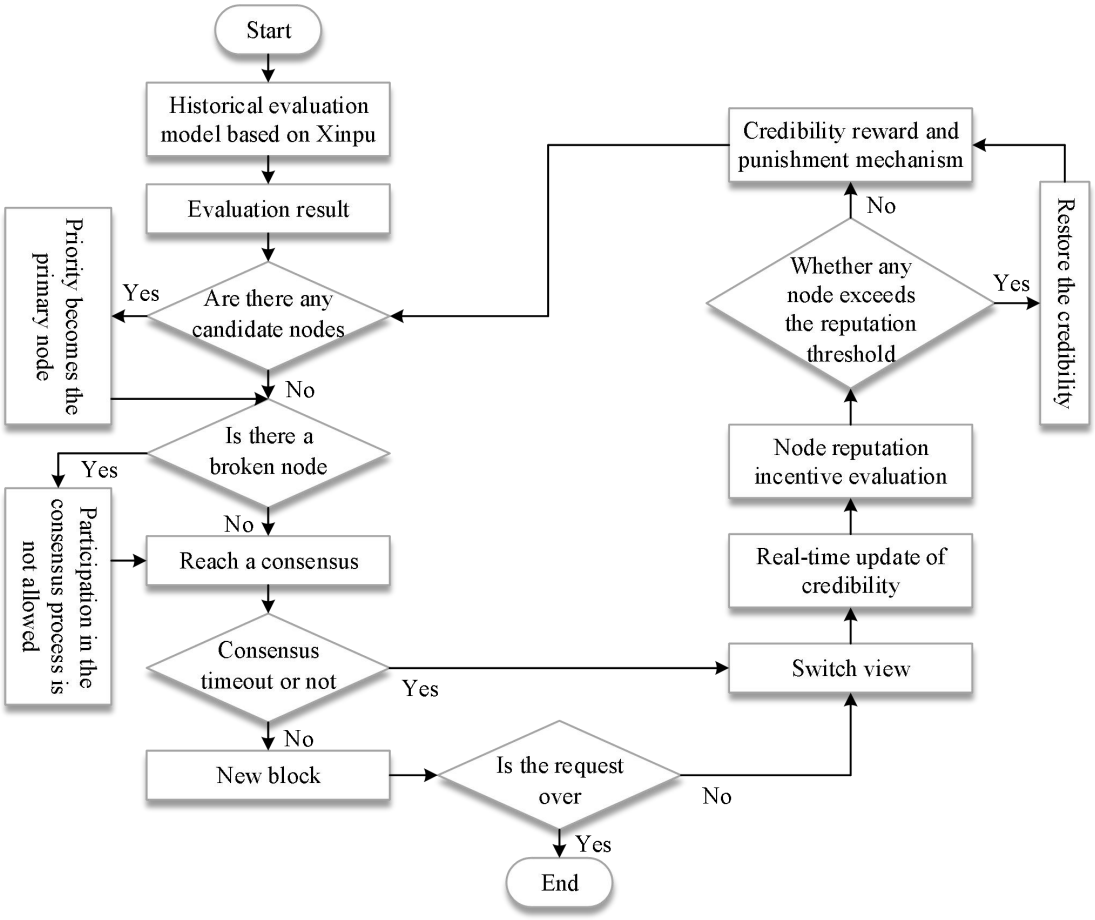


Figure 3. Flowchart of ITPBFT

2.3.2. Relevant systems

This section introduces the relevant systems of the optimization scheme ITPBFT. Specifically, it includes: reputation-based evaluation system, node hierarchy system and node reputation incentive system. The node hierarchy changes are shown in Fig. 4.

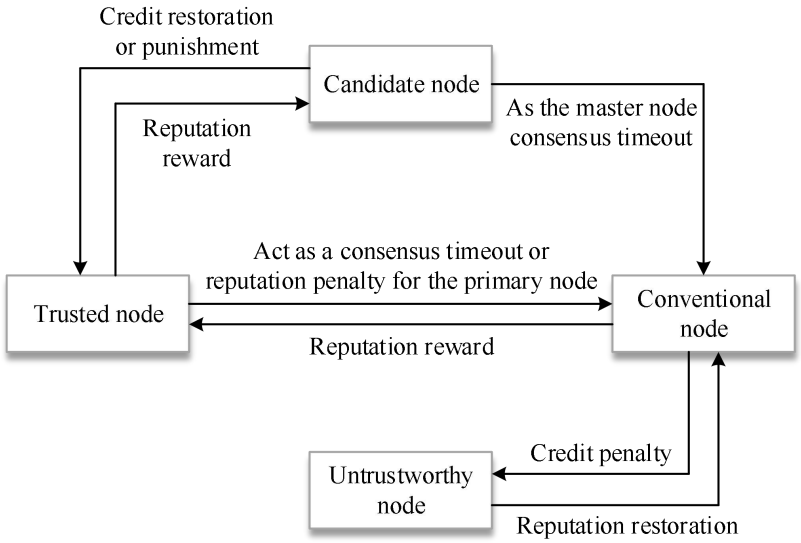


Figure 4. Changes in node levels

(1) Reputation-based evaluation system

Reputation model is to formalize reputation by way of mathematical model, mainly from the node

or user's attributes related to reputation to measure its reputation, and the current main reputation models include distributed reputation model and centralized reputation model. This chapter proposes a reputation-based evaluation system based on the Peer Trust distributed reputation model, combined with the PBFT consensus mechanism.

Definition 1: Node reputation evaluation model

The current status of a node's reputation is evaluated through a reputation model. The reputation evaluation model of node i is as follows:

$$Reputation_i = \alpha * S_i + \beta^* D_i^t + \gamma^* I_{ik} \tag{9}$$

$Reputation_i$ is the evaluation index of the current reputation status of node i, which mainly includes three parts: the reputation history evaluation S_i of node i, the reputation real-time evaluation D_i^t of node i and the reputation incentive evaluation I_{ik} of node i, respectively. The α, β, γ are the corresponding weight values of the historical evaluation S_i, the real-time evaluation D_i^t, and the incentive evaluation I_{ik}, respectively.

Definition 2: Node Reputation Historical Evaluation Model.

The reputation of a node is evaluated based on its performance in historical consensus. The following is the reputation history evaluation model S_i for node i:

$$S_i = \lambda^* A_i + \mu^* C_i \tag{10}$$

The reputation history evaluation S_i of node i mainly consists of two parts, the historical behavior factor A_i and the historical participation factor C_i in the consensus process, λ, μ are the weights of A_i and C_i respectively.

Definition 3: Historical behavior factor

Evaluating a node i based on its positive or negative behavior in the historical consensus process, this metric mainly indicates the impact of node i 's historical consensus behavior on its reputation evaluation, as follows as the historical behavior factor A_i:

$$A_i = \frac{\delta^* T_{is} - \varepsilon^* T_{if}}{T_i} \tag{11}$$

where T_{is} denotes the number of rounds that node i has behaved positively in the historical consensus cycle, T_{if} denotes the number of rounds that node i has behaved negatively in the historical consensus cycle, δ, ε are the weights of T_{is}, T_{if} respectively, and $\delta + \varepsilon = 1$, such that $T = T_i + T_{if}$, and T_i denotes the total number of historical consensus in which node i has participated.

Definition 4: Historical Participation Factor

This metric is mainly used to evaluate the historical activity level of a node. The following is the historical participation C_i of node i:

$$C_i = \frac{T_i}{T} \tag{12}$$

where T is the total number of rounds of consensus within the blockchain system in the past time period, and T_i is the total number of rounds of consensus in which node i has participated in total during this time period.

Definition 5: Reputation real-time evaluation

This metric evaluates the value of a node's reputation in real-time based on the node's behavior in each consensus round during the current consensus cycle. The real-time evaluation of the reputation of node i, D_i^t, is expressed as follows:

$$D_i^t = \begin{cases} \dfrac{\sum_{j=1}^{n} \dfrac{\sum_{k=1}^{m} f(k) * D_{ij}^{t_k}}{m}}{n} & m \neq 0 \\ 0 & m = 0 \end{cases} \tag{13}$$

Node i and node $j(j \neq i)$ are two nodes in the blockchain system, n is the total number of nodes within this blockchain system, and t is the consensus cycle requested by the client. In the process of real-time evaluation of node reputation, m denotes that a total of m rounds of consensus process have been carried out in the request cycle t, k denotes the k th round of consensus process, and $D_{ij}^{t_k}$ denotes the reflective evaluation of node j on node i in the k th round of consensus process. $f(k)$ is the time decay factor, which is mainly used to indicate that the consensus processes conducted at different times have different effects on the reputation evaluation, and $f(k)$ can be expressed as:

$$f(k) = \rho^{m-k} (0 < \rho < 1, 1 \leq k \leq m) \tag{14}$$

Definition 6: Reputation incentive evaluation

An incentive evaluation is performed on node i based on its performance in the current consensus cycle. Combined with the node's consensus performance in the cycle, the reputation reward and punishment is carried out to motivate its positive behavior, the reputation incentive evaluation I_{ik} of node i is denoted as follows:

$$I_{ik} = \begin{cases} \sin \dfrac{(1 - Reputation_{k-1})\pi}{2} & \text{(Positive behavior)} \\ \sin \dfrac{(-Reputation_{k-1})\pi}{2} & \text{(Negative behavior)} \end{cases} \tag{15}$$

The model $Reputation_{k-1}$ denotes the reputation of node i updated in real time at the end of the last consensus round.

(2) Node reputation hierarchy

The scheme introduces the node reputation hierarchy, which combines the reputation of nodes and categorizes them into the following four categories in the order of reputation: candidate nodes, trusted nodes, regular nodes, and discredited nodes, etc. The node reputation hierarchy is shown in Table 1.

Table 1. Node reputation rating system

Node type	Reputation threshold	Node function		
		Priority becomes the primary node	Become the master node	Become a replica node
Candidate node	$(T_{pri}, 1)$	√	√	√
Trusted node	(T_{cred}, T_{pri})	×	√	√
Conventional node	(T_{com}, T_{cred})	×	×	√
Untrustworthy node	$(0, T_{com})$	×	×	×

(3) Nodal reputation incentive system

Node reputation incentive system contains two aspects such as reputation restoration system and reputation reward and punishment system.

Definition 7: Node reputation restoration system

The system mainly regulates the problem of over- or under-reputation of nodes in the system through the method of reputation reduction. When the updated reputation value N_i of a node T_i is higher than the system's maximum reputation threshold of 1, the system will restore a part of the node's reputation so that the node's reputation will be replaced with T_{cred} and the node will be converted into a trusted node to prevent nodes with too high a reputation from centralizing or behaving lazily. When

the updated reputation N_i of a node T_i is lower than T_{com}, the node is prohibited from participating in the next round of consensus of the system, and when the rest of the nodes complete the real-time evaluation of their reputation at the end of the next round of consensus of the system, the node's reputation will be restored and replaced by T_{com}, and the node will be converted to a regular node,. Thus, it improves the initiative of low reputation nodes and prevents such nodes from doing continuity negative behavior in the subsequent consensus.

Definition 8: Nodal reputation reward and penalty system

The node reputation reward and punishment system mainly contains the following aspects:

1) If a candidate node, trusted node or regular node behaves positively in the last round of consensus, the node receives a reputation reward, and there is no reputation reward for a trustworthy node since it is prohibited from participating in the last round of consensus.

2) If a node behaves negatively as a sub-node during consensus, the corresponding reputation penalty will be enforced by deducting a certain amount of reputation.

3) If a candidate node or trusted node is selected as the master node to participate in the consensus, if the negative behavior of the node in the previous round of consensus causes the consensus timeout to fail, the node will be recognized as a regular node after the replacement of the view, and it will lose its eligibility to be the master node in the next round of consensus.

3. Experimental analysis

In this chapter, the designed blockchain-based shared energy storage secure transaction scheme is tested for performance and security analysis, and the performance of the proposed consensus mechanism optimization scheme ITPBFT is analyzed through comparative experiments.

3.1. Performance testing experiments of the program

The scheme proposed in this paper uses simulation experiments to test the relevant performance, the PC uses i7-10700 CPU, 16GB running memory, 300Mbit/s network bandwidth, Raspberry Pi 4B ARM development board, server builds Ubuntu 22.04 LTS system, and programming tools use Visual Studio Code. The program is divided into 3 main aspects: smart contract performance test, zero-knowledge proof efficiency test, and game profit distribution change test.

3.1.1. Smart Contract Performance

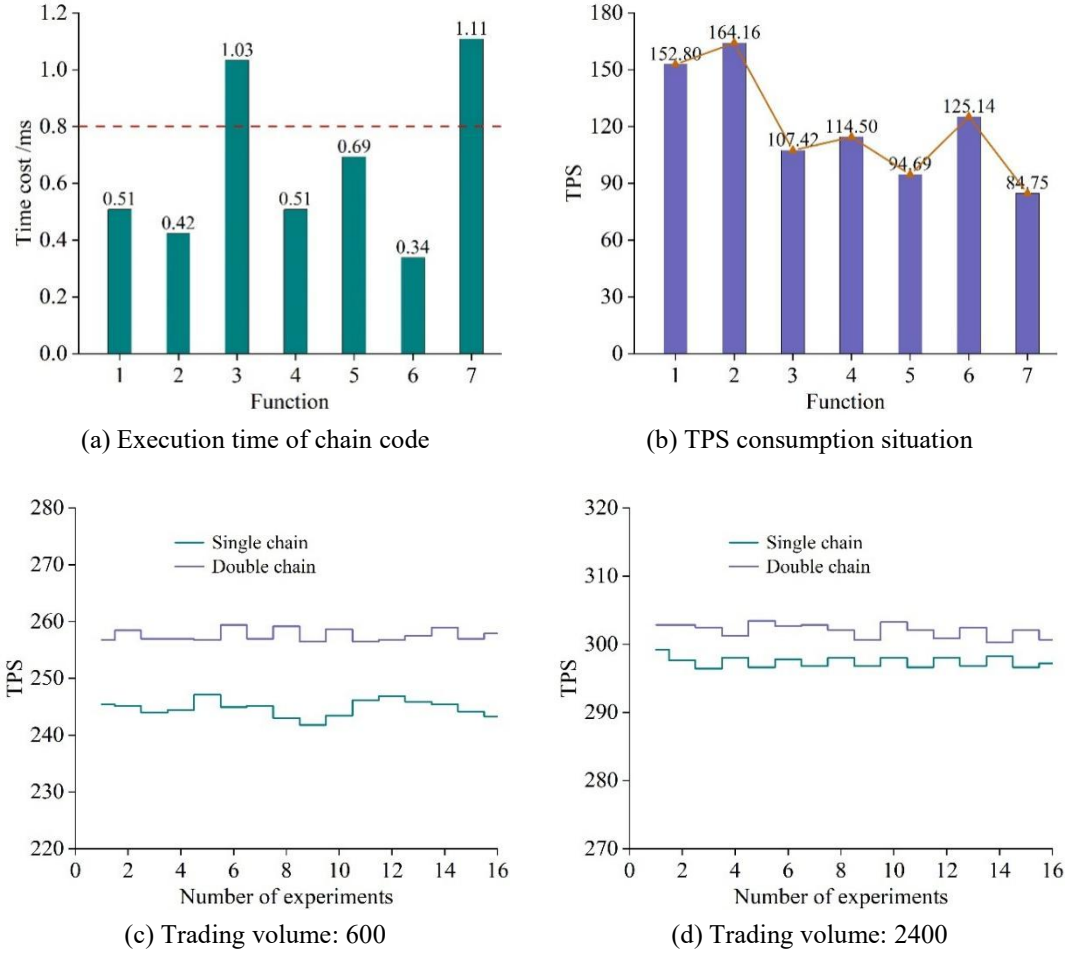
The blockchain platform for housing financial transactions is constructed using the federated chain architecture Hyperledger Fabric V1.4, 200 physical nodes are constructed using Raspberry Pi to simulate the transaction environment, smart contracts are written using Golang in combination with JavaScript, and dual-chain interactions are carried out through the cross-Channel approach. In this paper, we test the running time and throughput TPS of the smart contracts used in the scheme, test the advantages of the dual-chain architecture compared to the single-chain, test the generation and validation time of the zero-knowledge proof under different numbers of leaf nodes, and finally test the profits of the data owner as well as the distributor in the case of using a two-stage Stackelberg game.

The multimedia data transaction process simulation for housing finance transactions is performed using Caltech-256, a publicly available dataset containing 30428 images. The results of the smart contract performance test are shown in Figure 5.

Fig. 5(a) and (b) show the execution time as well as TPS test results of the smart contract, which tested seven main functions, namely: data owner registration, buyer registration, data search, dealership price agreement, perceived hash detection, main chain data transaction, and node zero-knowledge proof validation, which are denoted by the numbers 1 to 7. It can be seen that, except for data search as well as zero-knowledge proof verification, the execution time of other smart contracts is below 0.8ms. The data search in this scheme uses text vectors to compare the cosine distance, all vectors are stored in the ledger through smart contracts, and the five data with the largest similarity are obtained through cosine similarity calculation, i.e., top-5 search, and the time consumption increases with the increase in the number of vectors, and the number of vectors set up in the experiments is 2,400. In terms of the TPS test, since the size of the concurrent transactions has a significant TPS impact, the transaction size set in the experiment is 1200, and larger transaction concurrency means larger TPS.

Figure 5(c) and (d) shows the TPS comparison results of this paper's scheme using dual-chain and single-chain architectures under three nodes, corresponding to 600 transaction volume and 2400 transaction volume, respectively, mainly reflecting the impact of perceived hash on throughput with the increase of transaction volume under dual-chain and single-chain. Through the experiment, it can be seen that the larger the transaction volume in the case of TPS has a greater improvement, and

dual-chain query compared to single chain has obvious advantages.



(a) Execution time of chain code

(b) TPS consumption situation

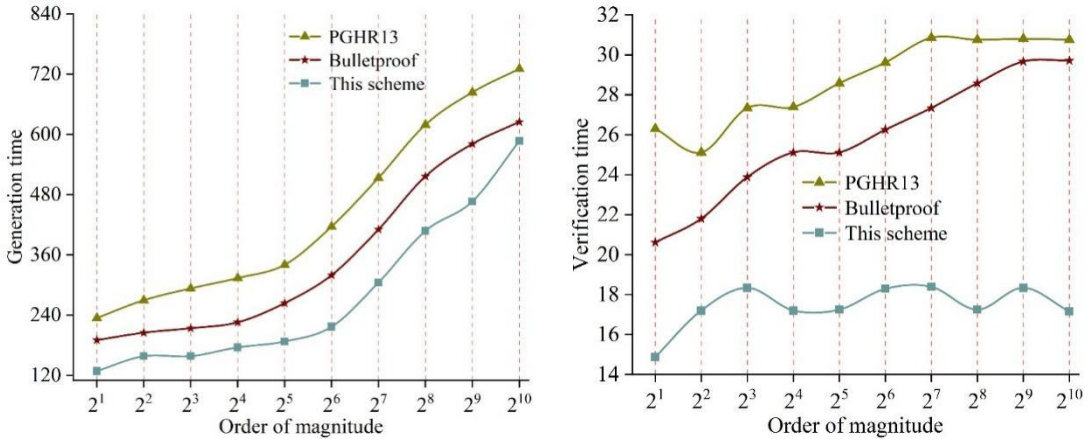
(c) Trading volume: 600

(d) Trading volume: 2400

Figure 5. Test results of smart contract performance.

3.1.2. Zero-knowledge proof efficiency

Compared to the mainstream zero-knowledge proof frameworks PGHR13 and Bulletproof, the scheme in this paper simplifies the steps of sending the commitment value, and the range of fluctuation of the proof generation time as well as the verification time is smaller with the increase of Leave value. The results of the efficiency test of the scheme in terms of generation time as well as verification time with the same Leave value are shown in Fig. 6, with (a) and (b) denoting the generation time and verification time, respectively. The experiment proves that the scheme in this paper has significant efficiency improvement in generation as well as verification time compared to the existing schemes. It should be mentioned that since the scheme proposed in this paper is based on zero-knowledge proof of blockchain, the time efficiency improvement will be more obvious with the increase of the number of IoT nodes under the federation chain architecture.



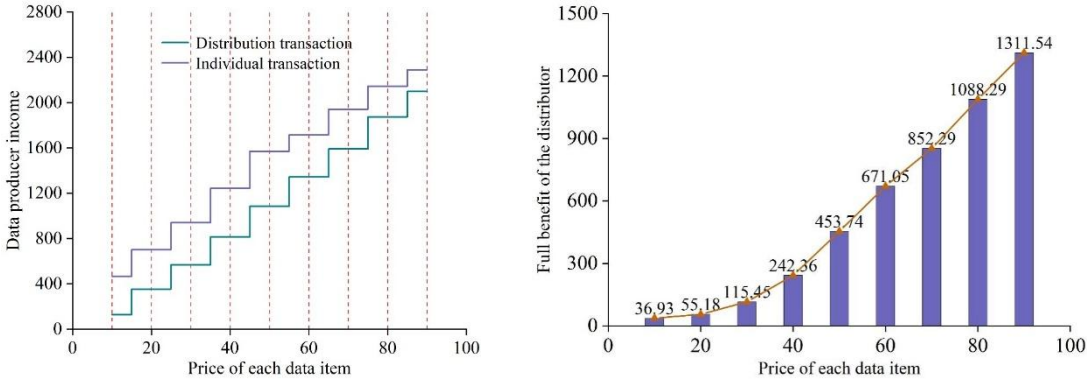
(a) Generation time comparison (b) Comparison of verification time

Figure 6. The test results of time efficiency

3.1.3. Changes in the distribution of gaming profits

In the case where the price of the data item increases and the revenue profit share remains constant, the profit income of the participants is shown in Fig. 7, where (a) shows the profit after the data owner sells the data alone and after joining the reseller, and (b) shows the change in the total profit of the reseller when the price of the data is increased and the revenue gained by the reseller from selling the data r_{ik} remains unchanged.

It can be seen that there is a significant increase in the profit of the data owner after the inclusion of the reseller. Meanwhile, the profit of the reseller shows a linear increase with the increase of the price of the data item. Through simulation experiments, it can be seen that this paper's scheme in the use of two-stage Stackelberg game to introduce dealers for the sale of data effectively enhances the profit of the participants and can promote the vitality of the market.



(a) The changes before and after the introduction of dealers (b) Change in total profit

Figure 7. The profit income situation of the participants

In addition, this paper's program uses the interstellar file storage system IPFS to store the data, and builds IPFS private nodes locally. Due to the large capacity of audio and video in multimedia data, this paper tests the data upload and download speed of 1-10GB and compares it with the efficiency of FTP file download and upload, which shows that the efficiency of IPFS is significantly higher than that of FTP, indicating that the use of IPFS provides a safer storage environment while the efficiency is also guaranteed.

3.2. Security analysis of the program

This section analyzes the possible security threats of the designed solution and shows the advantages of the solution in terms of security.

3.2.1. Risk of collusive attacks

In the data transaction scenario constructed by this scheme, there may be a collusion attack in which the reseller conspires with the end customer to bypass the data owner's authorization and confirmation, resell without authorization or buy the data at a price lower than the standard price, thus harming the rights and interests of the data owner. This collusion attack can be effectively avoided by a dual-chain anchored data transaction model. Specifically, the data owner can view the data transactions in the main chain to determine whether their data is normally traded, and the transactions are permanently recorded and traceable in both the side chain and the main chain, thus protecting against the risk of collusion attacks.

3.2.2. Risk of repudiation and entrapment

Repudiation is when a data purchaser who is not a qualified reseller does not admit or denies the transaction record after being caught illegally reselling the data. Framing is when a data owner constructs the same perceptual hash to frame an innocent purchaser. For denial, the dual-chain architecture stores all transactions and perceived hashes in a trustworthy and traceable manner, so that purchasers with illegal behavior cannot deny their actions. The data owner has uploaded the perceived hash value of the data before uploading the data to IPFS, and each transaction corresponds to a perceived hash value and a corresponding purchaser, and there is no illegal distribution behavior of unbound users. Moreover, under the dual-chain architecture, the users need to register and purchase the distribution qualification on the side chain before they can transact, so the scheme prevents the risk of repudiation and framing.

3.2.3. Risk of data loss

In this paper, the program uses IPFS, a distributed storage environment, to store data, compared to traditional cloud platforms, IPFS does not have downtime risk, once the data is stored that is permanently stored, and returns a unique storage address hash, the data owner will encrypt the hash using their own private key and store it in the ledger, and the buyer can only decrypt the data after getting the corresponding public key through a smart contract, so there is no risk of data loss in the program. There is no risk of data loss in the program.

3.3. Performance analysis of ITPBFT consensus algorithm

This chapter implements a blockchain simulation system using the Go language based on the experimental configuration used in the previous section. In this simulation system, this paper evaluates the performance of the PBFT, ITPBFT, P-PBFT and C-PBFT consensus algorithms by setting different numbers of nodes. In the experiments in this section, these algorithms are tested and analyzed mainly in terms of consensus latency, throughput and communication overhead.

3.3.1. Communication overhead

Communication overhead is the amount of communication generated during the execution of the consensus algorithm by the nodes.PBFT algorithm is a consensus algorithm based on the exchange of information, so the amount of communication becomes one of the important indexes for evaluating the algorithms of PBFT class.

In this experiment, this paper tests the single consensus communication volume of three consistency algorithms. The initial number of nodes is 120 and the number of groups is 30, and the test is subsequently conducted with every additional 120 nodes and 15 groups. The comparison of communication overhead of different algorithms is shown in Fig. 8.

It can be observed that as the number of nodes increases, the communication overhead of the three consistency algorithms increases accordingly. It is worth noting that the communication overhead of the ITPBFT algorithm in this paper is always lower than that of the C-PBFT and P-PBFT algorithms, and the advantage of the ITPBFT algorithm becomes more obvious as the number of nodes increases. When the number of nodes increases to 600 and the number of groups is 90, the communication overhead of the ITPBFT algorithm is reduced by 38.14% compared to the P-PBFT algorithm and 61.38% compared to the C-PBFT algorithm. When the number of nodes is increased to 1200 and the number of groups is 165, the communication overhead of ITPBFT algorithm is reduced by 46.19% as compared to P-PBFT algorithm and 64.17% as compared to C-PBFT algorithm.

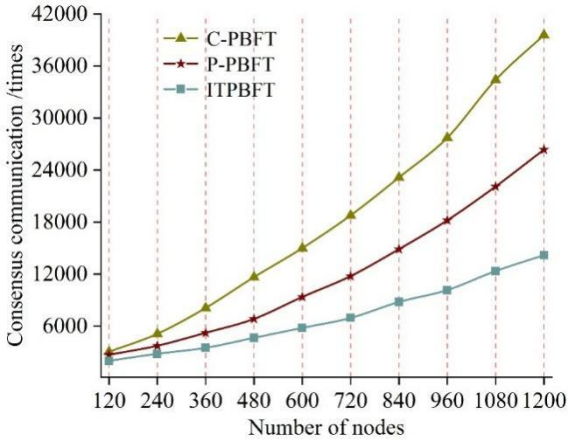


Figure 8. Comparison of communication overheads of different algorithms

3.3.2. Time delay analysis

Consensus latency is an important indicator of the consistency algorithm, which refers to the time required from the time the client sends a transaction request to the time the transaction is completed. Lower latency represents shorter execution time of the consensus algorithm, higher consensus efficiency, faster nodes in the network reach consistency, and more secure and efficient system operation. In order to evaluate the blockchain network under different number of nodes, this paper chooses a uniform grouping number of 10 and conducts 300 tests for different node scenarios. The maximum and minimum values are removed after every 30 experiments and the average value is taken as the experimental result.

The comparison of consensus latency of different algorithms is shown in Fig. 9. It can be observed that the consensus latency of the PBFT algorithm is significantly larger than that of the C-PBFT, P-PBFT and ITPBFT algorithms for the same number of nodes. This is due to the fact that the latter three use group consensus, which can significantly reduce the communication overhead in the consensus process. As the number of nodes increases, the latency of all four algorithms increases. However, it should be noted that the IT-PBFT algorithm shows the slowest increase. In particular, when the number of nodes is 220, the consensus latency of the IT-PBFT algorithm is reduced by 53.61% and 68.85% compared to the P-PBFT algorithm and the C-PBFT algorithm, respectively.

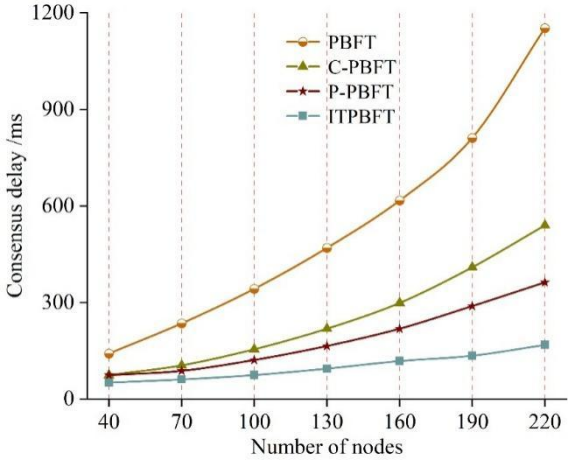


Figure 9. Comparison of consensus delay among different algorithms

3.3.3. Throughput analysis

TPS is the number of transactions that a system can complete per second. In blockchain systems, TPS reflects the ability of the system to process transactions and the high throughput.

The TPS of PBFT class algorithms is related to the number of nodes within the network, and when the number of nodes is high, the TPS will decrease significantly due to the increase of communication overhead. In the throughput experiments, this paper still chooses a uniform number of groups of 10 and conducts 300 tests for different node scenarios. The maximum and minimum values are removed after

every 30 experiments, and the average value is taken as the experimental result, and the TPS comparison results of different algorithms are obtained as shown in Fig. 10.

It is observed that the TPS of PBFT, C-PBFT, P-PBFT and ITPBFT decreases gradually with the increase in the number of nodes. Notably, the TPS of PBFT decreases most significantly when the number of nodes increases from 40 to 130. Although C-PBFT and P-PBFT have slower decreases relative to PBFT, their decreases are still significant compared to ITPBFT.ITPBFT is able to maintain a slower decrease as the number of nodes gradually increases. This is because ITPBFT combines a P2P reputation evaluation model with a node hierarchy, selects nodes with high reputation to become consensus master nodes, and introduces a reputation incentive system to realize real-time changes in node reputation. This mechanism not only ensures the accuracy of consensus, but also reduces the communication overhead and improves the throughput of the blockchain system. In addition, this feature of ITPBFT can also meet the demand for high-frequency transactions in distributed housing finance transactions.

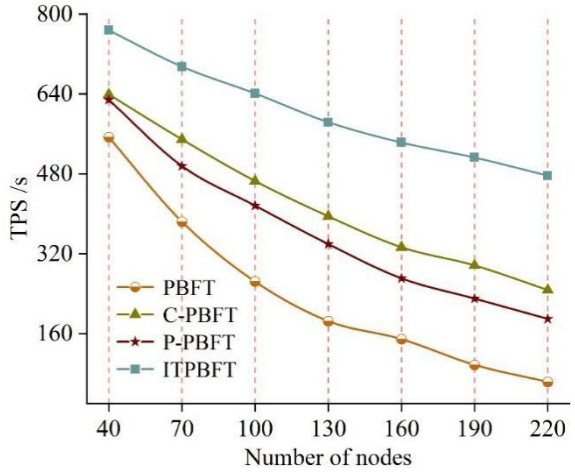


Figure 10. Comparison of TPS among different algorithms

4. Conclusion

The blockchain-based shared energy storage secure transaction scheme designed in this research excels in both data protection and transaction efficiency. By using distributed file storage and smart contract technology, the system is able to ensure the transparency and security of housing finance transactions. Experimental results show that when the transaction concurrency reaches 1,200, the maximum execution time of the smart contract stays within 0.8ms, and the throughput (TPS) is increased by 28% compared with the traditional single-chain architecture. In addition, the adopted ITPBFT consensus mechanism reduces the communication overhead by 46.19%, and the consensus delay is 53.61% lower than that of the traditional PBFT, which effectively improves the processing capability of the system. Further security analysis shows that the system is able to effectively prevent collusion attacks, denial and framing behaviors, and eliminates the risk of data loss by using IPFS storage technology.

These experimental data show that this scheme not only solves the security problems existing in traditional housing finance transaction platforms, but also provides higher efficiency and scalability in large-scale transaction scenarios. Therefore, the blockchain-based shared storage security transaction system provides a reliable and efficient data protection solution for the housing finance industry and lays a technical foundation for the digital transformation of the financial sector.

Funding

Project No.: 202204031401130

Project Title: Strategic Research on Cyber Security Innovation Talent Alliance Based on Regional Economy in Shanxi Province

Project from: Science and Technology Department of Shanxi Province, Technology Strategy Project

References

1. Xiang, G., Tang, J., & Yao, S. (2022). The Characteristics of the Housing Market and the Goal of Stable and Healthy Development in China's Cities. Journal of risk and financial management, 15(10), 450.
2. Borgersen, T. A. (2016). Housing appreciations and the (in) stable relation between housing and mortgage markets. International Journal of Housing Policy, 16(1), 91-110.
3. Frederick, T. J., Chwalek, M., Hughes, J., Karabanow, J., & Kidd, S. (2014). How stable is stable? Defining and measuring housing stability. Journal of Community Psychology, 42(8), 964-979.
4. Porter, L., Fields, D., Landau-Ward, A., Rogers, D., Sadowski, J., Maalsen, S., ... & Bates, L. K. (2019). Planning, land and housing in the digital data revolution/the politics of digital transformations of housing/digital innovations, PropTech and housing–the view from Melbourne/digital housing and renters: disrupting the Australian rental bond system and Tenant Advocacy/Prospects for an Intelligent Planning System/What are the Prospects for a Politically Intelligent Planning System?. Planning Theory & Practice, 20(4), 575-603.
5. White, T., Rogers, D., & Maalsen, S. (2024). Housing disruptions: six conceptual entry points for analysing the digital transformation of housing and home. Digital Geography and Society, 100109.
6. Gong, C. M., Lizieri, C., & Bao, H. X. (2019). "Smarter information, smarter consumers"? Insights into the housing market. Journal of Business Research, 97, 51-64.
7. Li, H., Wei, Y. D., & Wu, Y. (2019). Analyzing the private rental housing market in Shanghai with open data. Land Use Policy, 85, 271-284.
8. Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. Information & Communications Technology Law, 28(1), 65-98.
9. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. PloS one, 11(10), e0163477.
10. Belotti, M., Božić, N., Pujolle, G., & Secci, S. (2019). A vademecum on blockchain technologies: When, which, and how. IEEE Communications Surveys & Tutorials, 21(4), 3796-3838.
11. Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. Future Internet, 14(11), 341.
12. Levis, D., Fontana, F., & Ughetto, E. (2021). A look into the future of blockchain technology. Plos one, 16(11), e0258995.
13. Krichen, M., Ammi, M., Mihoub, A., & Almutiq, M. (2022). Blockchain for modern applications: A survey. Sensors, 22(14), 5274.
14. Ishmaev, G. (2017). Blockchain technology as an institution of property. Metaphilosophy, 48(5), 666-686.
15. Golosova, J., & Romanovs, A. (2018, October). Overview of the blockchain technology cases. In 2018 59th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS) (pp. 1-6). IEEE.
16. Woodside, J. M., Augustine Jr, F. K., & Giberson, W. (2017). Blockchain technology adoption status and strategies. Journal of International Technology and Information Management, 26(2), 65-93.
17. Schinckus, C. (2020). The good, the bad and the ugly: An overview of the sustainability of blockchain technology. Energy Research & Social Science, 69, 101614.
18. Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy challenges. Internet of Things, 8, 100107.
19. Priyadarshini, I. (2019). Introduction to blockchain technology. Cyber security in parallel and distributed computing: concepts, techniques, applications and case studies, 91-107.

20. Dang, T. L. N., & Nguyen, M. S. (2018, November). An approach to data privacy in smart home using blockchain technology. In 2018 International Conference on Advanced Computing and Applications (ACOMP) (pp. 58-64). IEEE.
21. Ogungbemi, O. S. (2024). Smart contracts management: The interplay of data privacy and Blockchain for secure and efficient real estate transactions. Journal of Engineering Research and Reports, 26(8), 10-9734.
22. Garcia-Teruel, R. M. (2020). Legal challenges and opportunities of blockchain technology in the real estate sector. Journal of Property, Planning and Environmental Law, 12(2), 129-145.
23. Kumar Sanjay & Sharma Deepmala. (2024). A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm. Artificial Intelligence Review,57(4).
24. Yassine Maadallah, Younès El Bouzekri El Idrissi & Youssef Baddi. (2025). Enhancing IoT security through blockchain an in-depth analysis of the proof-of-work consensus mechanism. EDPACS,70(5),1-44.
25. Dirk G Baur & Jonathan R Karlsen. (2024). Do crypto investors care about energy use and climate change? Evidence from Ethereum's transition to proof-of-stake. Journal of environmental management,369,122299.
26. Anqi Li, Yingbiao Yao & Xin Xu. (2024). Dynamic Byzantine Fault-Tolerant Consensus Algorithm with Supervised Feedback Mechanisms. Mathematics,12(17),2643-2643.
27. Chaokai He & Meng Wu. (2015). A New Reputation Model for P2P Network Based on Set Pair Analysis. The Open Cybernetics & Systemics Journal,9(1),1393-1398.