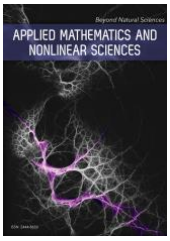
sciendo Applied Mathematics and Nonlinear Sciences, 9(1) (2024) 1-14



Applied Mathematics and Nonlinear Sciences

https://www.sciendo.com

Application of Digital RMB Smart Contracts in Grid Smart Payment Settlement

Dongliang Hou[1,†], Qing Yang[1], Shanshan Hao[2]

1. State Grid Hebei Electric Power Co., Ltd, Shijiazhuang, Hebei, 050000, China.
2. Information & Telecommunication Branch, State Grid Hebei Electric Company, Shijiazhuang, Hebei, 050000, China.

Submission Info

Communicated by Z. Sabir
Received March 26, 2024
Accepted June 16, 2024
Available online August 5, 2024

Abstract

The use of smart contract technology for contract execution and real-time payment can ensure the timely availability of funds, thus ensuring the security and authenticity of data in power grid transactions. In this paper, we design a digital RMB smart contract model based on blockchain technology and use the hexadecimal model to create, deploy, and execute smart contract functions. And through the DTSC algorithm, smart contracts can be applied to the grid smart payment settlement. At the same time, a privacy protection algorithm for transaction data is proposed, and finally, the grid smart payment settlement system is designed based on smart contracts and privacy protection algorithms. Simulation test results show that the cost required for the digital RMB smart contract proposed in this paper is lower than the existing schemes in terms of invocation and deployment costs. The average chain code invocation delay in smart contract technology decreases when the transaction sending rate increases from 250TPS to 300TPS. Moreover, the on-chain operation time of this system is only 2.69 seconds, which meets the demand of practical power grid smart payment settlement applications. This paper sets the foundation for the efficient operation of the grid smart payment and settlement system and provides a guarantee for payment and settlement security.

Keywords: Blockchain technology; DTSC algorithm; Smart contract; Payment settlement; Privacy protection.
AMS 2010 codes: 11A63

†Corresponding author.
Email address: yangqing522873086@163.com

ISSN 2444-8656
https://doi.org/10.2478/amns-2024-2201

1 Introduction

The research and development of China's digital RMB began in 2014, and after years of exploration, digital RMB has realized significant development in terms of back-end technical architecture, specific application scenarios, and ecosystem construction [1-2]. By the end of 2022, the stock of digital RMB in circulation reached 13.61 billion yuan, the pilot of digital RMB has been expanded to 26 regions in 17 provinces (municipalities), the top-level design and ecosystem construction continue to improve, and the effect of deepening the pilot is constantly highlighted [3-5]. From the current view of the actual promotion of the digital RMB pilot process, many places, in addition to creating general scenarios such as daily consumption and closed pilots, are also creating some special scenarios, such as the use of special funds, pre-payment, and other scenarios that have not been properly resolved [6-8]. Digital RMB can effectively empower the solution of the above problems by loading smart contracts that do not affect its monetary function [9-10].

The intelligent development of payment and settlement of digital RMB will bring a new round of leaps and changes in financial work [11-12]. The popularization of digital RMB will make the process of payment and settlement more efficient, convenient, and secure and provide a new opportunity for the development of intelligent payment and settlement systems [13-14]. Smart contract technology, on the other hand, can realize the customization and automation of payment and settlement, thus improving the financial efficiency of enterprises and reducing human errors [15-16]. However, on the other hand, the development of these two technologies will also bring more thoughts and challenges to finance personnel [17-18]. In order to adapt to the application and popularization of e-CNY and smart contracts in the future, accounting standards, enterprises' demand for financial talents' knowledge structure, enterprise capital management models, corresponding risk management measures, and data management systems need to undergo corresponding changes [19-21], which requires financial personnel to continue to learn and adapt to new technologies and changes with a more active and open mind, so as to become a more active and promising group in the digital wave [22-24].

Wang, J. stated that digital RMB is an important financial innovation of China's central bank, which is constructed into a payment system with security and intelligence, and efficient through blockchain technology, smart contracts, and cryptography, which promotes the innovation of financial science and technology and upgrading of payment methods [25]. Zheng, Y. et al. pointed out that embedding smart contracts into the whole process of issuing, circulating, and destroying digital RMBs can provide feasible guarantees for digital RMBs and slowly build up a system of rules that is compatible with the current laws in China [26]. Zheng, Y. et al. mentioned that the issuance of digital RMB is a challenge to China's financial system, and the emergence of digital RMB may lead to a fundamental change in the financial system. In addition, the promotion of digital RMB is a key national strategy for China and continuous efforts are made for its development [27]. Zou, X. specified that compared with crypto digital currency based on blockchain technology, digital currency e-payment has the characteristic of centralized management, and digital currency e-payment will have a profound impact on monetary policy, the operation of banks and other payment institutions, as well as the development of the digital economy, the internationalization of the RMB, and even for the governance of the society [28]. Zhang, T. found that digital currency electronic payments can improve monetary policy and stabilize the financial market to a certain extent, in addition to saving the cost of using cash and thus strengthening the central bank's financial regulatory capacity [29]. Liu, X. et al. show that digital currency electronic payment has the same legal status as the physical RMB, which will help to improve the efficiency of Chinese residents' daily payments, reduce the cost of central bank management, and thus accelerate the development of the digital economy and promote the progress of society and technology [30]. Dziwok, E. stated that new payment methods and new forms of currency are enabling the gradual internationalization of the Chinese renminbi, which increases the

international position of China in the field of payment systems. In addition, new payment methods and forms of currency play an intermediary role in strengthening the role of international transactions outside the traditional banking system [31].

This paper builds a digital RMB smart contract model using blockchain technology and deploys DTSC and CDSC through smart contracts. The DTSC algorithm is utilized to complete the functions of requesting purchase, successful payment and settlement, and resolving disputes in grid smart payment settlement to ensure smooth operation of grid smart payment settlement. Subsequently, this paper proposes a method for protecting payment settlement privacy that uses public and private keys to encrypt transaction data for storage and protection operations. Finally, based on the digital RMB smart contract and privacy protection algorithm, the grid-intelligent payment and settlement system is constructed, and the grid-intelligent payment and settlement is realized through the modules of identity management, data review, and calculation task execution. The function cost and deployment cost required for the smart contract to run on this basis have been tested and analyzed. Analyze the transaction delay and time consumption of the Grid Intelligent Payment and Settlement system in the simulation application and explore its application effects.

2 Method

2.1 Blockchain-based Smart Contract Model for Digital RMB

The Data Trading Smart Contract Model (DTCM) constructed in this paper based on blockchain technology [32] is a hexadecimal group, DTCM= (DS, DP, DTC, DT, CB, f), and the specific structure of the digital RMB smart contract model is shown in Fig. 1. SC denotes the smart contract, EOA represents the public key (i.e., Ether address), EPK stands for the private key, and the participating entities in the model have Ethernet addresses to ensure smooth communication between the entities and the smart contract on the chain.

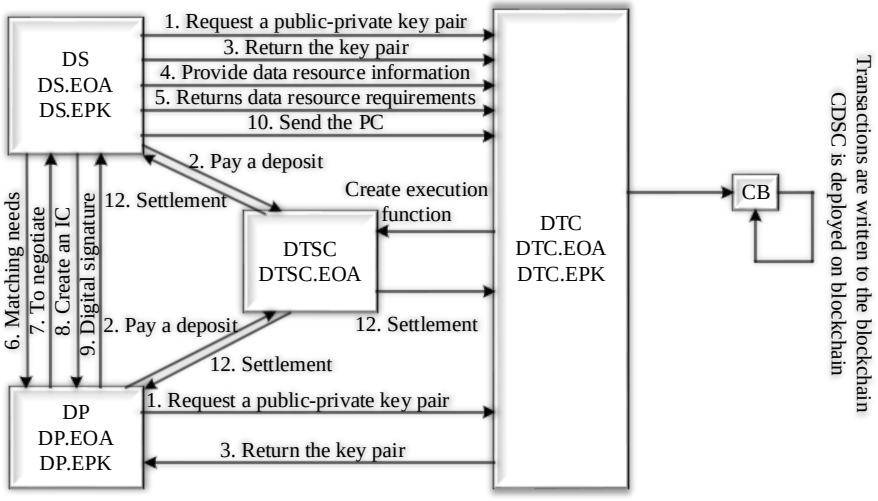


Figure 1. Digital yuan intelligent contract model

Ethernet users [33] are aware of how to create and deploy smart contracts, as well as functions to execute them.DTC has a set of public and private keys, i.e., (DTC. EOA, DTC. EPK), DS has a set of public and private keys, i.e., (DS. EOA, DS. EPK), and DP has a set of public and private keys, i.e., (DP. EOA, DP. EPK). The Parity-Ethereum wallet3-based federated blockchain will be used as a tool for application modeling, and the Digital RMB smart contract will be written using Solidity

language as well as will be debugged in Remix IDE. DTSC and CDSC will be compiled and deployed after the Parity network is configured in Truffle4.

In order to reduce the time spent waiting for blocks during testing and to address the situation where an organization's internal network or external network is unable to synchronize blocks, the PoA Consensus Algorithm-based federated blockchain was created. The characteristics of a PoA-based federated blockchain (PoA Chain) are divided into several points. PoA relies on pre-set Authority nodes to generate blocks. The second is that the number of Authority nodes can be set as required. Thirdly, the block generation time can be specified. For example, the block will be generated 5 seconds after the transaction is received. Lastly, Ether nodes can connect to the PoA Chain and start transactions, contracts, etc., normally. In addition, DTSC and CDSC will be deployed on the PoA Chain.

DS applies to DTC to join the PoA Chain and obtains the public and private keys from DTC.DS pays a deposit to DTSC to be eligible to sell resources.DS provides DTC with information about the data resources to be sold, and DTC sends the demand for the resources, the price of the resources, and the resource number to DS.DS broadcasts the demand for the resources to the whole network and listens to the demand from DP.DP applies to DTC to join the PoA Chain and obtains the public and private key pairs from DTSC to be eligible to purchase the resources. DP selects DS based on its demand and selects DP through DTSC to join the PoA Chain. DTC applies to join the PoA Chain and obtains a public-private key pair from DTC.DP pays a deposit to DTSC to qualify for the purchase. DP selects DS based on its demand and negotiates the transaction details with DS through the PoA Chain. DP, DTC, and DS form a supply path for data resources. After DS and DP reach a consensus through negotiation, the complete transaction authentication data will be written to CDSC.DTC verifies the CDSC and deploys it to the PoA Chain. At the same time, DTC is also the bookkeeping node that verifies this transaction. If the transaction between DP and DS is not disputed, the payment and settlement of the transaction are completed automatically. If the transaction between DP and DS is disputed, i.e., the data resources provided by DS do not meet DP requirements, DTC will arbitrate the dispute. Depending on the outcome of the arbitration, DTC will forfeit the deposit in order to penalize DS or DP. Additionally, the deposit can be refunded if DS and DP wish to withdraw from the transaction prior to its commencement.

The algorithm of DTSC mainly consists of the following steps.

1) Request to purchase data resources

   DP first calls the RequestGetData function in DTSC to pay the deposit for participating in the transaction and selects DS by matching the information of data resources. After DP selects DS, DP, and DS reach a consensus through negotiation and sign the CDSC. After that, DS sends the CDSC to DTC for verification. After DTC validates the CDSC, it will be deployed on the blockchain.

2) Successful transaction and payment settlement

   After DP obtains data resources from DS, DP needs to execute the ConfirmResult function in DTSC so that DTC knows that DP has obtained data resources. The payment settlement of the transaction is automatically carried out by the DTSC only after the DP is satisfied. The deposits of both DS and DP will be refunded once the transaction is successful. In addition, DTC and DS will receive their respective profit shares.

3) Dispute Resolution

If the confirmation result of DP is false, i.e., DP is not satisfied with the acquired data resources, DTC will intervene in the dispute arbitration. If the arbitration result is that DP is correct, then DP will receive a refund, and DS's deposit will be forfeited. If the arbitration result is that DP is incorrect, then DP's margin will be forfeited and DTSC will automatically proceed with the payment settlement of the transaction. Upon successful completion of the transaction, DTSC and DS will receive a share of the corresponding profits.

2.2 Payment settlement privacy protection methods

2.2.1 Data pre-processing

In this paper, we design the Grid Smart Payment Settlement privacy protection method, which first divides the data into two parts and calculates the hash value of each part separately before uploading the data to the smart contract. Then, each part is encrypted using Alice's private key in the blockchain. After completing this operation, the encrypted two parts are uploaded to IPFS.

After uploading these two parts of data to IPFS, two $IA_s(IA_1, IA_2)$ can be obtained, which represent the address information of these two parts of data in the IPFS network. Two *CHs* can be obtained from this address information:

$$\begin{aligned}&[CH1: QmY71M3cwu6zpp3qrXHUR2AmPb8rHdQWBFDM7pKhwHhjcM]\\&[CH2: QmPm1vjumDvMKwu3uEKh6wqypWKqLSyLBLUH3t2SK7irpx]\end{aligned} \tag{1}$$

The two *CHs* represent two file paths in the IPFS network. Based on these two *CHs*, two IA_s can be constructed, viz:

$$\begin{aligned}&[LA1: https://ipfs.io/ipfs/CH1]\\&[LA2: https://ipfs.io/ipfs/CH2]\end{aligned} \tag{2}$$

Everyone has access to a number of files based on these two IA_s. In this chapter, Alice needs to encrypt the *CH* of *the* IA as *EIA* using the public key of the recipient when obtaining the *IA* of the data in order to secure the private key of the *IA* during the checking step. The *EIA* is constructed as follows:

$$\begin{aligned}&[EIA1: https://ipfs.io/ipfs/E_{PB}(CH1)]\\&[EIA2: https://ipfs.io/ipfs/E_{PB}(CH2)]\end{aligned} \tag{3}$$

When Alice gets the data *EIA*, Alice uses two different keys generated in the symmetric algorithm, K_1 and K_2. Alice then uses K_1 and K_2 to encrypt the *EIA* of both data to $E_{K_1}(ELA_1)$ and $E_{K2}(ELA_2)$, respectively. Finally, Alice performs the following hash operation to obtain the hash value $h_1 = Hash(E_{K_1}(EIA_1) \| E_{K_2}(EIA_2))$ of $E_{K_1}(EIA_1) \| E_{K_2}(EIA_2)$. The bitstream is then encrypted using Bob's public key in the blockchain with the above hash result in the form of $(E_{K_1}(EIA_1) \| E_{K_2}(EIA_2 \| Hash(E_{K_1}(EIA_1 \| E_{K_2}(EIA_2))))$. After Alice obtains encrypted IPFS addresses, Alice sends these addresses to Bob via the blockchain. This paper assumes that Alice must send the correct *IA* to Bob, i.e., that the *IA* is indeed an IPFS address and stores data.

2.2.2 Exchange of I - upper half data

The proposed protocol in this paper is based on the unintentional transmission protocol [34], and therefore, the steps of the unintentional transmission protocol need to be followed. It is specified as follows.

1) Alice generates two public-private key pairs $(P_1, S_1), (P_2, S_2)$.

2) Bob generates a symmetric key K_3.

3) Alice sends the two public keys (P_1, P_2) to Bob.

4) Bob randomly chooses a public key of Alice (assumed to be P_1) and encrypts K_3 using P_1, i.e., its ciphertext result is $E_{P_1}(K_3)$.

5) Bob sends the ciphertext result $E_{P_1}(K_3)$ to Alice.

6) Alice decrypts $E_{P_1}(K_3)$ using her private key to obtain the following two keys as follows:

$$K_3 = D_{R_1}(E_{R_1}(K_3)), K_{wrong} = D_{R_2}(E_{R_1}(K_3))。 \tag{4}$$

One of the results is Bob's symmetric key K_3, and the other result is garbled K_{wrong}.

Alice uses the above two key results to encrypt Alice's two symmetric keys (K_1, K_2). i.e., the following ciphertext formula results are obtained:

$$EK_3(K_1) = E_{K_3}(K_1), EK_{wrong}(K_2) = E_{K_{wrong}}(K_2) \tag{5}$$

The result after Bob decrypts $EK_3(K_1)$ and EK_{wrong} using K_3 is shown below and obtains the correct Alice's symmetric key K_1. At this point, Bob obtains an exact *EIA*, and after decrypting *CH* with Bob's private key, he can obtain an exact *IA* and get the first part of the data. The formula is as follows:

$$K_1 = D_{K_3}(EK_3(K_1)), K_{wrong} = D_{K_3}(EK_{wrong}(K_2)) \tag{6}$$

By performing the above process, Bob can obtain half of the target data. After Alice obtains the value of half of the data from Bob, she can choose to terminate or continue the agreement depending on Bob's satisfaction with the data.

2.2.3 Exchange II - lower part of data

If Bob gets half of the target data and chooses to continue the protocol, they (Alice and Bob) can perform the following steps.

1) Alice combines the public key as $(S_1 // S_2)$ and encrypts it as $C = E_{P_{Bob}}(S_1 // S_2)$ using Bob's public key and sends it to Bob.

2) Bob decrypts $C = E_{P_{Bob}}(S_1 // S_2)$ using the private key in the blockchain and obtains S_1 and S_2 with the following decryption formula:

$$S_1 \square S_2 = D_{S_{Bab}}(C) = D_{S_{Bab}}(E_{P_{Bab}}(S_1 // S_2)) \tag{7}$$

3) Bob decrypts data $E_{P_1}(K_3)$ using S_1, S_2, and Bob gets K_3 and K_{wrong}, the two formulas are as follows:

$$K_1 = D_{K_3}(EK_3(K_1)), K_2 = D_{K_{wrong}}(EK_{wrong}(K_2))。 \tag{8}$$

4) Bob receives the next EIA and the other half of the parsed target data. By performing the above process, Bob can obtain the other half of the data and then terminate the protocol. In this process, all information exchanged between Alice and Bob is encrypted using the public key of the receiver in the blockchain to better protect the privacy of information in the grid smart payment settlement. Therefore, even though the scheme is based on the public chain, other nodes in the chain cannot directly obtain the information content from the interaction information between the two parties of the transaction.

2.3 Smart contract-based grid smart payment and settlement system design

The overall architecture of the system for designing smart payment settlement for the grid based on the smart contract model sub-design constructed above is shown in Figure 2. The data review module is primarily responsible for reviewing the data, and the incentive mechanism and mixed sampling strategy are essential in the review process. The identity management module is responsible for some operations at the user layer, in which different identities are managed in terms of permissions. In addition to realizing role-based permission management, the identity management module is also divided into identity registration and identity change, which require the use of the underlying blockchain platform and the relevant functions of the privacy computing network. The computational task execution module is responsible for the entire cycle from the execution to the end of the computational task, which requires the use of the blockchain platform and privacy computing network to collaborate to complete the work of the relevant computational tasks. The incentive mechanism is throughout the entire grid smart transaction, including the incentive mechanism based on the size of the data volume during the data review process and the incentive strategy after the computation task has been executed. The payment and order module is mainly responsible for processing payments after data transactions are completed, including processing completed and pending orders. The underlying blockchain platform is mainly responsible for the deployment and operation of some core functional chain codes to support the upper layer modules, including the use of smart contract technology and CA authentication technology; the privacy computing network is mainly responsible for the implementation of the core computing function logic in the process of computing tasks and the authorization management of data calculation results with the blockchain platform, including the use of multi-party security calculation in privacy computing to This includes the use of multi-party secure computing in privacy computing to serve as a technical solution for privacy computing on the platform. The underlying calling algorithms are the algorithms called for the completion of the security calculation, such as the secret sharing algorithm, etc., and the storage is the information storage of some core structures on the chain code and the intermediate and final storage in the process of data flow.

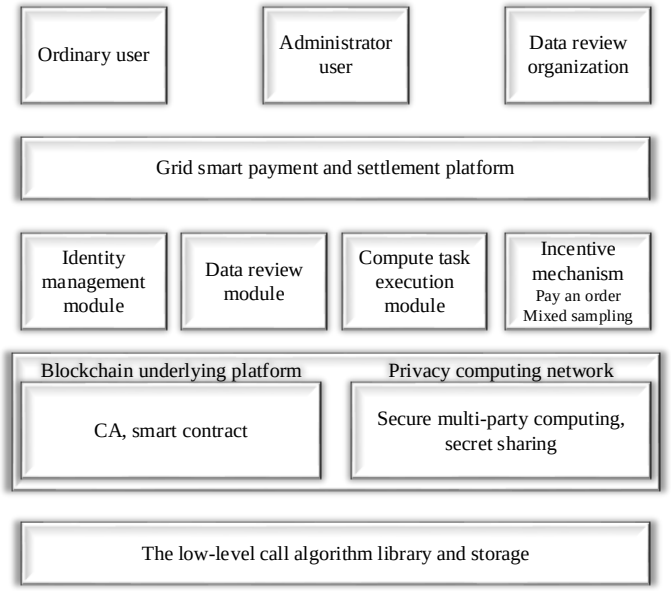


Figure 2. Overall system architecture

3 Results and discussion

3.1 Smart Contract Calling Cost Analysis

3.1.1 Function cost analysis results

In this paper, we first explore the invocation cost of the proposed digital RMB smart contract in the application by deploying the designed smart contract on the Ropsten test network of Ethernet, utilizing the Remix IDE compilation environment and the MetaMask wallet. This section focuses on analyzing the cost of creating and invoking smart contracts, which will pave the way for their application in grid smart payment settlement. The cost of executing different functions for the digital RMB smart contract is shown in Table 1. At the time of the experimental test, the conversion relationship between Ether and USD was $1\text{eth} \approx 1528.24\text{USD}$, and that between Ether and Gas was $1\text{gas} \approx 0.000000001\text{eth}$. The cost of creating and deploying a smart contract in the blockchain is 6.046 USD, which is a high cost compared to other function calls. However, contract creation and deployment is only a one-time cost to initialize the system. The cost of creating and calling smart contracts is minimal compared to purchasing and maintaining a private database.

Table 1. The cost of invocation of different functions in a smart contract

Function	Gas cost	Actual transaction cost	USD
Contract creation	3956241	0.003956	6.046
Add authorized user	95478	9.55E-05	0.146
Remove authorized user	26431	2.64E-05	0.040
Add authorized user role	112546	0.000113	0.172
Remove the authorized user role	25413	2.54E-05	0.039
Add role permission	211547	0.000212	0.323
Remove role permission	35264	3.53E-05	0.054
User role remapping	118542	0.000119	0.181
Is access	27854	2.79E-05	0.043

In this paper, the cost of a smart contract designed based on blockchain technology is compared and analyzed with the existing smart contract scheme 1 and scheme 2, and the result of the smart contract function cost comparison is shown in Figure 3. There are 8 main functions involved in this scheme, so the cost spent in the contract creation and deployment phase is compared to the other two schemes because the other two schemes do not contain add UserRole, remove UserRole, add Permission, remove Permission, re Mapping and is Access These six functions, so the cost of creating and deploying the digital RMB smart contract designed in this paper is more expensive. For the add User function, the invocation cost in Scenario 1 and Scenario 2 is 0.256USD and 0.112USD respectively, and the invocation cost of the smart contract designed in this paper is 0.146USD, which is higher than that of Scenario 2 but lower than that of Scenario 1. For the remove User function, the invocation cost of Scenario 1 and Scenario 2 is 0.182USD and 0.075USD, respectively, and the invocation cost of the digital RMB smart contract designed in this paper is 0.182USD and 0.075USD, respectively. USD, and the invocation cost in this paper's digital RMB smart contract is 0.04 USD. Compared with the other two schemes, the remove User function of this paper's smart contract spends the least amount of money, so the designed digital RMB smart contract is feasible in terms of the cost of these two types of function invocations.

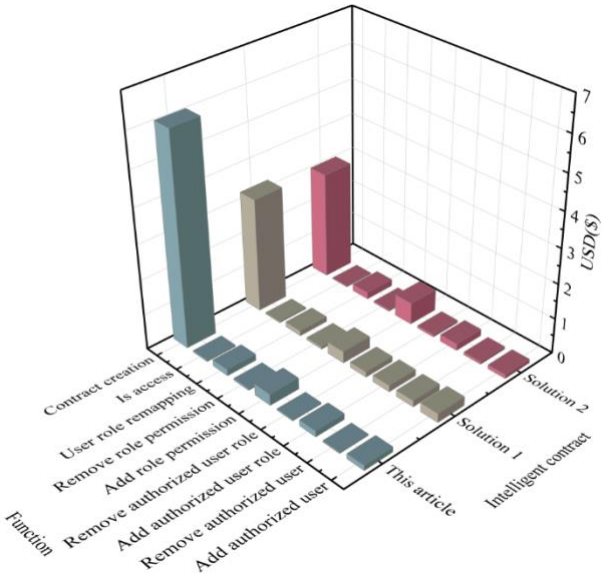


Figure 3. Cost analysis of intelligent contract function

3.1.2 Comparative analysis of deployment costs

This paper compares existing smart contract schemes 3 and 4 for cost because the smart contract designed in this paper will involve user role update operations in grid smart payment settlement. The results of the deployment cost comparison analysis are shown in Table 2. The cost of scheme 4, 0.0099eth, does not increase with the increase of the number of roles and the number of role updates, while the smart contract and scheme 3 in this paper increase with the increase of the number of roles and the number of role updates. When there are 5 roles in the smart contract and 15 updates, the cost of this paper's smart contract and scheme 3 is 0.0087eth and 0.0092eth, respectively, and the cost of this paper's smart contract is lower. When there are 15 roles in the smart contract and the roles are updated 15 times, the cost of the smart contract in this paper is 0.048eth, and the cost of Scheme 3 is 0.094eth. After that, as the number of roles and the number of times of updating increase, the increase in Scheme 3 is greater, so when the number of roles and the number of times of updating exist in the smart contract are equal to or higher than 15 times, the cost of the smart contract in this paper is more practical and feasible than the existing smart contract Scheme 4 is more practical and feasible. If the

number of roles and the number of updates present in the scheme are less than 15, the cost of the smart contract herein is more practical and feasible than the existing smart contract scheme 3.

Table 2. Deployment cost comparison analysis

Character number	Number of updates					
	5			15		
0	This article	Solution 3	Solution 4	This article	Solution 3	Solution 4
5	0.0024	0.0074	0.099	0.0087	0.0092	0.099
10	0.0052	0.032	0.099	0.024	0.052	0.099
15	0.0068	0.072	0.099	0.048	0.094	0.099
20	0.024	0.101	0.099	0.078	0.142	0.099
25	0.036	0.152	0.099	0.104	0.184	0.099
30	0.058	0.172	0.099	0.152	0.201	0.099
35	0.072	0.192	0.099	0.197	0.325	0.099
40	0.081	0.203	0.099	0.228	0.397	0.099
45	0.086	0.241	0.099	0.265	0.425	0.099

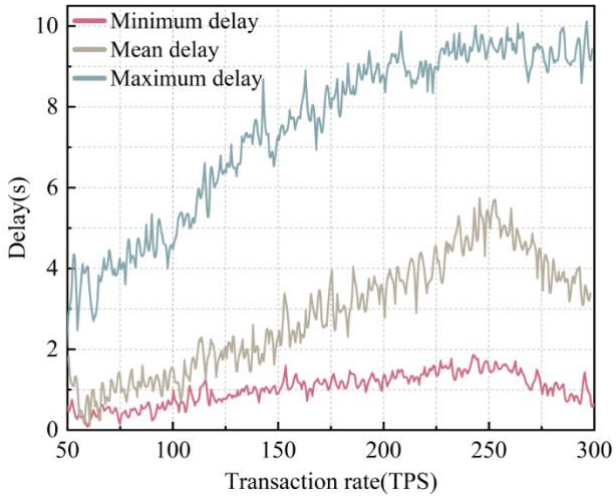
3.2 Application Analysis of Grid Intelligent Payment and Settlement System

The cost of the digital RMB smart contract was analyzed above, and in order to explore the performance of the grid smart payment and settlement system based on this smart contract, this section tests the performance of the model by deploying the grid smart payment and settlement system based on the digital RMB smart contract on Hyperledger Fabric. Specifically, the smart contract model and Hyperledger Fabric are deployed on a laptop computer configured with 16.04 Ubuntu, 2GB RAM, and a 1GHz processor. Hyperledger Fabric is used as the performance testing tool. A series of tests were done for the performance of the grid smart payment settlement system. Theoretically, in a realistic grid smart payment settlement environment, the throughput of Hyperledger is 2000 TPS (TPS refers to the number of transactions processed per second). Due to the test environment, the test system's throughput can only reach 100 TPS. Once the system is deployed in the grid smart payment settlement environment, the efficiency of the system will far exceed the test data, and all transactions will be recorded quickly in the smart contract.

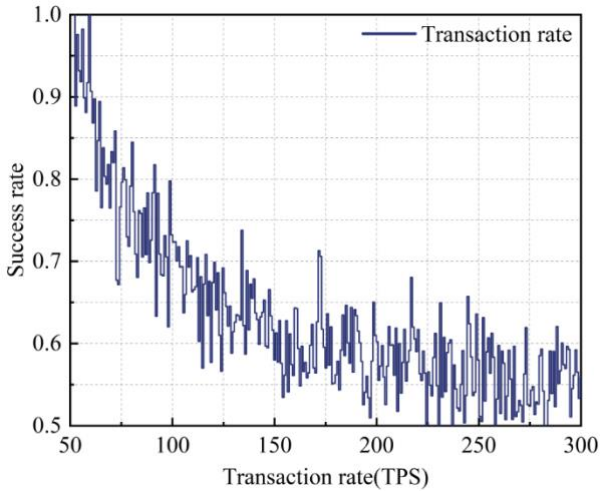
3.2.1 Transaction Latency and Success Rate Simulation Analysis

The Grid Smart Payment Settlement System's network performance is measured by chain code call latency, transaction upload success rate, request latency, and send rate in this paper. Specifically, chain code invocation delay refers to the delay in recording a transaction in the grid smart payment settlement system. The probability of a transaction being successfully recorded in the grid smart payment settlement system is known as the transaction success rate. Request delay is the time it takes for a node to access the grid smart payment settlement system. The send rate is the number of transactions sent by a node to the grid smart payment settlement system per second. In the test, the sending rate is changed from 50 to 300 TPS to observe the changes in other indicators, and then the performance of the system is analyzed based on the test results. The network performance test results of the digital RMB smart contract based on blockchain technology are shown in Fig. 4, (a)-(c) represent the chain code invocation delay, the success rate of transaction uploading, and the change of access delay with the transaction sending rate, respectively. From the overall trend, the delay in calling the chain code in smart contract technology generally increases with the rate of transaction

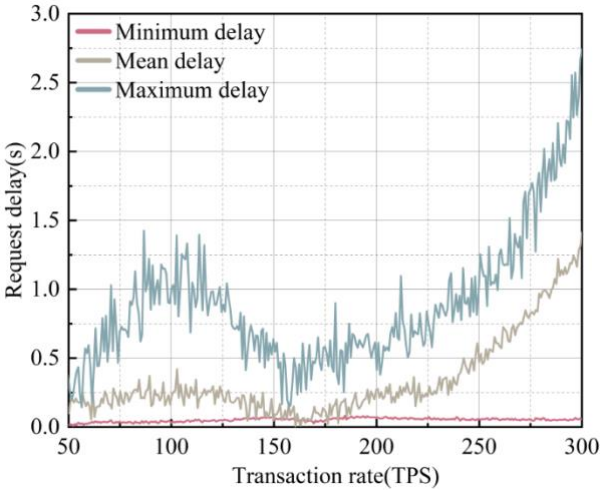
sending. When the transaction sending rate increases from 250TPS to 300TPS, the average chain code invocation latency in smart contract technology shows a decreasing trend. From the results in Fig. 4(b), the average transaction on-chain success rate of the digital RMB smart contract-based grid payment and settlement system generally decreases with the growth of the transaction sending rate. A small increase in the success rate of transaction on-chaining occurs when the transaction sending rate reaches 300 TPS. The small increase in this part is a test error, which occurs after several measurements for unknown reasons. From the analysis results of access delay with transaction sending rate, the average access delay of grid payment and settlement system increases with the increase of transaction sending rate, and the average access delay time reaches the maximum at 300TPS, which is 1.42s. The minimum access delay is always between 0-0.1s in 50-300TPS.



(a) Chaincode invoke latency



(b) Success rate



(c) Query latency

Figure 4. Network performance test results

3.2.2 Time consumption analysis

To analyze the time consumption of each step of the grid smart payment settlement system based on digital RMB smart contracts in real applications. The grid smart payment settlement system designed in this paper is deployed in a test environment, and the maximum order of homomorphic

multiplication that the server can handle is set to 10, and the throughput of the system is set to 100 TPS. Therefore, the grid smart payment settlement system based on the digital RMB smart contract designed in this paper can be deployed on lightweight clients, such as cell phones. The smart contract-based grid smart payment settlement contains seven steps, and in the test, the average running time of each step is shown in Fig. 5. Among them, Step 2 and Step 6 are the longest time-consuming ones, which are 3.20 seconds and 2.03 seconds, respectively. These two steps can be carried out in the preparation and validation phases prior to the grid-smart payment settlement operation, so these two steps have no impact on getting the payment settlement result quickly. Step 4 is the request phase, and steps 5 and 6 are the feedback phase. Step 7 is the recovery phase. It takes only 2.69 seconds from sending the request to finally recovering the result. Therefore, the theoretical on-chain operation time of this system is only 2.69 seconds. For grid smart payment settlement, this speed does not bring any extra delay, so this test result theoretically meets the demand of grid smart payment settlement practical application.

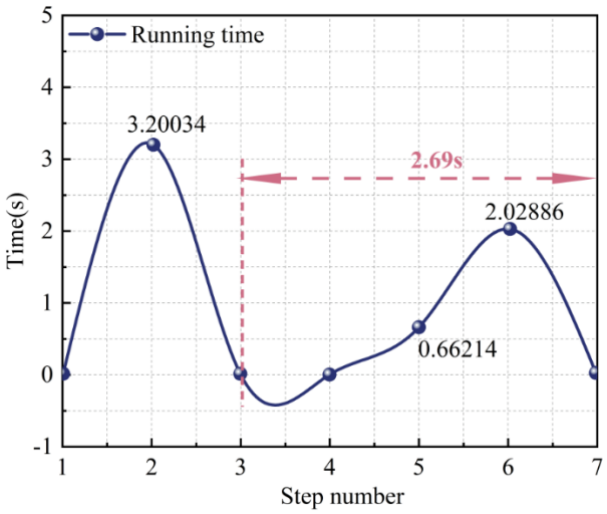


Figure 5. Delay in the step of the grid intelligent payment settlement system

4 Conclusion

This paper designs a digital RMB smart contract based on blockchain technology and combines smart contracts with privacy protection methods to construct a smart payment and settlement system for the power grid. The cost of smart contracts is verified, and the results show that for the remove User function, the invocation cost is 0.182USD and 0.075USD in Scheme 1 and Scheme 2, respectively, and the invocation cost in the digital RMB smart contract in this paper is 0.04USD, which is the least cost of the remove User function of this paper's smart contract compared with the other two schemes. The smart contract proposed in this paper has the lowest deployment cost among the existing schemes. The simulation analysis of the smart payment computing system for the grid reveals that the average chain code invocation latency in the smart contract technique shows a decreasing trend when the transaction sending rate is increased from 250TPS to 300TPS. The minimum access delay of the system is always between 0-0.1s in 50-300TPS. In addition, the theoretical on-chain operation time of this system is only 2.69 s, which meets the demand of the practical application of grid smart payment settlement. The results show that the application of the proposed smart contract in grid smart payment and settlement can reduce delays and improve payment efficiency in the payment and settlement system.

Funding:

This research was supported by the subject State Grid Co., Ltd. science and technology project funding：Research project on smart contract technology for digital RMB in smart payment settlement system and data security encryption in power grid (B604DY230041).

References

[1] Bhattacharya, D. (2022). Digital Yuan (e-CNY): China's official digital currency. Strategic Analysis, 46(1), 93-99.

[2] Knoerich, J. (2021). China's new digital currency: Implications for renminbi internationalization and the US dollar. The (Near) Future of Central Bank Digital Currencies, 145-166.

[3] Michelsen, B. (2021). China's Moonshot: How the Introduction of the Digital Renminbi Furthers China's Societal Grip and Threatens the Future of Digital Currencies. U. St. Thomas JL & Pub. Pol'y, 15, 813.

[4] Alwago, W. O. (2022). Is the Renminbi a Global Currency in the Making? Globalization of Digital yuan. PÉNZÜGYI SZEMLE/PUBLIC FINANCE QUARTERLY, 67(4), 553-566.

[5] Zhang, F., Cui, Y., & Campbell-Verduyn, M. (2023). Digital RMB vs. Dollar hegemony? Friendly foes in China-US currency competition. Journal of Chinese Political Science, 1-26.

[6] Aysan, A. F., & Kayani, F. N. (2022). China's transition to a digital currency does it threaten dollarization?. Asia and the Global Economy, 2(1), 100023.

[7] Louie, B. L., & Wang, M. (2021). China's forthcoming digital currency: implications for foreign companies and financial institutions in China. Journal of Investment Compliance, 22(2), 195-200.

[8] Yang, P., Fan, M., Li, Z., Cao, J., Wu, X., Wu, D., & Lu, Z. (2022). Digital finance, spatial spillover and regional innovation efficiency: new insights from China. Electron Res Arch, 30(12), 4635-4656.

[9] Wang, X., & Wang, X. (2022). Digital financial inclusion and household risk sharing: evidence from China's digital finance revolution. China Economic Quarterly International, 2(4), 334-348.

[10] Kshetri, N. (2023). China's digital yuan: Motivations of the Chinese government and potential global effects. Journal of Contemporary China, 32(139), 87-105.

[11] Slawotsky, J. (2022). Digital currencies and great power rivalry: China as a disseminator in the digital age. Asia Pacific Law Review, 30(2), 242-264.

[12] Deng, H. (2024). Negotiating currency internationalization: An infrastructural analysis of the digital RMB. Finance and Society, 10(1), 1-17.

[13] Shen, C. (2022). Digital RMB, RMB Internationalization and Sustainable Development of the International Monetary System. Sustainability, 14(10), 6228.

[14] Hasenstab, M., Officer, C. I., & Macro, T. G. (2021). China's Digital Currency Is A Threat To Dollar Dominance. Financial Times, 14.

[15] Mohanta, B. K., Panda, S. S., & Jena, D. (2018, July). An overview of smart contract and use cases in blockchain technology. In 2018 9th international conference on computing, communication and networking technologies (ICCCNT) (pp. 1-4). IEEE.

[16] Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R., & Wang, F. Y. (2018, June). An overview of smart contract: architecture, applications, and future trends. In 2018 IEEE Intelligent Vehicles Symposium (IV) (pp. 108-113). IEEE.

[17] Sayeed, S., Marco-Gisbert, H., & Caira, T. (2020). Smart contract: Attacks and protections. Ieee Access, 8, 24416-24427.

[18] Giancaspro, M. (2017). Is a 'smart contract'really a smart idea? Insights from a legal perspective. Computer law & security review, 33(6), 825-835.

[19] Allam, Z. (2018). On smart contracts and organisational performance: A review of smart contracts through the blockchain technology. Review of Economic and Business Studies (REBS), (22), 137-156.

[20] Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and smart contracts for insurance: Is the technology mature enough?. Future internet, 10(2), 20.

[21] Caudevilla, O., & Kim, H. M. (2022). The Digital Yuan and Cross-Border Payments: China's Rollout of Its Central Bank Digital Currency. University of Hong Kong Faculty of Law Research Paper, (2023/30).

[22] Taskinsoy, J. (2021). Say good bye to physical cash and welcome to central bank digital currency. Available at SSRN 3972858.

[23] Zhou, J., Huang, S. H., & Yan, S. (2024). Design and Research of Off-line Transaction Protocols in Remote Areas Under Smart Contracts. International Journal of Network Security, 26(2), 180-189.

[24] Liang, Y., & Ma, S. (2023). Analysis of Willingness Factors of Digital RMB Acceptance Based on PEST Perspective and TAM-SEM Model. Frontiers in Business, Economics and Management, 12(2), 115-123.

[25] Wang, J. (2024). Digital RMB Promoting Financial Digital Transformation in the Banking Sector. Financial Engineering and Risk Management, 7(1), 79-85.

[26] Zheng, Y., Hu, J., Ying, Z., & Wang, T. (2023). The Construction of digital RMB guarantee rule system realized by smart contract. Financial Engineering and Risk Management, 6(11), 39-44.

[27] Mue, I. (2024, February). An Analysis on Strategic Objectives of the Issuance of the Digital Renminbi. In 2024 2nd International Conference on Cyber Resilience (ICCR) (pp. 1-4). IEEE.

[28] Zou, X. (2021). China's national digital currency: An overview of digital currency electronic payment. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(11), 4279-4285.

[29] Zhang, T. (2021, December). Impacts of Digital Currency Electronic Payment (DCEP) on China's Banking System. In 2021 3rd International Conference on Economic Management and Cultural Industry (ICEMCI 2021) (pp. 3242-3246). Atlantis Press.

[30] Liu, X., Lu, F., Shan, W., & Zhang, J. (2021, December). The Progress of Digital Currency Electronic Payment. In 2021 3rd International Conference on Economic Management and Cultural Industry (ICEMCI 2021) (pp. 1489-1495). Atlantis Press.

[31] Dziwok, E. (2021). Digital Currencies and Payment Systems: Chinese Way into Internationalisation of the Renminbi. The Palgrave Handbook of FinTech and Blockchain, 431-444.

[32] Ju Huizhu,Zeng Qingcheng,Chu Xiang & Li Yimeng.(2024).Cooperative investment strategies of ports and shipping companies in blockchain technology.Operational Research(2).

[33] Tianhao Wang, Ke Chen, Zhaohua Zheng, Jiahao Guo, Xiying Zhao & Shenhui Zhang. (2024). PrivShieldROS: An Extended Robot Operating System Integrating Ethereum and Interplanetary File System for Enhanced Sensor Data Privacy.Sensors(10).

[34] Yang Penglin, Geng Huizheng, Su Li, Lu Li & Yang Tingting.(2022).BSOT: Bandwidth-saving oblivious transfer protocol with confidential computing.Journal of Physics: Conference Series(1).

About the Authors

Dongliang Hou, State Grid Hebei Electric Power Co., Ltd, bachelor of management, senior accountant.

Qing Yang, State Grid Hebei Electric Power Co., Ltd, master, senior accountant.

Shanshan Hao, Information & Telecommunication Branch, State Grid Hebei Electric Company, master, intermediate engineer.