# Smart Contract Credit Mortgage Transaction Systemarchitecture Design

Xirong Gao, Ping Wen

School of Economics and Management, Chongqing University of Posts and Telecommunications，Chongqing 400065, China.

## Abstract

**In this paper, the structure of smart contract credit mortgage transaction system is built based on three aspects: participants, accounting channels and functional modules, and the transaction rules are formulated.The credit mortgage transaction alliance of the participants is responsible for the key nodes in the chain and exercises the supervision authority. The participants conduct transactions on the chain, and the trust data source provides external data as the basis for the results of running the smart contract.The accounting channel records all data in the chain, and each functional module provides technical support for credit mortgage.**

## Keywords

**Credit mortgage, Smart contract, System architecture.**

## 1. Introduction

At present, blockchain system can be divided into public chain, alliance chain and private chain according to different application scenarios and design systems.The alliance chain is composed of several people and institutions. Compared with the other two forms of blockchain, it does not need to consume too much computing resources, and the transaction processing speed is relatively fast, and it is multi centralized, and the data is secure and cannot be tampered with.Hyperledger is an open-source project launched by Linux foundation in 2015 to promote blockchain digital technology and transaction verification. Fabric is a subproject of this project, and its main research direction is the infrastructure of enterprise alliance chain.Fabric can develop corresponding blockchain solutions for problems in various industries and support the deployment and execution of smart contracts. Currently, it is the most widely used blockchain form adopted by large enterprises.In view of this, this paper designs a smart contract credit mortgage transaction system based on fabric.

## 2. Research Status

Smart contract was first proposed by Nick Szabo (1995), which was defined as "a smart contract is a set of commitments defined in digital form, including the agreements on which the contract participants can implement these commitments".bencong (2008) proposed blockchain, which is a kind of decentralized shared general ledger that combines data blocks into a specific data structure in a chain way according to the time sequence, and ensures that it can not be tampered with or forged by cryptography.Swan M (2015) divides the blockchain into three stages: blockchain 1.0, blockchain 2.0 and blockchain 3.0.Among them, blockchain 2.0 is programmable finance, and smart contract is its representative application.Buterin (2013) proposed the Ethereum blockchain platform, which not only can realize the digital currency transaction based on the built-in Ethereum, but also provides Turing complete programming language to write the smart contract.In 2015, the Linux foundation launched the open source project hyperledger to promote blockchain digital technology and transaction verification. Androulaki (2018) is a system designed for the deployment of commercial application license blockchain, which has good flexibility and versatility, supports a wide range of uncertain smart contracts (chain codes) and pluggable services, and pluggable components make fabric flexible and scalableSex.William mougayar (2016) blockchain smart contract is a valuable property in the real world controlled by digital means. See Christopher (2016) smart contract template aims to support the management of the whole life cycle of smart legal contracts. Even if there is a

dispute, they are also conducive to the automatic execution of contracts and provide direct contact with relevant legal record documents.Ni Yunwei, Chai Zhenguo, et al. (2019) think that the essence of smart contract is to use technical means to add the guarantee function of auxiliary performance on the contract or offer. The function is to seek to make up for the shortcomings of traditional contract law, increase the safety and efficiency of transactions and eliminate the necessity of legal enforcement.

Hu Shouyong (2013) according to statistics of the Supreme People's court, more than 70% of the cases executed by the national courts from 2008 to 2012 have property, and less than 30% of the cases executed by the courts have evaded, evaded or even violently resisted execution.Shen Jing et al. (2016) believed that in judicial practice, there are a large number of execution cases that have the ability to perform judgments but refuse to perform, evade execution and evade execution. With the diversification and concealment of evasion methods, such cases have been increasing year by year.Tan qiugui (2009) believes that the multiplicity of causes and the complexity of causality determine that the difficulty of civil execution is not a simple legal problem, but a complex social problem.

## 3. The structure and rules of intelligent contract credit mortgage transaction system

### 3.1 The structure of intelligent contract credit mortgage transaction system

Based on the characteristics of fabric alliance chain and the functions required by credit mortgage exchange, the structure of smart contract credit mortgage trading system is established, as shown in Figure 2.1:

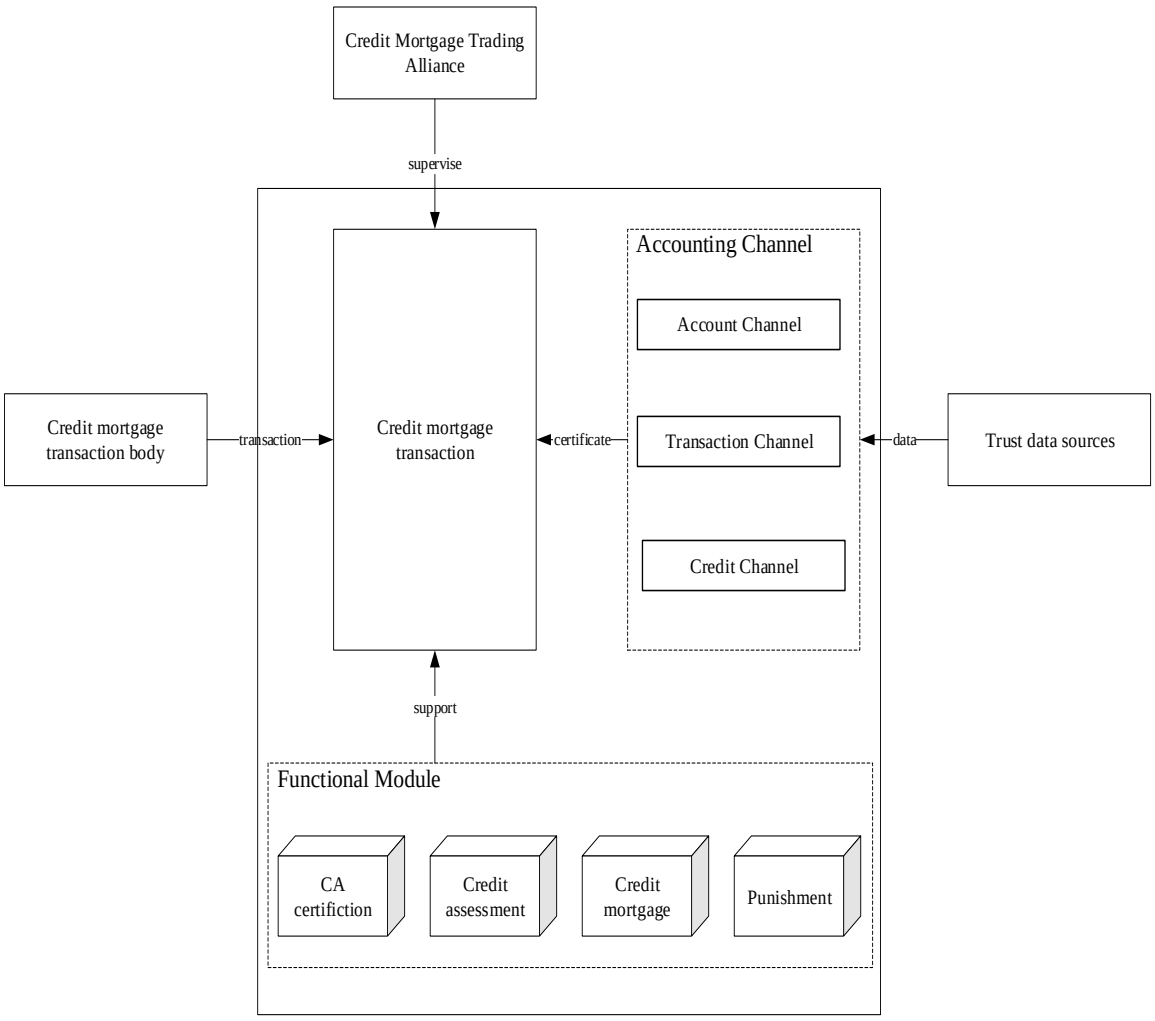


Figure2.1 The structure of intelligent contract credit mortgage transaction system

It can be seen from figure 2.1 that the participants in the smart contract credit mortgage transaction in this paper are respectively the alliance composed of the government, enterprises, associations, etc., the transaction subjects composed of enterprises, individuals, etc., and the trust data sources composed of the government, banks, institutions, etc.Among them, the alliance is responsible for the supervision of all transactions, as well as the handling of abnormal transactions, to ensure the rationality and legitimacy of all transactions; the transaction subject mainly uses the smart contract for transactions in the chain; the trust data source provides the data basis for the transaction and credit evaluation, to ensure the smooth implementation of the contract.

The core infrastructure consists of three parts: account chain, transaction chain and credit chain.The account chain is used to store the basic information of the transaction account; the transaction chain is used to store the transaction records on the blockchain; and the credit chain is used to store the credit situation of the transaction subject.Each chain in the alliance chain is separated from each other, but there are corresponding links. Through the query of the chain, we can know the basic information, credit situation and historical transaction situation of each transaction subject, making all kinds of information transparent and searchable.

The supporting infrastructure consists of three parts: CA authentication module, credit evaluation module and credit mortgage module.CA authentication module is used to check whether the identity is legal and valid. Only after CA authentication can the account have the qualification to trade on the blockchain, and the account information can be stored in the account chain. The credit evaluation module evaluates the credit of the transaction subject based on the financial situation, the credit under the chain and the transaction data on the transaction chain, and the data after evaluation will be stored in the credit chain. The credit mortgage module evaluates the credit based on the creditThe data in the chain and transaction chain evaluate the credit value of the transaction subject, which can be used to offset the collateral assets to be written when signing the smart contract transaction.

### 3.2 Smart contract credit mortgage transaction rules

#### 3.2.1 Application of smart contract credit mortgage transaction

This paper divides the smart contract transaction into two situations according to the writing of transactions when creating a contract.

When an agreement is reached to write the content of the contract into the smart contract, if both the transaction object and the transaction capital can be converted into digital form, the transaction entity will write the contract into the contract when creating the contract, and the contract can be executed automatically according to the transaction conditions when the contract expires, without the transaction entity writing other assets or goods.In this case, because the transaction subject has written the transaction object into the contract and fulfilled the contractual obligations in advance, it is not necessary to write it into the mortgaged assets when signing the contract.When creating a smart contract, one or more parties in the transaction cannot write the transaction objects into the smart contract. If the transaction funds or transaction objects are no longer written in the future, the transaction cannot be successfully completed when the contract expires, the party needs to write the mortgage assets when preparing the smart contract to provide guarantee for the subsequent execution of the contract.The smart contract credit mortgage transaction described in this paper is applicable to the second transaction.

#### 3.2.2 Counting rules of times of smart contract credit mortgage transactions and flow direction of mortgage assets

Although credit value is introduced into the transaction described in this paper to offset the mortgaged assets, due to the credit value needs to be accumulated in the transaction, and the value is limited and can not be infinitely deducted, in the early stage of the transaction or when the transaction subject with poor credit conducts the smart contract transaction, it is still necessary to write a certain amount of mortgaged assets to ensure that the contractual obligations can be fulfilled on time.

See Table 2.1 for the flow of mortgaged assets in credit mortgage transactions based on smart contracts:

Table2.1 Counting rules of transaction times and flow direction of mortgaged assets

| Contract execution type | Transaction subject | Default times | Times of keeping promise | Total transactions | Flow of mortgaged assets |
|---|---|---|---|---|---|
| Both parties fail to implement the negotiation | Trading parties | +0 | +0 | +0 | Return the original account according to the contract |
| One party fails to execute the contract | Defaulting party | +1 | +0 | +1 | Return the original account after compensation; If the party fails to actively compensate for the loss, it will automatically auction according to law to compensate the party in breach of contract for the loss |
| | Defaulted party | +0 | +1 | +1 | Return the original account according to the contract |
| Contract executed successfully | Trading parties | +0 | +1 | +1 | Return the original account according to the contract |

(1) Both parties fail to implement the negotiation

The contract is written into the computer to the contract execution period, there is a certain time, and the market has various unstable factors.Before the contract execution period comes, if one or more parties want to terminate the execution of the contract, they need to negotiate with the common signing body of the contract. If they reach an agreement finally, all parties agree to stop the execution of the contract, and can supplement and update the smart contract, so as to terminate the contract.In this case, because the contract is terminated after negotiation, there is no defaulting party and the defaulted party, so this transaction is not included in the total number of transactions of the transaction subject, and the mortgaged assets will be returned to the original account according to the provisions of the contract.

(2). One party fails to execute the contract

After the contract execution period, if one party fails to perform its obligations in accordance with the contract, resulting in the failure of this transaction, it is the defaulting party; if it performs its obligations in accordance with the contract, but suffers losses due to the actions of the defaulting party, it is the defaulted party.In this case, the defaulting party of this transaction is recorded as the default transaction, and the defaulting party is recorded as the non-compliance transaction.The defaulting party shall take the initiative to compensate the losses of the defaulted party, otherwise its mortgaged assets will be auctioned automatically according to law, and the proceeds will be used to compensate the losses caused.The mortgaged assets of the defaulted party will be returned to the original account in accordance with the contract.

(3). Contract executed successfully

After the contract reaches the execution period, the transaction is executed automatically.In this case, the transaction subjects in this transaction are all recorded as complying with the contract, and their mortgaged assets will be automatically returned to the original account according to the contract provisions.

## 4. Components of smart contract credit mortgage transaction system

### 4.1 Participants of smart contract credit mortgage transaction

The participants of smart contract credit mortgage transaction system are credit mortgage transaction alliance, credit transaction entity and trust data source. Different participants have different responsibilities and authorities in the alliance chain.In order to facilitate the management of data on the chain, the permissions of all nodes in the fabric alliance chain, bitcoin, Ethereum and other public chains are the same and different nodes in the chain have different permissions. The corresponding nodes and permissions of each participant in the smart contract credit mortgage transaction described in this paper are shown in Table 3.1:

Table3.1 Corresponding node of participant

| Participants | Node type | Node permissions | Node responsibility |
|---|---|---|---|
| Credit mortgage transaction Alliance | Endorsement node | Endorsement right and bookkeeping right | Check the validity of the smart contract, run the smart contract, and each endorsement node must access all chain data |
| | Sorting node | Sorting right and bookkeeping right | Sort transaction requests and transaction results and package them into blocks |
| Transaction subject of credit mortgage | Accounting node | Accounting right | Partial or all chain data can be recorded optionally |
| Trust data source | | | |

On the basis of multi centralization, it is necessary to ensure the rationality and legitimacy of the contract. Therefore, members of the trading alliance act as endorsement and sorting nodes in the chain, and are responsible for the verification, packaging, bookkeeping and other responsibilities of the smart contract transactions on the chain.The transaction subject and data source are the participants of the alliance chain, which can only be used as the accounting node to realize multi centrization, so that the data on the chain cannot be tampered with.An account can be used as multiple nodes.

#### 4.1.1 Credit mortgage transaction Alliance

Credit mortgage transaction alliance, as the core participant in the transaction, is responsible for the operation of the whole alliance chain and the supervision of the transaction, which is also the most important part.In order to ensure the fairness and fairness of smart contract transactions on the chain, alliance members should come from all walks of life, including but not limited to government agencies, associations, business representatives and personal representatives.

The credit mortgage transaction alliance is organized and established by the relevant government agencies with public trust. The members of the alliance are responsible for the operation of the alliance chain, and the government agencies are responsible for the account authentication and transaction supervision of the alliance chain.All members of the alliance shall be strictly checked and

screened by government agencies, and their information shall be deposited in account books.At present, there are many mature centralized trading platforms in China, such as ali1688 for wholesale business, alitaobao, Jingdong and pinduoduo for retail business. These trading platforms have very mature experience in regulating transactions, credit evaluation and credit transactions.Through the combination of these trading platforms, and with banks and other organizations to form a trading alliance, based on the alliance chain to achieve transaction transparency, multi center.

The credit mortgage transaction alliance is responsible for sorting nodes and endorsement nodes in the alliance chain, and has sorting right, endorsement right and bookkeeping right.The sorting node is similar to the miner in bitcoin mechanism. It sorts the transaction request and the transaction result, and packs them into blocks. However, since the node is held by alliance members, it does not need to consume a lot of computing power to fight for the accounting right.The responsibility of endorsement node is similar to that of consensus node in bitcoin mechanism, which tests the validity of smart contract and runs smart contract. If the operation result is correct, the sorting node will be packaged into blocks and stored in the alliance chain.Endorsement nodes need to master all the data on the alliance chain to verify and run the smart contract, so each endorsement node must access all the chain data.

#### 4.1.2 Transaction subject of credit mortgage

The main body of credit mortgage transaction refers to the account that uses the smart contract to carry out credit mortgage transaction in the alliance chain, as the participant of the service, only has the bookkeeping right.Any legal person or individual can become the transaction subject and carry out credit mortgage transactions on the alliance chain. However, before the first transaction, it is necessary to register and pass the CA certification of the alliance chain, the account will be valid, and the relevant account information will be stored in the account chain; if it cannot pass the CA certification and the account is invalid, it cannot be traded on the alliance chain.

When the credit mortgage transaction subject signs the smart contract on the alliance chain for transaction, if it needs to write in the mortgage assets to ensure that it can fulfill its obligations according to the contract, it can deduct part of the mortgage assets to be written in through the account credit value, which can not only guarantee the rights and interests of the transaction subject, but also not increase its capital pressure.The transaction subject can not only propose the transaction invitation through the smart contract on the alliance chain and wait for the response from the interested customers on the chain, but also can reach an agreement between two or more parties online to convert the contract into a fixed language and format of the smart contract through the API interface and deploy it on the alliance chain.

#### 4.1.3 Trust data source

Smart contract credit mortgage transaction does not exist independently. When the smart contract is automatically executed, the endorsement node needs external transaction data as the basis to judge whether the contract meets the execution conditions.The source of trust data is the provider of external data on the alliance chain. Through the smart contract, the data off the chain is linked and the blockchain ledger is updated.

The external data mainly includes two types: one is the account information on the alliance chain, which is used to improve the basic information of the account and serves as the basis for evaluating the original credit, and will be stored in the account chain; the other is the data related to the transactions on the alliance chain, which is the basis for the endorsement node to evaluate the implementation of the contract, and will be stored in the transaction chain.As a provider of external data, the data written into the alliance chain affects the credit and execution of the transaction entities on the chain, so it needs 100% credibility.Trusted data sources mainly refer to authoritative databases directly connected to the alliance chain, including institutions, Internet of things devices, alliance chain accounts, etc.To register as a trusted data source, it needs to pass the CA authentication of the alliance chain, and its account information will also be deposited into the account chain.

In the form of creating a smart contract, the data outside the chain will be written into the corresponding chain, and the source account will be automatically signed to ensure that the data source on the chain can be checked.In the process of smart contract execution, it is necessary for the transaction subject to fulfill all terms and obligations in the contract, as a condition to judge the execution of the contract.At this time, it can access authoritative data centers such as the state and the government; or it can automatically detect and record the transportation status of physical goods by Internet of things devices; it can also select credible data sources through incentive mechanism, which will write external data into the blockchain ledger in the form of smart contracts.When the contract execution period is reached, the endorsement node runs the smart contract based on the data.

### 4.2 Smart contract credit mortgage transaction accounting channel

In order to reflect the credit value, reduce the probability of default in the transaction without increasing the capital pressure, create a good market transaction atmosphere, and make the relevant data transparent and searchable, this system plans to establish three channels, account, transaction and credit, based on the fabric alliance chain, respectively to record all account information, intelligent and contractual transactions, and account credit on the chain.Multi channel can be understood as dividing the whole alliance chain into multiple sub chains, each sub chain is separated, but there are corresponding links. Compared with a single chain, it is more convenient for data management on the chain.

#### 4.2.1 Account chain

The account chain records the information of all kinds of accounts on the alliance chain.The traditional blockchain guarantees the security of accounts and transactions through asymmetric encryption of public key and private key, but at the same time, it also makes the transaction subject anonymous, which becomes the hotbed of nourishing illegal transactions and makes transactions uncontrollable.Smart contract transaction based on credit mortgage requires openness and transparency, so when creating new users, it is necessary to create corresponding blockchain users on the chain at the same time, including user name, user phone, user core basic information, etc., and generate corresponding private key and public key by using elliptic curve encryption rules, and the public key information is stored in the deblock account book.Any account can download the blockchain ledger to the local, and query the corresponding account's financial status, transaction information, credit value and other information through the blockchain user information or public key.

#### 4.2.2 Trading chain

The transaction chain records all information of transactions through smart contracts on the alliance chain.During the transaction, the transaction entity can put the physical transaction objects into the IOT intelligent equipment transport box, which is used to record the goods status such as quantity and quality at any time.When the seller puts the goods into the intelligent equipment transportation box, the equipment will record the goods status at this time and send it to the contract of the blockchain in the form of transaction; during the transportation, it will record the goods status regularly and send it to the contract of the blockchain; when the goods are transported to the buyer, the intelligent equipment will also record the goods status at this time and send it to the blockchain.The signature of the transaction is completed by the device to prevent artificial forgery.The goods status will be automatically recorded in the blockchain ledger. When the bookkeeping node runs the smart contract, the contract code will automatically get the operation result according to all the relevant records on the blockchain. After the code runs, the corresponding result operation will be performed on the trading entity account.

#### 4.2.3 Credit chain

The credit chain records the credit information of the account on the alliance chain.Based on the financial status of the transaction subject and the important credit information such as credit, the original credit obtained shall be interconnected with the authoritative credit platforms such as the bank and the national credit statistics platform to update the original credit value of the transaction

subject in real time; the transaction credit shall be updated after each transaction is completed; if any credit value is changed, the total credit will be updated in real time and recorded in the blockchain ledgerMedium.

### 4.3 Function module of smart contract credit mortgage transaction

#### 4.3.1 CAAuthentication module

CA authentication module is used to verify the validity of the account on the alliance chain, and to ensure the authenticity and legitimacy of user information.

CA center issues a digital certificate for each user who uses the public key. The function of the digital certificate is to prove that the user listed in the certificate legally owns the public key listed in the certificate.The digital signature of Ca organization makes it impossible for attackers to forge and tamper with certificates.CA is responsible for issuing certificates, certification certificates and management of issued certificates.It needs to formulate policies and specific steps to verify and identify the user identity, and sign the user certificate to ensure the identity of the certificate holder and the ownership of the public key.The CA also has a certificate (with a public key) and a private key.Public users on the Internet trust Ca by verifying CA's signature. Anyone can get CA's certificate (including public key) to verify the certificate it issues.

If the user wants to get a certificate of his own, he should first apply to the ca.After the CA determines the identity of the applicant, it assigns him a public key, and the CA binds the public key with the identity information of the applicant, and signs for it, and then forms a certificate and sends it to the applicant.If a user wants to verify the authenticity of another certificate, he uses the CA's public key to verify the signature on that certificate. Once the verification is passed, the certificate is considered valid.

#### 4.3.2 Credit evaluation module

In the credit evaluation module, according to the account information, transaction information and credit information in the account book of the alliance chain, the credit value obtained will be stored in the credit chain and the account credit information on the alliance chain will be updated.

The original credit of the transaction subject, including its asset status, credit status and other original information as well as the transactions in the smart contract, will be included in the database of the module. The server will conduct standardized credit evaluation on the transaction subject based on the data in the database.The result of credit evaluation serves as the basis for judging the credit situation and calculating the credit value of the transaction subject.

#### 4.3.3 Credit mortgage module

The credit mortgage module calculates the credit value based on the credit value obtained in the credit evaluation module and the average transaction amount of the transaction subject, and can offset the mortgage assets that need to be written in advance in the transaction.When a transaction entity creates a smart contract, if it is unable to write in enough transaction funds temporarily, and needs to write in the mortgaged assets, it can write the credit value into the contract, so as to write in the mortgaged assets with the corresponding value deducted.So as to realize the use of the credit value of the transaction subject and reduce the occupation of the assets of the transaction subject.

#### 4.3.4 Default penalty module

If there is a breach of contract in the transaction process, the mortgaged assets are required to make up for the loss of the defaulted party. According to the law, the mortgaged assets cannot be transferred directly to the defaulted party.In case of default, if the defaulting party takes the initiative to compensate the losses of the defaulted party, its mortgaged assets will be automatically returned to the original account; otherwise, the defaulting party's mortgaged assets will automatically carry out the auction procedure according to the contract provisions, and the auction proceeds will preferentially repay the losses of the defaulted party.If the auction proceeds are insufficient to compensate, the defaulting party shall make up the losses. Before the losses are made up, the account and assets of the defaulted party will be locked and cannot be traded on the smart contract system; if

the auction proceeds are higher than the losses of the defaulted party, the remaining auction proceeds will be transferred to the account of the defaulting party.

## 5. Conclusion

In this paper, the intelligent contract credit mortgage transaction system is established from three aspects: participant, accounting channel and function module.Participants include three parts: transaction alliance, transaction subject and data source, which are the operation supervisor, transaction party and data provider outside the chain of intelligent contract credit mortgage transaction system; accounting channel includes account chain, transaction chain and credit chain, and all kinds of data on the system are recorded in different chains to facilitate data search and use; functional modules include CA certification, credit evaluation and credit offsetThere are four modules of pledge and penalty for breach of contract. Each module cooperates with each other to jointly realize credit mortgage and promote compliance transactions.

## References

[1] Androulaki E, Barger A, Bortnikovv, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains[C]//Proceedings of the Thirteenth EuroSys Conference. ACM, 2018: 30.

[2] Buterin V. A next-generation smart contract and decentralized application platform [EB/OL]. 2013[ 2018-11-12].https://github.com/ethereurm/wiki/wiki/white-paper.

[3] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[EB/OL].2008-8-04[ 2018-6-04]https:/ /bitcoin.org/bitcoin.pdf.

[4] See Christopher D.Clack,Vikram A. Bakshi & Lee Braine, Smart Contract Templates: Foundations, Design Landscape and Research Direction [EB/OL].2016-08-04[ 2018-11-12]. https://arxiv.org/pdf/1608.00771v2.pdf.

[5] Swan M. Blockchain: Blueprint for a New Economy [M] Sebastopol, CA: O'Reilly Media, Inc, 2015.

[6] Szabo N. Formalizing and securing relationships on public networks [EB/OL].1997[ 2018-6-04]https://firstmonday.org/ojs/index.php/fm/article/view/548/469.DOI:http:/dx.doi.org/10.5210 /fm.v2i9.548.

[7] William Mougayar, The Business Blockchain: Promise, Practice and Applications of The Next Intermet Technology.[M]. Wiley, 2016:42.

[8] Chai Zhenguo. Thinking about the contract law of smart contracts under blockchain [J]. Guangdong Social Sciences, 2019 (04): 236-246.

[9] Hu Shouyong. Social effects of the system of releasing the list of dishonest Executees [J]. Chongqing Social Sciences, 2013 (09): 30-36.

[10] Ni Yunwei. Civil law analysis, application and Enlightenment of smart contract under blockchain technology [J]. Journal of Chongqing University (SOCIAL SCIENCE EDITION), 2019,25 (03): 170-181.

[11] Shen Jing, Tian Qiang, Du Yuyong. Statistical analysis on the implementation of the system of publishing the list of dishonest Executees [J]. Hebei law, 2016,34 (05): 188-198.

[12] Tan qiugui. On the relationship between civil enforcement mechanism and social credit system [J]. Quest, 2009 (02): 132-134.