A lending scheme based on smart contract for banks

Fujian Zhu*, and *Chunhai* Zhang

Ocean University of China, Department of Computer Science and Technology, 266100 Qingdao, China

Abstract. In this paper, we work towards bank loans. This task is non-trivial due to the following problem: small enterprises and individuals have difficulties in lending, banks bear high risks, and the lending business is greatly affected by the subjective influence of staff. Towards this end, we propose a novel loan investment model and smart contract algorithm. Afterwords, we build an intelligent risk control evaluation algorithm based on deep learning. To justify our work, we implemented a distributed application that can run safely. In addition, using the data set of paipai loan, the accuracy of our intelligent risk control evaluation algorithm is 94.33%.

1 Introduction

In the traditional way of bank lending, some users deposit money in the bank, and the bank lends money to borrowers. In the loan, the bank bears the risk of the loan alone. According to the survey, banks tend to grant loans to industries supported by the government in each period, and the staff are more optimistic about relevant enterprises subjectively[1], resulting in difficulties in lending to small enterprises and individuals.

It is worth mentioning that blockchain have been devoted to digital asset trading[2], crowd funding[3], product traceability[4], etc. In particular, according to Chunhua's analysis and comparison of various lending methods, it is proved that blockchain technology has a good application prospect in lending[5], which cannot be applied because it does not realize a complete lending process; To alleviate such problem, some scholars designed a simple one-to-one loan scheme[6]. However, the lack of a solution when the loan is not repaid on time leads to the incomplete loan processing scheme. Nevertheless, this method ignores the loan needs of small enterprises, who have greater capital needs. Besides, they suffer from the inability to review the qualifications of borrowers. However, it is non-trivial to build an effective lending scheme for the following reasons: 1)The anonymity of the blockchain[7] cannot locate specific users. Therefore, it is impossible to review the borrower's qualification and solve the problem of default. 2)To reduce the subjectivity of loan business personnel, it is important to have an accurate intelligent evaluation model. To improve the success of borrowing, more diversified forms of borrowing are needed[3].

* Corresponding author: attachedjeff@gmail.com

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).

To address the above issues, we propose a multi-party participation model, which is BBBI lending investment model based on blockchain, as illustrated in Figure 1. We first design three participation roles: bank, investor and borrower to reduce the harm of anonymity.Thereafter, we adopted the many to one crowd-funding method for the loan relationship and conducted transactions based on the smart contract algorithm. Meanwhile, in order to provide better repayment ability evaluation, we trained an intelligent evaluation model based on deep learning. The contribution of this work are three-fold: 1)We propose BBBI(Blockchain-Borrower-Bank-Investor) loan investment model and design a complete trading intelligent contract algorithm, which is able to meet the loan needs of small enterprises and individuals and disperse the risks in loans. 2)We trained an intelligent evaluation model to provide more accurate prediction results than the existing schemes, which can reduce the impact of subjective decision-making of banking personnel. 3) We demonstrate the feasibility of the scheme by implementing a distributed program.

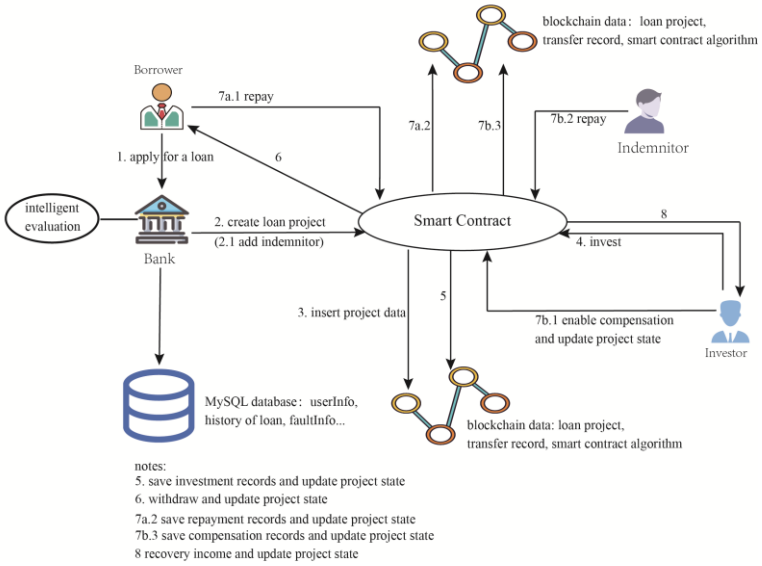

Fig. 1. BBBI model.

2 Design and implement BBBI loan invest model

2.1 Blockchain and smart contract

Blockchain is a chain composed of blocks containing data transaction information in sequence. In a narrow sense, each block contains the hash value and timestamp of the parent block. Cryptography technology is used to ensure that the data can not be tampered and forged. It is a decentralized distributed ledger database[8]. Blockchain plays an important role in trading and lack of trust by virtue of its tamperability and traceability. Ethereum blockchain[9], which supports smart contracts, is called the blockchain 2.0 era. It enhances the script function and makes it possible to use blockchain in real scenarios.

Smart contract[10] points out that "many contract terms can be embedded into the hardware and software we process, so that the violation of the contract becomes expensive". Combined with blockchain, it can program participants, legal agreements and relevant business logic, and can be regarded as laws in the code to ensure the normal implementation of loan and mortgage agreements.

2.2 BBBI loan invest model

We designed a BBBI lending and investment model with banks as intermediaries. In this model, participants include borrowers, investors, banks. On the one hand, in order to store the borrower's personal information and evaluate and detect the borrower's repayment ability, on the other hand, in order to protect the borrower's privacy, the privacy data is not stored in the blockchain, and these contents are uniformly responsible by the bank. After the borrower submits an application and passes the intelligent evaluation, the bank creates a loan project and stores it in the blockchain. The loan transaction is completed by the borrower and the investor through the intelligent contract algorithm. The indemnitor is a credit endorsement when the borrower lacks mortgaged assets. When the borrower defaults, the bank will contact the indemnitor for handling. The overall model flow chart is shown in Figure 2.

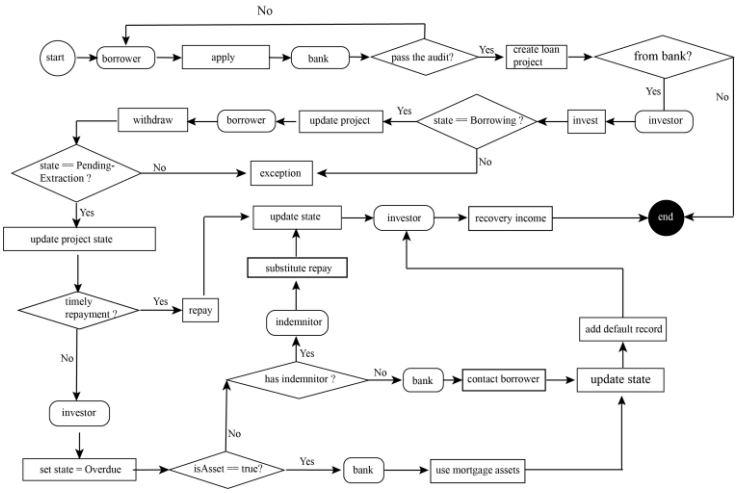

Fig. 2. Model flow chart.

2.3 Smart contract algorithm

This part is used to describe the relevant smart contract algorithms designed. Due to the limited space, it only introduces the algorithms for creating loan projects, investing loan projects and compensation. At the same time, it explains some ingenious designs to ensure the legitimacy of the algorithm.

2.3.1 Create loan project

In order to store loan information in the blockchain, we constructed a loan information

Structure, as shown in Table 1. The enumeration type SubjectState represents the state of an

Object. It includes five states: Borrowing, PendingExtraction, Extraction, Overdue and Completed. If there is a indemnitor, you can associate the information of the indemnitor after creating the loan project and store it in the creditPeople (mapping (uint = > address) variable. In order to protect the privacy of the indemnitor, this information is not displayed with the loan information.The borrower can set the loan interest amount. If the borrower wants to successfully borrow as soon as possible, it can appropriately increase the loan interest to the extent permitted by law. When a loan project is created, the creator's address

is reconfirmed to ensure that it is created by the bank. The algorithm for creating a loan project is as follows:

Input: borrowerPK, desc, interest, targetTotal, endTime, repayTime,isAssert,state=SubjectState.Borrowing, amount=0, isCompensation=false

Output: transaction hash value

Step 1: if (msg.sender == Owner) then; // chechk address valid

Step 2: id = subjectNum++; // generate new ID

Step 3: Subject = new Subject(id,...state); // create new loan

Step 4: end if;

Step 5: else return Error;

Step 6: return transaction hash;

Table 1. Loan information structure.

	Field	Data type
1	id	address
2	borrower	string
3	loanDetail	uint
4	loanInterest	uint
5	loanAmount	uint
6	deadlineTime	uint
7	repayTime	uint
8	amount	uint
9	isCompensation	bool
10	isAsset	bool
11	state	Subject State

2.3.2 Invest loan project

The investor calls the investment contract algorithm to complete the judgment of relevant conditions and transfer transactions. In the program, the subject And Investor (mapping (uint => Investors) variable is stored to ensure that a loan project corresponds to an investor set. The structure of the loan project and the investor set is shown in Figure 3. Through the project ID, it can quickly locate the investor set to query the investor and the corresponding investment amount, and the query time complexity is O(1). The funds will be deposited in the smart contract account, and the borrower can withdraw the total borrowed amount after deadline. The preconditions for investing a loan project are: the project status is Borrowing, the current time is earlier than the deadline and the investment amount is legal. If the amount in the project is equal to the loanAmount after the investor transfers, the status of the project will be set to PendingExtracted. The algorithm for investing a loan project is as follows:

input: msg.sender, projectId, msg.value

output: transaction hash value

step1: Subject sub = subjects(projectId); // get loan project

step2: if (sub.state == 0 && now() < sub.deadlineTime) then;

step3: if (msg.value > 0 && msg.value <= NEED) then;

step4: sub.amount += msg.value; // update amount

step5: if (sub.amount == sub.loanAmount) then;

step6: sub.state = PendingExtracted;

step7: end if;

step8: subjects(ID) = sub; // update project

step9: subjectAndInvestor[ID].nums++;

step10: recordInvestor = msg.sender;

step11: recordValue = msg.value;
step12: withdrawState = false;
step13: end if;
step14: else return Erroe;
step15: return hash;

2.3.3 Compensation

If the borrower fails to repay on time, any user of the investor can set the project state as Overdue. The smart contract algorithm will automatically judge whether the subject matter has mortgage assets. If so, the bank will perform mortgage asset liquidation; Otherwise, the project will appear in the account of the indemnitor and be repaid by the indemnitor. The precondition for the implementation of compensation is: the status of the project is Overdue, the investor enables the compensation, the compensatory account is consistent with the current calling account and the amount of repayment is in line with the actual amount. The algorithm is as follows:

Input: msg.sender, msg.value, projectId
Output: transaction hash value
step1: Subject sub = subjects(projectID); // get loan project
step2: creditPeople.address = creditPeople(projectID);
step3: if (creditPeople.address==msg.sender) then;
step4: if(sub.state==Overdue) then;
step5: if (sub.isCompensation) then;
step6: repayTotal = a * sub.loanInterest + sub.amount; // a is sub.amount / sub. Loan Amount
step7: if (repayTotal == msg.value) then;
step8: sub.state = Completed; // update project state
step9: subjects(ID) = sub; // update project
step10: end if;
step11: return transactionHash;

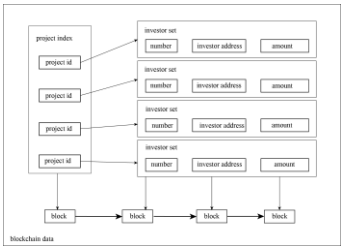

Fig. 3. Investors structure of project.

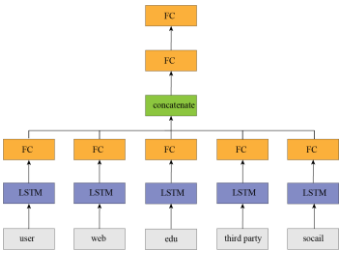

Fig. 4. Network model diagram.

2.3.4 Intelligent risk control algorithm

We used 30000 risk control data sets from paipai loan disclosure, including 255 attributes in five categories, including user information, educational background and third-party platform information. The labels of the data set are 0 (default) and 1 (non default). We randomly took 24000 as the training set and the remaining 6000 as the test set to evaluate the performance of the model.

In the field of intelligent evaluation and prediction of loan risk control, machine learning methods such as logistic regression and gradient boosting decision tree have been widely used[11-12]. However, few researchers use the idea of deep learning based on

neural network to solve this prediction problem. The deep learning model we built is shown in Figure 4. The overall idea is to learn and reduce the dimension of each category of features separately, and make a prediction after comprehensively considering all the dimensionality reduction features. After data processing, the data are input to the corresponding network branches according to categories for feature learning and dimensionality reduction. Each network branch contains two hidden layers. The first layer is a long-term and short-term memory network for learning the input nonlinear features, which performs well in nonlinear relationship modeling; The second layer is the full connection layer which compresses and reduces the dimension of features to reduce the amount of calculation of neural network. Finally, all the features after dimensionality reduction are connected together, and the prediction results are obtained after the learning of two-layer full connection layer. We use Adam as the optimizer, set the learning rate to 0.01, select cross entropy as the loss function, batch size = 100, and train the final model after 150 rounds.

3 Results

We implemented a distributed application to verify the scheme, which is based on Mac OS operating system, adopts truffle framework and related dependencies, and uses Ganache Ethereum blockchain and Metamask wallet.

In order to test the time delay and gas cost of creating loan projects, the results of every five projects are used as a group to calculate the average time delay of each group. Randomly select 10 groups of data, and the test results are shown in Figure 5. The complexity of the algorithm for creating the loan project is O(1). Since all data needs to be stored on the chain, the amount of data in each subject will affect the gas fee. The delay is mainly affected by the network during operation. When the gas price is 20gwei, it can be seen that the lowest delay in the test results is 3S, the highest is 4S, and the highest average gas fee is 0.005553eth, The lowest average gas cost is 0.004197eth, which achieves the ideal effect.

The throughput change of function write data is shown in Figure 6. The write data includes verification conditions, packaged transactions and generated blocks. The repayment algorithm process is relatively simple, so the write data throughput is the highest. With the increase of the number of visits, the throughput decreases slightly. However, it tends to be stable as a whole, which can meet the needs of users.

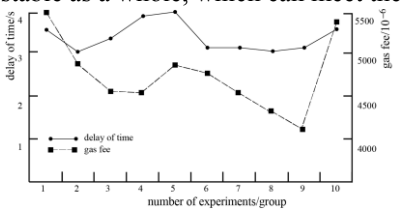

Fig. 5. Analysis diagram of create project.

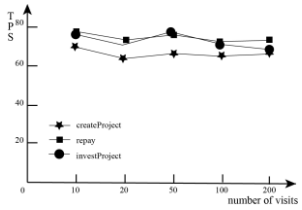

Fig. 6. Throughput of write data.

Table 2 shows that compared with the prediction results of logistic regression and gradient boosting decision tree, the accuracy of our evaluation model has reached 94.33%, reaching the current mainstream level.

Table 2. Comparison of prediction result.

	Prediction model	ACC
1	Logistics regression	94.23
2	Gradient boosting decision tree	94.30
3	Our model	94.33

4 Conclusions

The main research of this paper is to provide a new way for bank loans based on blockchain and smart contract. We propose an BBBI loan investment model, design the relevant smart contract algorithm, and build an intelligent risk control evaluation model algorithm based on deep learning. Finally, we implement a program to verify the feasibility of the research. With the further development of technology, blockchain and deep learning will be more closely combined with financial lending scenarios. We will continue to improve the logic of relevant smart contract algorithms to adapt to more complex financial scenarios.

References

1. J. Y. Hu, The status, problems and countermeasures of credit financing of strategic emerging industries-based on the game analysis of "Hasani Conversion", Soft Science, **35(2)**,1-6(2021)
2. K. Lv and K. J. BAO, Design and implementation of digital asset trading system based on blockchain, Software Guide, 17(7), 209-213(2018)
3. J. H. Huang, L. C. Gao and Y. Z. Xu. Smart contract design on crowdfunding blockchain, Journal of Information Security, **3(3)**,211-219 (2017)
4. K. K. Wang, Z. D. Chen and J. Xu, Efficient traceability system for quality and safety of agricultural products based on consortium blockchain, Journal of Computer Applications, **39(8)**, 2438-2443(2019)
5. C. H. Ju, J. B. Zou and X. K. Fu, Design and application of big data credit reporting platform integrating blockchain technology, Computer Science, **45(11A)**, 522-526(2018)
6. Y. Li, Y. J. ZHOU and Y. T. Liu, *Design of decentralized personal loaning platform based on blockchain.*(IEEE International conference on electronic information technology and computer engineering. Xiamen, April 2019)
7. S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system, https:// bitcoin.org/files/bitcoin-paper/bitcoin_zh_cn.pdf, 2008
8. J. F. Wei, X. D. Li and F. R. Yu, *Blockchain Principle, Architecture and Application*, Beijing: Tisinghua University Press, 2019
9. V. Buterin, Ethereum: a next generation smart contract and decentralized application platform.https://ethereum.org/en/whitepaper/, 2017
10. N. SZABO, The Idea of Smart contracts, https://www.fon.hum.uva.nl/rob/
11. Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/
12. szabo.best.vwh.net/idea.html.
13. M. Ben Rabha, M.F. Boujmil, MZ. Y. Liu, Research on credit risk control based on machine learning. Nanjing, Nanjing University of Posts and Telecommunications, 2020
14. X. Y. Wang, Research on big data risk control model based on GBDT algorithm. Journal of Zhengzhou Institute of Aeronautical Industry Management, **38(05)**, 108-112(2020)