Based on point-to-point network extended credit authentication model

Jianyao Ma¹, Zhanjie Wen²

¹,²Internet financial information engineering college, Guangdong University of Finance, Guangzhou City, Guangdong Province, P. R. China

Corresponding author and e-mail: Zhanjie Wen, 70-154@gduf.edu.cn

Abstract. Research shows that P2P technology exist many problems about reliability in the Internet credit industry. It has become particularly important to ensure the reliability of users and improve the success rate of transactions. In this paper, the traditional trust identification model is improved, and the P2P business transaction is integrated into the credit identification model as a dynamic indicator. On this basis, a block chain is constructed with credit recognition model as intelligent contract. Through the block chain network based on the credit identification model, the credit value of each user will be dynamically evaluated. The block chain network will ensure the credibility of the dynamic indicators of transactions, so as to ensure the reliability of the customer credit value evaluation. Therefore, a quantitative standard that both parties can trust can be established. Without the guarantee of the third party, both sides of P2P transaction can define the trustworthiness of the transaction parties. That guarantees the reliability of the transaction.

1. Introduction
P2P (peer to peer), also known as point-to-point connection or peer-to-peer network, is an Internet technology, which changes the traditional server-centric Internet application model into a user-centric peer-to-peer model. The domestic P2P market was launched at the end of 2000. After nearly 20 years, P2P technology has developed rapidly in China and has been successfully applied in many industries. Among them, the application in the Internet credit industry is particularly prominent. However, due to the characteristics of P2P network with anonymous letters, the reliability of both sides of the transaction cannot be guaranteed, resulting in uncertain risks in the transaction and restricting the scale of the transaction. Therefore, it is particularly important to solve the reliability of P2P transaction. Therefore, this paper according to the reliability of the P2P trading problem, put forward a model based on peer-to-peer network extend credit certification. Through the model for each customer credit assessment of P2P trading, defines the credible degree of both parties, and the reliability of the definition of trade, so as to reduce the risk of trading, as well as P2P enterprises improve risk control ability to provide a reference.

2. Based on point-to-point network extended credit authentication model

2.1. Based on the point - to - point network extended credit authentication model framework
2.1.1. **Personal credit risk assessment.** Personal credit risk assessment can accurately estimate the risk of consumer credit, providing lenders with a technical means to avoid bad credit and reduce the risk of lending. At present, the common methods of personal credit risk assessment at home and abroad mainly include discriminant analysis method, expert scoring method and neural network method.

The decision analysis method generally selects some indicators of the credit characteristics of the evaluation object and builds a relevant model through the deduction of the judgment. Through this model, the research object can be classified and predicted, and its credit rating can be located. After Fisher et al. [1] highlighted the discriminant analysis method, Durand et al. [2] first applied it to the identification of non-performing loans, and many researchers later improved this method, such as the multivariate judgment analysis method, so as to better predict the personal credit risk.

2.1.2. **Personal credit risk assessment factor.** Based on the understanding of the current research on personal credit model [3], the paper takes it as an influence factor of the credit model and define it as Per. Due to different judgment models of personal credit evaluation, the output result may be continuous value, binary value or discrete value, so the paper defines the influence factor Per as the following expression in detail.

\[
\text{All}_\text{Per}(u_i) = \left \{ \begin{array}{ll}
\text{Per} & (\text{Per} \in \{x|x \text{ is a continuous value}\}) \\
\text{Per}_i & (\text{Per} \in \{x|x \text{ is a discrete value}\}), \ i \in \mathbb{Z} \end{array} \right.
\] (1)

In equation (1), when the Per is a continuous value, the paper directly take the Per factor as an influence factor of the model, and then make a weight on it when building the model. When Per is a discrete value, the model encode different discrete values of Per factor, and set the code as integer I. The code is processed by the actual application scenarios of the model, so as to make the discrete value continuous. The coding process should be segmented with the continuous value to obtain a corresponding number.

2.1.3. **Guarantor factor.** Borrowing from the model of Lending Club [4], the paper add a guarantor factor into the credit identification model to increase the credibility between customers through the guarantor. For this, the paper use Bon(u_i, u_j) to indicate that user u_j is the guarantor of user u_i. As explained in the first part, the guarantor assumes part of the transaction responsibility of user u_i and also enjoys part of the benefits provided by u_i. In this regard, there are different weights for different undertakers, and different guarantors are given weights in the model. The guarantor factors are defined as follows.

\[
\text{All}_\text{Bon}(u_i) = \sum_{j=h:b \to h+1} d_j \text{Bon}(u_i, u_j) \quad (i, j \in \mathbb{N})
\] (2)

In formula (2), since there may be one or more guarantors, or there may be no guarantors, and they are integers, the values of i and j belong to natural Numbers. For different guarantors, the risks shall not be different. The model uses weighted representation, and j represents the serial Numbers of different guarantors. Finally, the model sum up the values of all the guarantors, and finally it gets that the value of the guarantors is\text{All}_\text{Bon}(u_i), and u_i represents the user.

2.2. **User trust on both sides of the transaction**

2.2.1. **User trust model.** Trust refers to the supplier's belief in the demander's ability to deliver the agreed services in a given context and time frame. In peer-to-peer networks, the paper measures the reliability of transactions using point-to-point, or trust, between users.

Through the research, it can find that the trust relationship is generally dependent on the context environment of the user, and has the properties of unidirectionality, inequality, dynamics, transitivity, homogeneity and so on. Here the model represents trust relationships between users through directed graphs.
In Figure 1, the trust relationship between users on each node can be seen. In addition, due to the transitivity of trust, as can be seen that A indirectly trusts C, and different values after connection can reflect the asymmetry of trust relationship. Based on the above theory, the model of this paper will improve the existing context and graph trust model.

2.2.2. An improved user trust model based on P2P transaction scenarios. The research of I-Trust model shows that Trust between users is related to user similarity, interaction degree and user reputation. Through the graph model and the trust relationship, it is found that the trust between users is related, rather than isolated. Considering the characteristics of P2P transactions, the model of paper improved the context-based trust model and added dynamic evaluation factors. The output of the trust model is denoted as Tr, and the frame diagram of the trust measurement model is as follows.

Figure 2. Frame diagram of credit model.

Figure 3. The influence of equal weight coefficient on trust value.

Figure 2 shows the frame diagram of the trust model of user A and user B, which is improved by combining the features of P2P transactions with the context-based trust model. User trust was calculated by the similarity of customer base information, the number of co-sponsors and the degree of customer transactions.

From the frame diagram of the trust model, the trust value formula between users as follows.

\[
All_{-}Tr(u) = \sum_{j\neq i} Tr(u, u_j)
\]
Tr(u_i,u_j) = a \cdot Bis(u_i,u_j) + b \cdot Gua(u_i,u_j) + l \cdot Dea(u_i,u_j) \quad (4)

In equations (3) and (4), \(u_i\) and \(u_j\) represent the two sides of the P2P transaction, \(Bis\) represents the similarity between the two sides, \(Gua\) represents the number of co-guarantors between the two sides, \(Dea\) represents the existing common trading volume between the two sides.

For the output of the model, there are three types of binary discrete trust, multi-valued discrete trust and continuous value according to the different measurement criteria. Discrete trust is used in decision making, including trust, distrust, general trust and extraordinary trust. However, since the trust model includes dynamic P2P trading as an evaluation factor, and different exchanges focus on different factors. For this, the model weighted the three factors of the trust model, and set the sum of the weighted coefficients as \((\alpha + \beta + \lambda = 1)\), and standardized the trust value obtained by the score. The following is the specific definition of the three factors.

Basic similarity value \(Bis(u_i,u_j)\); According to the research, each node in the social network has homogeneity, that is, it tends to be connected with similar nodes. For this reason, in the trust model based on P2P transaction, the model add similarity between nodes to balance the trust value between users improved by clustering effect brought by homogeneity. Take the trust frame diagram 2-2-2 as an example, the basic information set is denoted as \(S_{\text{basic}}\), and the transaction preference set as \(S_{\text{hobby}}\). The basic information set includes a subset of the commonly used factors of personal credit assessment, mainly including the basic financial information and basic information of users.

According to the Jaccard similarity coefficient, the basic information similarity formula is as follows:

\[
Bis_{\text{basic}}(u_i,u_j) = \frac{\text{size}(S_{\text{basic}}(u_i) \cap S_{\text{basic}}(u_j))}{\text{size}(S_{\text{basic}}(u_i) \cup S_{\text{basic}}(u_j))}
\quad (5)
\]

In formula (5), the \text{size()} function is defined to calculate the number in the set, so as to make the ratio of the set continuous.

According to the Jaccard similarity coefficient, the similarity formula of trading preference information is as follows:

\[
Bis_{\text{hobby}}(u_i,u_j) = \frac{\text{size}(S_{\text{hobby}}(u_i) \cap S_{\text{hobby}}(u_j))}{\text{size}(S_{\text{hobby}}(u_i) \cup S_{\text{hobby}}(u_j))}
\quad (6)
\]

In formula (6), the \text{size()} function is defined to calculate the number in the set, so as to make the ratio of the set continuous.

The formula for the basic similarity measure is as follows:

\[
Bis(u_i,u_j) = w \cdot Bis_{\text{basic}}(u_i,u_j) + (1 - w) \cdot Bis_{\text{hobby}}(u_i,u_j)
\quad (7)
\]

In formula (7), the model uses parameter \(w\) as the regulating parameter to standardize \(Bis(u_i,u_j)\) and adjust the evaluation data according to different trading objects. When \(w\) is small, the impact ratio of basic information is small; When \(w\) is large, the impact ratio is large.

Common guarantors; the co-sponsor factor is written as \(S_{\text{Bon}}\). According to the rule of "150", it can be known that in social network, the number of people in contact is about 150. For this, the model takes 150 as the denominator and set the upper limit of co-sponsors at 150. The formula of co-guarantor is as follows:

\[
Gua = \frac{\text{size}(S_{\text{Bon}}(u_i) \cap S_{\text{Bon}}(u_j))}{150}
\quad (8)
\]
In formula (6), the size() function is defined to calculate the number in the set, so as to make the ratio of the set continuous. \( S_{\text{Bon}}(u_i) \) is the guarantor collection of user \( u_i \); \( S_{\text{Bon}}(u_j) \) is the guarantor set of user \( u_j \), and when the co-guarantee set between users is \( \emptyset \), the function size() is 0; when the co-guarantee set is greater than 150, the size() is 150.

Measurement of customer transactions; For the calculation of user transaction measurement value, the model calculate the number of common transactions between user \( u_i \) and user \( u_j \), and calculate the ratio with user \( u_i \) and user \( u_j \) respectively, so as to obtain the transaction value of user \( u_i \) and user \( u_j \) relative to each other. The formula is as follows:

\[
\text{Deal}(u_i,u_j) = \frac{\text{size}(S_{\text{Ord}}(u_i) \cap S_{\text{Ord}}(u_j))}{\text{Ord}(u_i)}
\]

(9)

Formula (9) represents the transaction degree value of user \( u_i \) to user \( u_j \), while \( \text{Ord}(u_i) \) represents the number of P2P transactions conducted by user \( u_i \). \( S_{\text{Ord}}(u_i) \) represents the user's set of transactions.

2.3. Experimental analysis of improved user trust model

2.3.1. The experimental data. The analytical experiment used new media to broadcast the bidding sales data of e-commerce providers, and defined the live broadcast sales in the data as the result value of the trust model. The related live broadcast was used as the measurement of customer transaction degree, and the related celebrity was used as the measurement of co-guarantor. Based on the trust model previously established, the formula can be transformed based on the states of data as follows.

\[
\text{Tr}(u_i,u_j) = \alpha \cdot C + \beta \cdot \frac{N_{\text{rb}}}{\text{Max}(SN_{\text{rb}})} + \lambda \cdot \frac{N_{\text{rs}}}{\text{Max}(SN_{\text{rs}})}
\]

(10)

In formula (10), \( N_{\text{rb}} \) stands for the number of associated live broadcasts, \( N_{\text{rs}} \) stands for the number of associated celebrities, \( SN_{\text{rb}} \) stands for the number of live broadcasts of sample data, and \( SN_{\text{rs}} \) stands for the number of associated celebrities of sample data. Since the measurement of similarity is determined by the actual situation of the user, the model use constant C instead, and the other Numbers are equivalent replaced by the sample data.

2.3.2. Experimental parameter setting. In the model of sample data above, the model need to estimate each coefficient of the weighted co-efficient \( \alpha + \beta + \lambda = 1 \). For different model parameters, there may be different weighting coefficients. Based on the data of this sample set, it can be seen that when all three weighting coefficients are 1/3, the relation between the curves of the three factors and the resulting curves is as Figure 3.

As can be seen from Figure 3, the transaction degree represented by the number of live broadcast fields is the closest to the sales curve, that is, the trust value. Therefore, this example can give a higher weight to the distribution weight, while that can judge the weight of other parameters by the same method when the data are sufficient and complete.

2.4. The summary of model

Based on the above, the model be constructed according to the three factors of the point-to-point network expansion model, with a comprehensive formula (1)–(9). Finally, the model is as follows

\[
\text{Cr}(u_i) = e \cdot \text{All PER}(u_i) + m \cdot \text{All Bon}(u_i) + s \cdot \text{All Tr}(u_i)
\]

(11)
In order to make the model more adaptable, we weighted all the three impact factors of the model for different scenarios. The model could weighted and assign values to the emphasis of different factors. In order to standardize the data, we stipulated that \( \varepsilon + \mu + \sigma = 1 \).

3. Blockchain architecture of the credit authentication system

Through the second part of the building of credit identification models, as can be seen that credit authentication model have added trade as the deal P2P the impact factor, thus making credit that value into dynamic floating, this allows the user's credit and P2P trading contact more closely. However, there exists fake trades in fact, which affect the credit rating result. In addition, as for the operation of the model, in the previous centralized data storage, it was difficult to ensure the fairness of the data, and it was likely that the data was tampered, leaked and other problems seriously harmed users.

In this regard, this paper applies the improved credit authentication model to the block chain network, so that every transaction is authenticated on the block chain network. Therefore, the transaction can be dynamically added into the evaluation of credit recognition and the model is decentralized.

3.1. Consensus mechanism and smart contract of the Blockchain 3.0

Block chain technology is a deep application based on point-to-point network, which has many advantages such as anonymity, confidentiality, reliability and scalability. In this article, the Blockchain 3.0 technology will be used to build the credit authentication model.

In the architecture of Blockchain 3.0, the application of Blockchain goes beyond the application scope of finance. As a general solution, Blockchain technology is applied to all walks of life. Therefore, the architecture needs to have enterprise-level attributes, such as authentication, licensing, encryption transmission, and so on. This part of the paper highlights the concepts of consensus mechanisms and smart contract. Consensus mechanism represents an outcome that everyone agrees is right. For example, before the guessing game, a consensus is reached on who will win. This is a simple consensus mechanism in reality. Each smart contract is a set of digitally defined commitments, including agreements on which contract participants can enforce these commitments. By understanding these two definitions and combining the dynamic factor of transaction in the model, each P2P transaction is uploaded to the block chain network and broadcast to all nodes on the chain. At the same time, an intelligent contract is built according to the model. Through the contract, an account is created for each user on the block chain, and every transaction on the block chain will be broadcast on the whole block chain network. At the same time, whenever a transaction is added to the chain, the smart contract needs to be passed when building in the smart contract [5]. After the trade is verified by the corresponding work node, the user's credit value is dynamically increased according to the trade.

3.2. Construction of credit Recognition Model on Blockchain 3.0

According to the architecture of Blockchain 3.0, users can choose different consensus mechanisms or combinations of consensus mechanisms according to the actual situation. Intelligent contract is a conditional agreement running in the block chain. When the data environment meets the conditions stipulated in the contract, the contract will be automatically executed without manual triggering. To this end, that only need to write the corresponding intelligent contract and then the model can be easily deployed in a blockchain network.

3.3. The following is a credit that blocks the process of the construction of the chain network [6].

In the chain structure, there are two lists, one is the main chain formed by all the block data, and the other is the block header list formed by all the block header data. The transaction is an important data structure of the block body. The transaction is encrypted and signed by the nodes to form an instruction, and then submitted to the block chain. For this purpose, this model need construct the information of the trade in the block chain network.
The development of intelligent contract is divided into two steps, namely, the construction of user information and the realization logic of main functions. Firstly, the user information structure is constructed, and then the intelligent contract is constructed according to the model logic. The main logic of intelligent contract is to determine the credit of users and package each transaction verified by consensus mechanism into block chain.

Thus, a block chain corresponding to the point-to-point extended network credit authentication model [7] is constructed. The node issues transactions to the block chain network, and after the node consensus verification, the authorized credit value of the corresponding node is changed.

4. Summary and outlook
According to the characteristics of P2P transactions, P2P transactions are dynamically added to credit identification and evaluation, so as to specify a common judgment standard, and the judgment model is closely related to transactions, so as to reduce the risks of transactions. After the credit identification model is established, intelligent contract is written according to the characteristics of the model, and corresponding block chain is established at the same time. Thus, the credit changes in the transaction process are verified by the consensus mechanism of the nodes in the Blockchain. In this way, the reliability and traceability of the changes are guaranteed. In addition, decentralized Blockchain technology avoids the operation of third parties, thus making the data more reliable.

The disadvantages: firstly, the evaluation standards of personal credit identification are different, and the weighted parameters of the three factors cannot be adjusted well. Secondly, the parameter transition of the trust model depends on the historical data. Finally, in the construction of Blockchain network, different consensus mechanisms lead to different efficiency of transaction verification on the chain, making the efficiency of transaction non-quantifiable.

Acknowledgement
This thesis is supported by the funding from Special fund for science and technology innovation of Guangdong university students (Project number: pdjh2020b0401).

References
[1] Fisher R. A. The Use of Multiple Measurements in Taxonomic Problems[J]. Annual Eugenics, 1936,(7): pp 179-188.
[2] Durand D. Risk Elements in Consumer Installment Financing[M]. New York: National Bureau of Economic Research, 1941: pp 105-142.
[3] Theodorakopoulos G, Baras JS. On trust models and trust evaluation metrics for ad-hoc networks. IEEE Journal on Selected Areas in Communications, 2006,24(2): pp 318 – 328.
[4] Aleum Kim, Sung-Bae Cho. An ensemble semi-supervised learning method for predicting defaults in social lending[J]. Engineering Applications of Artificial Intelligence: 2019(81) pp 193-199.
[5] He Haiwu, Yan'an, Chen Zehua. Overview of intelligent Contract Technology and Application based on Block chain [J]. Computer Research and Development, 2018 (11). (In Chinese)
[6] Cai Weide, Yu Lian, Wang Rong, et al. Research on application System Development Method based on Block chain [J]. Journal of Software, 2017(6) pp 1474-1487. (In Chinese)
[7] Bi Fangming, ZHANG Hong, Yan Dashun. Research and Implementation of a Peer-to-peer Trust model [J]. Computer Application: 2006 (10) pp 2315 — 2317. (In Chinese)