Journal of Intelligent Management Decision
https://www.acadlore.com/journals/jimd

Optimization of the Trust Propagation on Supply Chain Network Based on Blockchain Plus

Ling Chen[1*], Shan Su[2]

[1] School of Management Science and Engineering, Chongqing Technology and Business University, 400067 Chongqing, China
[2] International College, National Institute of Development Administration, 10240 Bangkok, Thailand

[*] Correspondence: Ling Chen (2020658010@email.ctbu.edu.cn)

Received: 06-02-2022 **Revised:** 07-19-2022 **Accepted:** 07-30-2022

Citation: L, Chen and S. Su, "Optimization of the trust propagation on supply chain network based on blockchain plus," *J. Intell Manag. Decis.*, vol. 1, no. 1, pp. 17-27, 2022. https://doi.org/10.56578/jimd010103.

Abstract: The decentralization of blockchain technology greatly improves the trust relationship in the supply chain network. In view of the lack of trust, uncertainty, and asymmetry in the supply chain network, this paper integrates the blockchain technology to build a network dynamics model of trust representation, calculation, and propagation, and explores how the blockchain influences the supply chain network. The result indicates that the network scale increased by 115.89%, the network connectivity increased by 60.31%, and the average shortest path decreased by 4.95%, after the blockchain trust framework had been deployed in the agricultural supply chain. Meanwhile, the network topology performance such as degree distribution and average clustering coefficient were optimized to varying degrees. Taking agricultural supply chain as an example, the practical significance of topological change was explained. Overall, the blockchain trust mechanism improves the topology of the supply chain network by affecting the trust relationship between nodes.

Keywords: Trust; Blockchain; Supply chain network; Complex network

1. Introduction

Blockchain, which is widely used in supply chain networks [1], aims to form a trusted network connecting all parties [2]. According to Metcalfe's law, the value of a network equals the square of the number of nodes in that network. Therefore, the more members connected to the network, the greater its network value; the more flexible the application on the blockchain, the more prosperous its ecology; the richer the data on the chain, the more obvious its credit amplification effect.

However, the scale-free features of the supply chain network show that the few core enterprises usually establish trust relationships with multiple enterprises, while most non-core enterprises merely establish trust relationships with a few enterprises [3]. Besides, the interest bond between supply chain members is not perfect. The lack or instability of the trust relationship makes poor cooperation a common occurrence [4]. Take the agricultural product supply chain for example. Many small farmers are scattered geographically. The trust in the supply chain is mainly established through lineage and blood relations, and the cooperation between farmers and agricultural enterprises relies on emotional trust, which makes it difficult for small farmers, who appear on the edge of the network, to establish trust among supply chain members [5]. If the trust relationship between supply chain members is abstracted into a directed graph, the network would appear as a complex network containing sparse edges and lots of nodes with small in- and out-degrees.

The literature has extensively introduced the blockchain information traceability framework [6, 7] to the supply chain, trying to improve the trust relationship. However, few articles and models take basis on the trust relationship, and study how the blockchain affects supply chain networks, from the dynamics of the trust propagation network. Concerning the propagation dynamics of trust networks, the existing researches focus on the selection, prediction, optimization and propagation incentives of propagation paths. There is still a lot of room for mining network topology. Kang et al. [8] explored the problem of blockchain incentive consistency propagation, and established a

Stackelberg game model to optimize consensus propagation. Using Hamming distance, Kou et al. [9] predicted the trust between two users in trust and distrust symbolic social networks. However, trust, as quantifiable information, is not a binary choice of 0 or 1, but a trust value distributed in a certain interval.

To reveal the law that blockchain affects the evolution of supply chain trust network from the perspective of network dynamics, this paper establishes a weighted trust diffusion model based on the susceptible-infectious-removed-susceptible (SIRS) propagation model [10], and realizes the calculation and propagation of trust in the supply chain network. After the blockchain trust mechanism is introduced into the network, the authors investigated the changes in the network topology and indices of the supply chain trust relationship, evaluated the value of the supply chain network, and took the agricultural supply chain as an example to explain the practical significance of the changes in the topology indices.

2. Improved Trust Model

The modeling of supply chain network is the basis for studying the evolution and propagation of trust relationship. In this paper, the main body of the supply chain network is abstracted into nodes, and the directed edges in the network represent the trust relationship between nodes. The evolution of supply chain network conforms to the growth and preferential connection features of the scale-free network [11]. The modeling of supply chain network needs to solve three problems:

-Calculation of trust value: how nodes in the network update the trust value of other nodes according to the change of trust data;

-Propagation of trust value: how trust is propagated and represented in the network;

-Dynamic update of trust value: the trust relationship of other nodes in the network will change with the spread of trust, but the SIRS propagation model only considers the node state transition, without considering the changes of edges and edge weights in the network brought about by the node state transition. The change of the weights on the edge cannot reflect the reality that trust propagation changes the trust connection.

This paper improves the SIRS model on a scale-free network, and describes the change of trust between nodes due to the spread of trust in the network. Different from Huo et al.'s [12] study on how the scale-free network evolution affects the SIRS trust diffusion model, this paper focuses on the evolution of the scale-free network under the effect of the SIRS trust diffusion model. Considering the reality of the supply chain trust network, the authors fully characterized the network topology. Based on the directed weighted scale-free network, the SIRS trust diffusion dynamics model was improved to describe the network evolution process, including the entry of new nodes in the network, the spread of trust information in the network, the representation and calculation of trust, the dynamic change of trust relationship, and the exit of nodes from the network.

2.1 Trust Representation

To depict the trust between supply chain network with complex network theory, the supply chain network can be abstracted as a graph $G=(V,E)$ composed of the node set $G=(V,E)$ and the edge set v_i, where V is the node (enterprise or individual in the supply chain network), and v_i is the trust relationship between nodes. If trust exists between node v_i and node v_j, then there is a directed edge $e_{ij}=<v_i,v_j>$ between the two nodes. The trust relationship varies in degree between nodes. The degree of trust is represented by the trust tr_{ij} on directed edge e_{ij}. Let $tr_{ij(t)}\in[0,1]$ be the trust of v_i in v_j at time t. The greater the $tr_{ij(t)}$, the stronger the trust; if $tr_{ij(t)}=0$, there is no trust; if $tr_{ij(t)}=1$, there is full trust. Let $TR_{(t)}=(tr_{ij(t)})_{N\times N}$ be the network trust matrix at time t. If $(v_i,v_j)\notin E$, $tr_{ij(t)}$ is null, suggesting that v_i has not established the trust evaluation of v_j; if $tr_{ij(t)}$is below the trust threshold δ, then v_i does not trust v_j.

2.2 Entry of New Nodes

There are a large number of isolated nodes in the network. These isolated nodes enter the network as new nodes connecting existing nodes. Before the entry, they often do not know the trust status of the nodes in the network, and usually choose to connect the larger nodes in the network, i.e., the nodes with larger degrees in the network (including out-degree and in-degree). The probability of a new node entering the network to connect the existing nodes in the network can be expressed as $\prod i=\frac{k_i}{\sum_j k_j}$, where k_i is the degree of v_i. The number of connected edges is $m=1+[(p-\delta)\times 10]$, with $p\in(\delta,1)$ being the trust value of the new node.

2.3 Trust Calculation

The nodes that are already connected by trust edges in the network are called existing nodes. These nodes will continuously spread the trust information. They recalculate the trust value of the partners according to the updated

trust information, thereby changing the trust connections. The trust of existing nodes in the network can be calculated by the following rules.

2.3.1 Direct trust

The trust of node v_i in node j, which it has interacted with before, belongs to direct trust. If they do not trade in the next stage, the trust will continue to decay with time [13]. The decay factor is introduced as f_t(f_t<1). Then, the trust value decay of the next time step is:

$$tr_{ij(t+1)} = f_t \times tr_{ij(t)} \tag{1}$$

If they trade in the next stage, they will get a post-transaction evaluation v_j. In this case, the trust value in the next time step is:

$$tr_{ij(t+1)} = \alpha tr_{ij(t)} + \beta v_{ij(t)'},\ \alpha < \beta,\ \alpha + \beta = 1 \tag{2}$$

If the trust value $tr_{ij(t+1)} \leq \delta$, then v_i's trust in v_j turns into distrust. After a period, the state of v_i relative to v_j may turn into a trust-unaware state. Then, the directed edge e_{ij} in the network disappears.

2.3.2 Recommended trust

The recommended trust refers to the trust of nodes recommended by other nodes without interaction history. When the demand for direct trust partners is insufficient, the node will give priority to the recommended trust of trusted neighbor nodes. When calculating the recommended trust, the node will first rely on the direct trust of the intermediary to assess the reliability of the intermediary. If the intermediary is not credible, the trust value of the node its recommends will lose its reference value, because the node is more likely to trust the trust data from trusted users [13].

If node j is recommended by multiple intermediary nodes, then the more trusted the node r, the higher the weight tr_{ir} [14]. The recommended trust can be calculated by:

$$tr_{ij(t)} = \frac{\sum_{r=1}^{n} tr_{ir(t)} \bullet tr_{rj(t)}}{n} \left(tr_{ir(t)} > \delta \right) \tag{3}$$

where, n is the number of trusted intermediaries. If the recommended trust $tr_{ij(t)} > \delta$, a directed edge e_{ij} is added to the network.

2.4 Trust Propagation

Trust can be spread as information in the supply chain network, inducing the dynamic change of trust relationship in the network. The dynamic change of trust relationship in this network can be described by a typical SIRS model.

Concerning the trust of other nodes in the network for v_j, there are three types of node states in the supply chain network:

S^j: Trust unknown nodes; the trust situation for v_j is unknown.

I^j: Trust propagation node; v_j is believed as trustworthy, and its trust situation is spread out.

R^j: Distrust node; v_j is believed as untrustworthy; the trust situation of the node is not spread, and no rust will be passed onto the node.

The purpose of trust transfer between nodes is to find trusted partners and establish a transaction relationship with them. Thus, the dissemination of node distrust information is not considered.

Let $S^j_k(t)$, $I^j_k(t)$, and $R^j_k(t)$ be the relative densities of trust unknown node, trust propagation node, and distrust node of a node with degree k at time t, respectively, k=1,2,…, k_{max}. Here, k_{max} is the maximum node degree of the network. Besides, $S^j_k(t) + I^j_k(t) + R^j_k(t) = 1$ is the normalization condition.

The SIRS trust propagation model is shown in Figure 1. The state transition rules of the model abide by the following rules:

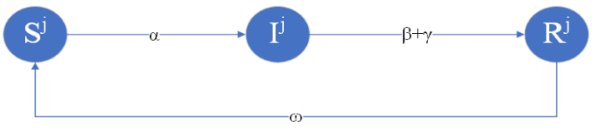

Figure 1. SIRS trust information diffusion model of traditional network

For node v_i that trusts an unknown state S^j is infected by the infected node it trusts with a trust infection rate $\alpha \in (0,1)$, i.e., the trust infection rate. This is related to the node's trust acceptance rate, and the willingness of spreading the trust information. The better the trust environment, the higher the trust infection rate.

The node v_i in the state of trust propagation $I^j(tr_{ij(t)}>\delta)$ acts as an intermediary node to propagate trust, but the trust transmitted is usually fuzzy. It only transmits whether a certain node can be trusted, and does not transmit the specific degree of trust. Therefore, the trust value transmitted through the intermediary is vaguely considered as 1, and a trust bias 1- $tr_{ij(t)}$ is generated during propagation. The credit risk brought by the trust bias may turn trusted nodes into untrusted nodes, and the probability is the mean trust bias in the network $\gamma = \overline{(1 - tr_{IJ(t)})}$ $(tr_{ij(t)}>\delta)$. The trust nodes may also provide business feedback. If they do not trade for a long time, the trust will decay and make the node untrustworthy. This probability is set as the trust decay rate $\beta>0$. Thus, trust nodes become untrust nodes with probability $\beta+\gamma$.

For the node v_i in the untrusted state R^j, the untrusted node does not accept the trust information from v_j in a short time, but may regard it as an unknown trust node after not accepting the trust information of the node for a long time. The node changes from the untrusted state to the unknown state at the probability of $\omega>0$, which is usually a very low probability.

According to the mean field theory, the propagation dynamics can be described by:

$$\begin{cases} \dfrac{dS^j{}_k(t)}{dt} = \omega R^j{}_k(t) - \alpha k S^j{}_k(t)\Theta(t) \\ \dfrac{dI^j{}_k(t)}{dt} = \alpha k S^j{}_k(t)\Theta(t) - (\beta+\gamma) I^j{}_k(t) \\ \dfrac{dR^j{}_k(t)}{dt} = (\beta+\gamma) I^j{}_k(t) - \omega R^j{}_k(t) \end{cases} \tag{4}$$

where, $\Theta(t)=\sum_j p(j/k_{(mid)}) I_j(t)$; $k_{(mid)}$ is the number of trusted infected nodes connected by the node; $k_{(out)}$ is the out-degree of the node $(0 \le k_{(mid)} \le k_{(mid)})$; $\Theta(t)$ is the probability that the node connects to any trusted infected node j at time t.

2.5 Trust Update

The spread of trust in the network will change the trust relationship between network nodes, and the transfer of the trust state of the node will alter the trust weight of the node to the node (Figure 2).

Case a: Node v_i has not established a trust relationship with node v_j. When the trust state of v_i changes from S^j to I^j, v_i establishes the trust in v_j, and $tr_{ij(t)}>\delta$;

Case b: Node v_i has established a trust relationship with node v_j, and $tr_{ij(t)}>\delta$. When the trust state of v_i changes from I^j to R^j, v_i no longer trusts v_j; the connection weight declines to $tr_{ij(t+1)} \le \delta$;

Case c: Node v_i has established a distrust relationship with node v_j. When the trust state of v_i changes from R^j to S^j, v_i loses the trust in v_j.

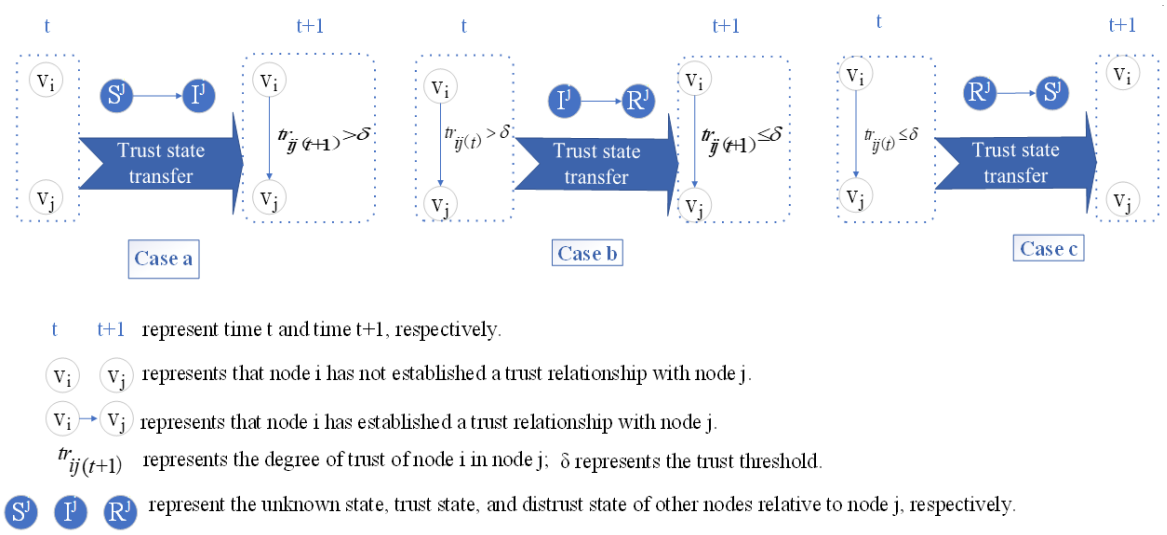

Figure 2. Transfer of trust states

3. Blockchain-Based Trust Propagation

The dissemination of trust information in the traditional supply chain network (indicated by the left superscript T) is relatively random. Recommended trust often occurs randomly with the dissemination of trust information. In a blockchain-based supply chain network (represented by the upper left subscript B), however, nodes can quickly find trusted partners to update their partner pools, according to the blockchain trust framework. The consensus network includes demanders and providers of the use value of trust data, consensus nodes, and computing nodes. Supply chain members can be demanders and providers at the same time. Mobile devices using blockchain clients can participate in consensus, and nodes with sufficient computing power can as a computing node. In the blockchain trust network, the nodes look for recommended trust nodes as follows:

3.1 Trust Digest Search

Each node stores its previous transaction information, and saves the obtained trust evaluation locally to assist itself in choosing partners. To realize the safe use of trusted data on the blockchain, the provider uses a Merkle tree to store the trust data [15]. The value of the tree root represents the "trust digest" of the trust data, the trust digest storage and the legal ID of the node. After the association is uploaded to the blockchain, the node can prove to other nodes that it has a certain trust data without exposing other information [15]. Consensus nodes in the network can view the trust digest to gain the trust data of which nodes possessed by other nodes, and the computing nodes can extract the trust data and perform calculations. There is a large fixed cost for a node $\varphi_i = \frac{h_i}{H_i}$ to find new partners through the blockchain, so nodes need to measure demand and costs. This paper uses the proportion of untrusted nodes relative to node $\varphi_i = \frac{h_i}{H_i}$ with trusted data to measure the willingness to use blockchain to find new partners:

$$\varphi_i = \frac{h_i}{H_i} \text{ (h is the number of nodes requesting distrust of node v_i; H is the number of nodes requesting trust of node v_i)} \tag{5}$$

3.2 Trust Demand Broadcast

After confirming the trust demand, the demander broadcasts it across the network. Selecting the receivers from its neighbors can effectively reduce the transaction propagation delay [16]. Thus, this paper transmits trust the demand through neighbor nodes in the blockchain network. The collection scope of trust data determines the range of demand delivery. Collecting trust data in different regions will incur different costs. Therefore, nodes need to pre-define the range of demand delivery according to their own budgets. The trust prediction of nodes using the trust data of neighbor nodes is referred to as the first-level trust propagation, and the trust prediction by the trust data of neighbor nodes of neighbors is known as the second-level trust propagation. The rest can be deduced by analogy. To compare with the neighbor node propagation trust in the traditional supply chain network, this paper assumes that the network only performs first-level trust propagation.

3.3 Consensus Processing and Trust Computing

Consensus nodes carry out transaction propagation and verification, and obtain trust computing rules. To facilitate the use of trust data and ensure that trust data is not tampered, leaked, or misappropriated, this paper adds computing nodes to the network, which will verify that neighbor nodes have indeed submitted the correct trust data. Then, the recommended trust is calculated according to the rules provided by the consensus nodes, and the calculation results are returned to the demand node.

In the traditional supply chain network, nodes do not directly disclose their trust data to other nodes. There are two possible reasons: First, the trust level of nodes to other nodes is fuzzy. Second, the leakage of trust data will cause risks to the enterprise. Therefore, the relatively vague "trust" and "distrust" information will be spread in the network. Here, ${}^{(T)}tr_{ij(t)}=[0,1]$ represent the situation of distrust and trust in the traditional supply chain network, respectively, i.e., the trust value spread through the intermediary. However, the trust of a node in the intermediary node is not fuzzy. Therefore, calculating the recommendation trust becomes the calculation of the trust in the intermediary node. The recommended trust can be calculated by:

$${}^{(T)}tr_{ij(t)} = \frac{\sum_{r=1}^{n} tr_{ir(t)}}{n}\left(tr_{ir(t)} > \delta, tr_{rj(t)} > \delta\right) \tag{6}$$

Since the trust of new nodes cannot be obtained, the authors set $p(t)=\delta$, which leads to ${}^{(T)}m=1$.

In the supply chain network environment supported by blockchain, trust data is completely recorded and traceable at all times. The collection and processing of trust data is completed by consensus nodes and computing nodes, avoiding trust data leakage, data tampering, and trust data spread in the network. For accurate and real trust data, the recommended trust value can be calculated by:

$$ {}^{(B)}tr_{ij(t)} = \frac{\sum_{r=1}^{n} tr_{ir(t)} \bullet tr_{rj(t)}}{n} \left(tr_{ir(t)} > \delta, tr_{rj(t)} > \delta \right) \tag{7} $$

3.4 Trust Update

The demand node selects the partner preferentially according to the result returned by the consensus node, completes the update of the partner pool, and updates the local trust data. The blockchain trust diffusion model is shown in Figure 3. The state transition rules of the model are as follows:

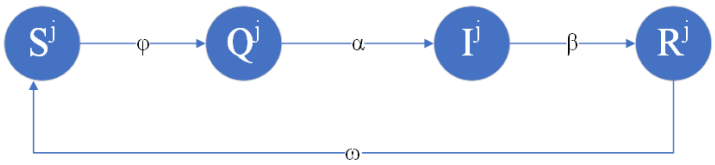

Figure 3. SIRS trust diffusion model in blockchain environment

In the complex network, the trust unknown node S^j that is willing to find partners via blockchain will temporarily transform into a blockchain survey node. The proportion of distrust nodes is denoted by $\varphi = \frac{h}{H}$, which indicates how willing a node is to look for partners via blockchain. The greater the proportion, the stronger the desire to look for new trust partners, and the higher the probability of using the blockchain tool.

The trust environment of the blockchain network is good. In this paper, the trust infection rate α of the supply chain network in the blockchain environment is set to 1 (considering the competition relationship, it is less than 1 in the actual situation).

According to the mean field theory, the propagation dynamics can be described by:

$$ \begin{cases} \frac{dS^j{}_k(t)}{dt} = \omega R^j{}_k(t) - \varphi S^j{}_k(t) \\ \frac{dQ^j{}_k(t)}{dt} = \varphi S^j{}_k(t) - kQ^j{}_k(t)\Theta(t) \\ \frac{dI^j{}_k(t)}{dt} = kQ^j{}_k(t)\Theta(t) - \beta I^j{}_k(t) \\ \frac{dR^j{}_k(t)}{dt} = \beta I^j{}_k(t) - \omega R^j{}_k(t) \end{cases} \tag{8} $$

4. Simulation and Network Evaluation

To verify the validity of our model and compare topological performance between the traditional network and the blockchain network, network evolution experiments were performed on NetworkX plus Gephi, using a Windows 10 computer with 3.20 GHz R7 5800H and 16G memory. The experimental results were randomly selected as the average of 20 replicate experiments. The network performance was evaluated by network statistical indices, such as degree distribution, average shortest path, clustering coefficient, etc. The degree distribution measures the connectivity of nodes in the network, the average shortest path refers to the average of the shortest path lengths between any two nodes in the network, and the clustering coefficient indicates the degree of node aggregation. Some studies have shown that the supply chain network would be efficient, if the average path length is short and the clustering coefficient is high [17]. In addition, the agricultural supply chain was taken as an example to analyze the practical significance of network topology optimization.

4.1 Network Initialization and Parameter Setting

In this paper, NetworkX is used to randomly generate a scale-free network of 500 nodes. The probability of a new node randomly connecting to the existing nodes of the network according to the in-degree is 0.4, and the probability of the new node randomly connecting to the existing nodes of the network according to the out-degree

is 0.1. The probability of connection between nodes is 0.5, and the trust value is randomly assigned to two decimal places. Figure 4 shows the network layout optimized by the Ruchterman-Reingold algorithm. The network is randomly generated in the light of the topological features of the supply chain trust network. The larger the node, and the greater its degree. The different colors represent the community division of the node. To improve the reliability of the experimental results, the experiment was repeated 20 times to generate 20 initial networks with an average of 808 directed edges. The maximum propagation evolution time was set as T=500; the evolution experiment was repeated in 20 initial networks respectively, and the average value was taken as the experimental result. Drawing on Hearnshaw and Wilson and Xu et al. [18, 19], the trust infection rate, immunity loss rate, trust decay rate, and trust threshold were set as α=0.29, ω=0.002, β=0.02, and δ=0.7, respectively.

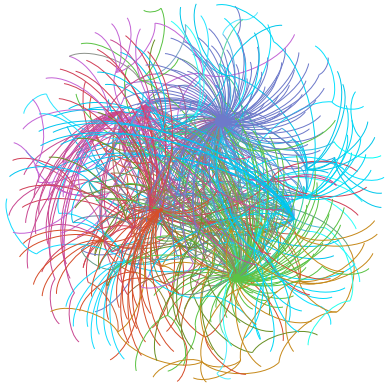

Figure 4. Original network diagram (Generation network diagram for one of the 20 experiments)

4.2 Comparison of Network Topological Features

The traditional trust network and the blockchain trust network are evolved with a time step of 500 on the original network with a scale of 500. The experiment was repeated 20 times. The resulting traditional trust network has an average of 958.5 nodes, 972.85 edges, and a network connectivity of 1.01. The obtained blockchain trust network has an average of 2069.35 nodes, 3367.05 edges, and a network connectivity of 1.63. Compared with the traditional network, the blockchain trust network saw its network scale increased by 115.89%, and network connectivity increased by 60.31%. These data show that, after the introduction of blockchain, it is easier for isolated nodes to establish trust connections to enter the network, thereby promoting the growth of the network. The nodes in the network establish more trust relationships and improve the trust connection degree of the network.

On the basis of Figure 4, the traditional network and the blockchain network evolved respectively, as shown in Figure 5 and Figure 6. It can be seen that the traditional network and the original network show the same community aggregation, but the nodes in the blockchain network nodes do behave like this. Thus, the blockchain trust mechanism breaks the trust barriers of acquaintance relationships and geographical relationships in the traditional network, but establishes a data-based trust relationship. In the blockchain trust network, the new node trust endorsement mechanism greatly improves the survival rate of new nodes. The trust transfer under the blockchain trust framework promotes the cooperation of network nodes. That is why the blockchain network is larger than the traditional network. According to Metcalfe's law, the blockchain network has better value than the traditional one. The following indices were chosen to compare the topology performance of different networks.

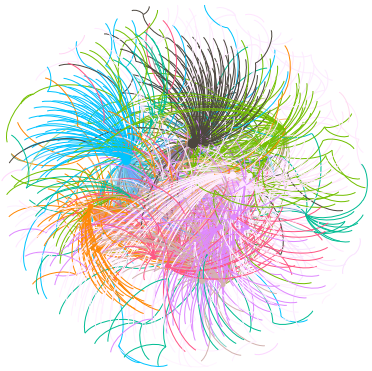

Figure 5. Evolution diagram of traditional network

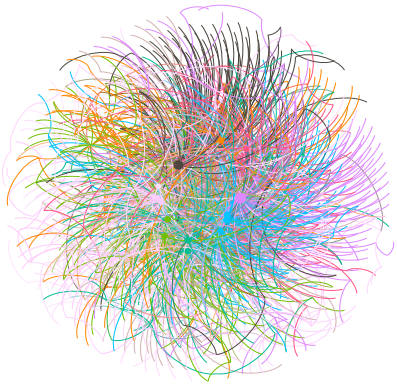

Figure 6. Evolution diagram of blockchain network

4.2.1 Average shortest path length

Figure 7 shows the average shortest path length of the two networks in the 20 experiments. Except for the eighth group of experimental data, the average shortest path length of the blockchain trust network was less than or equal to the traditional trust network, and the average shortest path of the traditional network was 3.05. The average shortest path of the blockchain network was 2.90. After the introduction of the blockchain, the average shortest path was reduced by 4.95%. The nodes in the network need to pass through the intermediary nodes to obtain the trust data of other nodes. The more intermediary nodes to pass through, the higher the cost of obtaining the trust data. Therefore, the smaller the average shortest path length, the higher the network efficiency. In the blockchain trust network, the willingness of nodes to find new trust partners was divided, which improves the efficiency of nodes to find partners. As a result, the network has more connections and shorter delivery paths. Different from the traditional agricultural supply chain that spreads trust through social networking, the blockchain trust propagation is anonymous and credible, safe and transparent, as well as traceable. This significantly improves the efficiency of trust spreading and establishment.

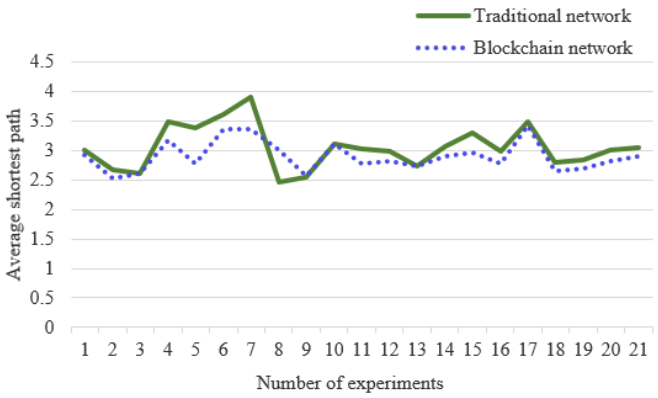

Figure 7. Average shortest path length

4.2.2 Degree distribution

Figure 8 presents the average degree distribution of the 20 experiments of the traditional trust network and the blockchain trust network. After the introduction of the decentralized blockchain evolution in the supply chain network, the network degree distribution still obeys the power-law distribution. The probability of nodes with a degree of 1 in the blockchain trust network is smaller than that of the traditional trust network. This means there are fewer edge nodes with only a single connection. The introduction of the blockchain trust tool helps the single-connected edge nodes to establish a new trust relationship. This result proves that small and medium-sized farmers who are on the edge of the agricultural supply chain can establish more trusting and cooperative relationships through the blockchain. The middle part of the scatter diagram represents the intermediate group in the supply chain network. In this group, the probability of the blockchain trust network is greater than that of the traditional trust network, a sign that the trust and cooperation in the network are more concentrated in the intermediate group, and the degree distribution declines by a smaller degree. Thus, the power-law distribution is more balanced, and such a network is more robust. At the tail of the scatterplot, that is, the large nodes in the network, the degree distribution probability amplitude of the blockchain network is smaller and the balance is better. Judging by network degree distribution, the blockchain trust network structure is more balanced and stable.

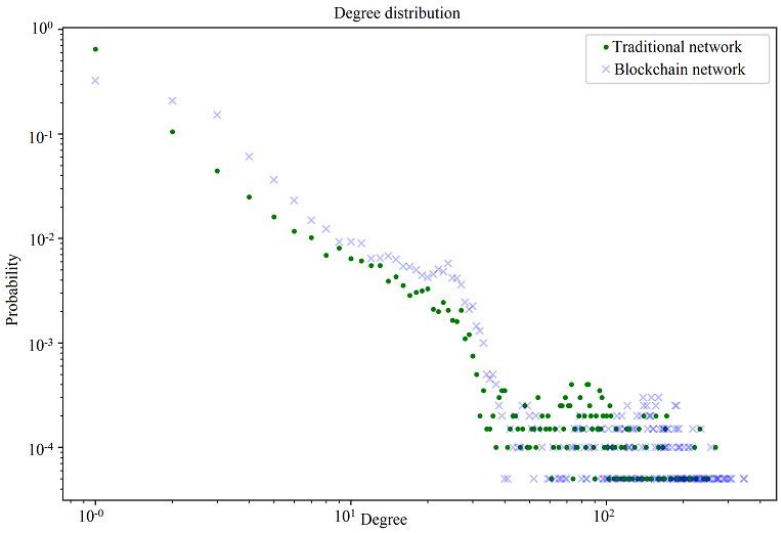

Figure 8. Degree distribution

4.2.3 Average clustering coefficient

Figure 9 shows the average clustering coefficient distribution of the 20 experiments of the traditional trust network and the blockchain trust network. In the lower range of the degrees, the average clustering coefficient of the blockchain trust network is larger than that of the traditional trust network. In the long tail range, there is not much difference between the two networks. A small clustering coefficient indicates a sparse subgraph, and a large clustering coefficient indicates a dense subgraph. In the dense subgraph, the trust data is richer, the information exchange is more frequent, and the activity is higher. In the blockchain trust network, the average clustering coefficient among small-scale farmers is greater than that in the traditional trust network, which improves the survival ability of small-scale farmers.

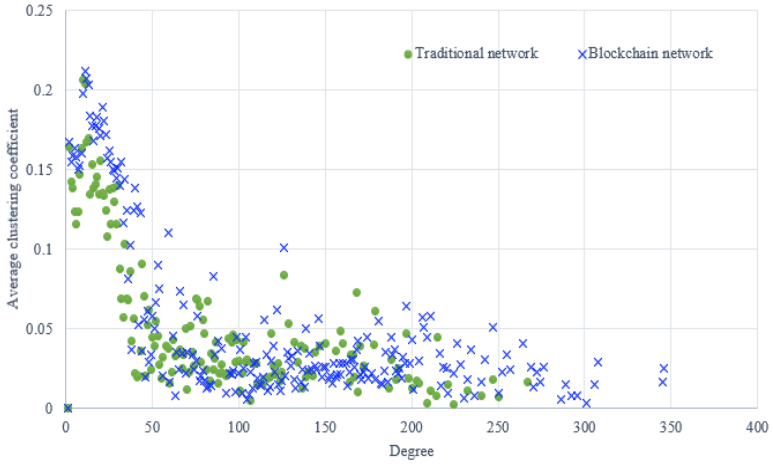

Figure 9. Average clustering coefficient

5. Conclusions

To reveal the topological structure and law of the supply chain trust network evolution via the gradual formation in the blockchain environment, this paper firstly establishes a scale-free supply chain network trust propagation evolution model based on the SIRS propagation model, which completely describes how the trust propagation in the supply chain network changes the network trust relationship. Next, the blockchain trust propagation mechanism is introduced into the model based on the blockchain consensus process, and the supply chain network trust propagation process is described under the blockchain. Finally, simulation experiments were carried out to compare the evolution trend and law of supply chain trust network and blockchain trust network. The simulation analysis shows that the blockchain trust mechanism deployed in the supply chain network has better network value, network efficiency, and topology performance than the traditional network. This confirms that the blockchain technology can improve the trust relationship of the supply chain network, and the introduction of the decentralized

blockchain does not affect the scale-free features. These findings are consistent with previous research. This paper takes a step further by studying the impact of blockchain on the supply chain network topology, and comparing the changes of topology indices under different degrees. As a result, it was verified that the blockchain can significantly improve the trust environment of non-core nodes in the network. Taking the agricultural supply chain as an example, the authors explained the changes of network topology indices, and the topological optimization encourages non-core nodes in the agricultural supply chain to actively apply blockchain technology to break through the trust dilemma.

In this paper, the trust threshold is set to a fixed value that is uniform for all nodes. In practice, however, the trust thresholds of different nodes are different, and the trust thresholds of nodes are time-varying. The evolution of the actual network will be better tracked by realizing this feature of adaptive nodes. Therefore, the future research can focus more on the influence of adaptive trust thresholds over network evolution, as well as the threshold setting mechanism in the blockchain environment.

Data Availability

The data used to support the findings of this research are available from the corresponding authors upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] A. Park and H. Li, "The effect of blockchain technology on supply chain sustainability performances," *Sustainability-Basel*., vol. 13, no. 4, pp. 1726-1726, 2021. https://doi.org/10.3390/su13041726.

[2] P. De Filippi, M. Mannan, and W. Reijers, "Blockchain as a confidence machine: The problem of trust & challenges of governance," *Technol Soc*., vol. 62, Article ID: 101284, 2020. https://doi.org/10.1016/j.techsoc.2020.101284.

[3] R. Jiang, Y. Kang, Y. Liu, Z. Liang, Y. Duan, Y. Sun, and J. Liu, "A trust transitivity model of small and medium-sized manufacturing enterprises under blockchain-based supply chain finance," *Int. J. Prod Econ*., vol. 247, Article ID: 108469, 2022. https://doi.org/10.1016/j.ijpe.2022.108469.

[4] Y. Wu and Y. Zhang, "An integrated framework for blockchain-enabled supply chain trust management towards smart manufacturing," *Adv. Eng Inform*., vol. 51, Article ID: 101522, 2022. https://doi.org/10.1016/j.aei.2021.101522.

[5] G. Zhao, Y. Yang, X. Bao, and Q. Peng, "On the topological properties of urban complex supply chain network of agricultural products in mainland China," *Transp. Lett. Int. J. Trans. Res.*, vol. 7, pp. 188-195, 2015. https://doi.org/10.1179/1942787515Y.0000000007.

[6] T. K. Agrawal, V. Kumar, R. Pal, L. Wang, and Y. Chen, "Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry," *Comput. Ind Eng*., vol. 154, Article ID: 107130, 2021. https://doi.org/10.1016/j.cie.2021.107130.

[7] S. Hu, S. Huang, J. Huang, and J. Su, "Blockchain and edge computing technology enabling organic agricultural supply chain: A framework solution to trust crisis," *Comput. Ind Eng*., vol. 153, Article ID: 107079, 2021. https://doi.org/10.1016/j.cie.2020.107079.

[8] J. Kang, Z. Xiong, D. Niyato, P. Wang, D. Ye, and D. I. Kim, "Incentivizing consensus propagation in proof-of-stake based consortium blockchain networks," *IEEE. Wirel Commun. Le*., vol. 8, no. 1, pp. 157-160, 2018. https://doi.org/10.1109/LWC.2018.2864758.

[9] H. Kou, F. Wang, C. Lv, Z. Dong, W. Huang, H. Wang, and Y. Liu, "Trust-based missing link prediction in signed social networks with privacy preservation," *Wirel Commun. Mob Com*., vol. 2020, pp. 1-10, 2020. https://doi.org/10.1155/2020/8849536.

[10] C. Xia, Z. Liu, Z. Q. Chen, and Z. Z. Yuan, "SIRS epidemic model with direct immunization on complex networks," *Cont Decis*., vol. 23, no. 4, pp. 468-468, 2008.

[11] F. Wang and L. Lin, "Spare parts supply chain network modeling based on a novel scale-free network and replenishment path optimization with Q learning," *Comput. Ind Eng*., vol. 157, Article ID: 107312, 2021. https://doi.org/10.1016/j.cie.2021.107312.

[12] H. F. Huo, P. Yang, and H. Xiang, "Dynamics for an SIRS epidemic model with infection age and relapse on a scale-free network," *J. Frankl Inst*., vol. 356, no. 13, pp. 7411-7443, 2019. https://doi.org/10.1016/j.jfranklin.2019.03.034.

[13] R. Urena, G. Kou, Y. Dong, F. Chiclana, and E. Herrera-Viedma, "A review on trust propagation and opinion dynamics in social networks and group decision making frameworks," *Inform Sciences*., vol. 478, pp. 461-475, 2019. https://doi.org/10.1016/j.ins.2018.11.037.

[14] Y. Hou, X. Wang, Y. J. Wu, and P. He, “How does the trust affect the topology of supply chain network and its resilience? An agent-based approach,” *Logist. Transport Rev*., vol. 116, pp. 229-241, 2018. https://doi.org/10.1016/j.tre.2018.07.001.
[15] Z. Wang, Z. Zheng, W. Jiang, and S. Tang, “Blockchain-enabled data sharing in supply chains: Model, operationalization, and tutorial,” *Prod. Oper Manag*., vol. 30, no. 7, pp. 1965-1985, 2021. https://doi.org/10.1111/poms.13356.
[16] W. Bi, H. Yang, and M. Zheng, “An accelerated method for message propagation in blockchain networks,” *Net. Int. Arc.*, vol. 2018, Article ID: 180900455, 2018. https://doi.org/10.48550/arXiv.1809.00455.
[17] Y. Zuo and Y. Kajikawa, "Toward a theory of industrial supply networks: A multi-level perspective via network analysis," *Entropy Switz*., vol. 19, no. 8, pp. 382-382, 2017. https://doi.org/10.3390/e19080382.
[18] E. J. Hearnshaw and M. M. Wilson, “A complex network approach to supply chain network theory,” *Int. J. Oper Prod. Man*., vol. 33, no. 4, pp. 442-469, 2013. https://doi.org/10.1108/01443571311307343.
[19] Y. Xu, Z. Gong, J. Y. L. Forrest, and E. Herrera-Viedma, “Trust propagation and trust network evaluation in social networks based on uncertainty theory," *Knowl-Based. Syst*., vol. 234, Article ID: 107610, 2021. https://doi.org/10.1016/j.knosys.2021.107610.