ISSN 2616-5902 Vol. 5, Issue 7: 78-86, DOI: 10.25236/AJBM.2023.050712

Exploring the Construction of a Social Credit System Based on Blockchain Technology and Digital Trust

Liu Zichan[1,a], Zhao Xincheng[2]

[1]School of Economic and Management, Guangzhou City Construction College, Guangzhou, China
[2]Department of Development Planning, Guangzhou City Construction College, Guangzhou, China
[a]277282469@qq.com

Abstract: *The degree of information transmission and trust are closely related, and in socio-economic activities, information transmission often faces difficulties such as fragmentation, distortion, inadequacy, and asymmetry. With the development of information technology, social relationships have been reconstructed, and traditional trust mechanisms based on acquaintances and institutional trust can no longer meet the transactional needs of socio-economic activities. Therefore, a new form of digital trust has emerged, with blockchain technology as an important foundation, which can construct more direct, efficient, and reliable trust relationships. The advantages of blockchain technology in information sharing, data authentication, and automated transactions are suitable for solving the difficulties of narrow credit data scope, poor timeliness, difficult aggregation, information silos, and unclear digital property rights in the construction of a social credit system. Based on this, a practical approach to the construction of a social credit system based on digital trust and blockchain technology is proposed.*

Keywords: *Trust; Blockchain; Digital trust; Social credit system*

1. Introduction

Trust plays a crucial role in social coordination and is the foundation of economic activities. Nobel laureate Kenneth J. Arrow once said, "almost all economic transactions involve trust. It can be said that the lack of mutual trust largely explains the backwardness of economies in most regions of the world." Zhang Weiying analyzed survey data from various provinces in China and concluded that trust is positively correlated with regional economic efficiency[1]. Trust is essential for economic prosperity as it reduces transaction costs, while lower levels of trust incur high transaction and monitoring costs. However, trust relationships are not built out of thin air and require significant resources to collect and analyze relevant information. People tend to maintain cooperation with partners with whom they have worked before, as this reduces the time and manpower cost of information collection.

Information can alter the degree of trust. If information is abundant, people can quickly make trust decisions based on the information they obtain. However, information scarcity creates uncertainty, which can lead to adverse selection and moral hazard. The widespread use of modern Internet technology enables people to freely and smoothly exchange information. Although information appears to be more abundant, the Internet eliminates the traditional fixed scenario for trading cooperation, and important identity information is concealed, resulting in significant uncertainty that makes it difficult to establish trust relationships. The development of information technology is causing unprecedented changes in information operation mechanisms, and trust mechanisms are gradually taking on new forms.

2. Difficulty in Establishing Trust due to Information Transmission

Establishing trust is a dynamic process of information interaction, and frequent and open information sharing and communication between parties can help build trust relationships. When dealing with unfamiliar transaction parties, there is no direct trust basis between them, and reaching a trade agreement requires sufficient information transmission between parties. However, there are many objective obstacles to obtaining and processing information. Firstly, information is fragmented and difficult to record. Evaluating whether a party is trustworthy requires comprehensive consideration of multiple dimensions, including their possible actions and potential risks. However, all the information related to a party is fragmented, and important soft information such as honesty, reputation, and values is difficult to quantify and evaluate. Secondly, it is difficult to discern the truthfulness of information. The information received by parties is always second-hand, and after passing through multiple layers of the market, it is difficult to reflect the true and accurate original state of events. Filtering and identifying information require high costs and can hinder the establishment of mutual trust relationships. Thirdly, there is information asymmetry between parties. The sources and channels of information obtained by parties differ greatly, resulting in significant differences in the quantity and quality of information obtained. Being in a disadvantaged position with regards to information can easily lead to moral risks and adverse selection.

The transmission of information between parties usually faces difficulties such as fragmentation and distortion, and their mutual information is often insufficient. Trust exhibits the following characteristics:

Firstly, trust is asymmetric. Parties obtain different quantities and qualities of information, and their evaluations and feedback on the same event are not the same, or even completely opposite. Therefore, the level of trust between them is asymmetric. Secondly, trust is domain-specific. Due to information fragmentation and difficulty in measurement, information sources and channels are limited. Perhaps limited by information costs, the information that can be obtained may be concentrated in a certain area. Parties can only establish trust relationships in a certain aspect where information is sufficient, and it is not trust in the entire domain. For example, the degree of trust in the opinions of an information technology expert on the field of information technology and on the field of finance would be different. Thirdly, trust can be transmitted. Information can flow, and trust naturally flows between different parties based on information flow between them. However, information transmission involves distortion and distortion, so the degree of trust will quickly decline as the transmission chain lengthens. Fourthly, trust is dynamic. Parties decide whether to trust each other based on the information they obtain, and they will also adjust the degree of trust in real time as the information they receive changes.

3. Evolution of Trust Mechanisms

3.1 Acquaintance-Based Trust Mechanism

In a society where people are familiar with each other, long-term interactions lead to mutual recognition and the formation of a common set of values, which in turn construct a stable social circle and norms of conduct. This results in mutual trust due to the familiarity between individuals. Traditional Chinese social trust was built on the basis of blood ties, geographical proximity, as well as long-term living and working contacts such as attending the same school or working at the same company. It was non-closed and expanded through social relationships, forming a relatively generalized network of personal relationships. Relationships built on this foundation have a high degree of elasticity and uncertainty, with the level of trust depending on the closeness of the relationship. Financial transactions in an acquaintance-based society tend to be based on trust, as once someone breaks trust, they can no longer operate within the social circle and lose their social activity space. In real life, people who are untrustworthy often flee and sever connections after their dishonesty is revealed.

This trust mechanism is strongly emotional, direct, and spontaneous, and is often referred to as "direct trust." The formation and maintenance of trust in an acquaintance-based society mainly rely on frequent and multidimensional interactions between acquaintances, including soft information that institutions find difficult to collect and quantify. The stable operation of Chinese private finance is based on the norms of acquaintance-based society. However, it is difficult to form high levels of direct trust between strangers who lack information interaction, making it challenging to achieve mutually satisfactory transactions. Additionally, compared to the vast trading market, the scope of acquaintance-based society is limited. Furthermore, it is challenging to establish and maintain a high level of trust with strangers on a low foundation of acquaintance-based trust[2]. As the relationship chain lengthens, the level of trust rapidly decreases. It is difficult to expand the trust required for transactional cooperation through these relationships, making it easy to encounter scale bottlenecks that hinder operation. The development of private finance often starts with rapid growth and prosperity, but then collapses suddenly.

3.2 Institutional Trust Mechanism

With the continuous development of global information technology and social division of labor, various interactions and cooperation occur between people across time and space, making trust between the parties in transactions extremely important. However, there is no process for long-term acquaintance and understanding of each other's character among strangers, and there is a lack of direct trust basis and effective information interaction. If self-information collection, screening, and analysis are used, the cost

ISSN 2616-5902 Vol. 5, Issue 7: 78-86, DOI: 10.25236/AJBM.2023.050712

is often high and lacks timeliness. The development of the Western market economy has promoted the construction of a trusted medium for information exchange and sharing, which reduces the adverse selection and moral risks caused by information asymmetry through third-party authentication, third-party guarantees, credit ratings, etc., and is supplemented by contractual and legal elements for supervision and implementation, ensuring the smooth progress of transaction cooperation. Based on the deterrent effect of contracts and laws, third-party institutions become trusted intermediaries to achieve indirect trust, promoting effective operation of modern economic activities among unfamiliar entities and establishing a set of effective institutional trust mechanisms.

In modern financial transactions under the operation of institutional trust mechanisms, banks have become intermediaries for financial transactions, establishing close relationships with both suppliers and demanders of funds. In the long-term interaction, they store massive data information and gradually obtain a central position in financial information. Banks then use this information advantage to manage and control risks, reduce adverse selection and moral risks, gradually become the credit consensus of financial activities, and develop into the most credible institutions for financial transactions, led by centralized credit institutions with the endorsement of national credit.

3.3 Digital Trust Mechanism

In 2008, the US subprime mortgage crisis led to the global financial crisis, exposing problems such as profit-seeking financial institutions, missing financial regulation, distorted credit ratings, and bank credit bubbles. The bank-dominated centralized trust mechanism faced serious challenges. The third party designed by the institutional trust mechanism was originally intended to reduce information asymmetry and play a role in trust guarantee, but gradually evolved into an information opaque center. With the progress of information technology, the digital economy has gradually prospered, and direct trust relationships between two or more parties have been established based on objective technical and computational systems.

As social activities become digitized, the generation of human social relationships is described, expressed, and constructed through information and data, creating a different kind of digital trust[3]. Digital trust is the reconstruction of interpersonal trust and system trust by digital technology and is the result of "trust transfer" between interpersonal trust, system trust, and trust channels[4]. Digital trust enables trust relationship subjects to shift from trust between people, trust in organizational systems to trust in technology. Trust relationships established based on technology can avoid subjective biases caused by human factors, and rely more on transparent first-hand information instead of receiving second-hand information, effectively reducing the risk of trustors and increasing trustworthiness[5].

The birth of blockchain technology makes it possible to build digital trust. In 2015, The Economist published a cover article comparing blockchain to a "trust machine." The blockchain technology, which integrates achievements in cryptography, mathematics, economics, network science, and other fields, has created a technology-based digital trust. Transaction parties no longer rely on third-party financial institutions such as banks, but instead achieve peer-to-peer transactions in a distributed system through decentralization, timestamps, data encryption, and economic incentives, forming a node trust mechanism. Blockchain can be seen as an open, distributed, and trusted database system where the transaction process is jointly created by different nodes, and the data information is immutable, undeletable, and traceable. The data information is shared and maintained by all parties involved, even if they are strangers to each other, they can still conduct transactions based on technical trust.

4. Challenges in Building a Social Credit System

The social credit system is an important part of the socialist market economy and social governance system, and trust is the cornerstone of social credit. With the advancement of digital technology, social credit systems based on personal trust and institutional trust have been challenged and exposed some drawbacks. The role of social and economic interactions and credit governance is gradually weakening and is difficult to adapt to social development. Emerging technologies are promoting economic development and entering the digital age, but China's existing credit data is scattered across various government departments, industry associations, and commercial institutions, and information construction is not interconnected. The construction of the social credit system mainly faces the following challenges:

ISSN 2616-5902 Vol. 5, Issue 7: 78-86, DOI: 10.25236/AJBM.2023.050712

4.1 Narrow scope of credit data, poor timeliness, and difficult collection

The credit information collected in traditional social credit system construction is mainly concentrated in loan information and compliance with laws and regulations, with a single data dimension. Negative credit information is mainly focused on punishing dishonesty, while positive information is relatively scarce, lacking incentives for honesty. Credit information is updated by each institution according to the prescribed time, leading to poor timeliness and lagging information. Raw data is not easily collected into useful information. On the one hand, data standards are not uniform, and data redundancy leads to low data quality and low utilization value. On the other hand, credit information itself is a network relationship, and the effective use of information requires the association of various types of data. However, data information lacks key fields.

4.2 "Information island" caused by data barriers

Data has gradually become an important asset of various institutional departments, and data competition and protection systems are becoming a new "barrier." Data only applies within the vertical system of each institution and is not open to the outside world, nor is it integrated and shared, and data resources are divided into information islands. This barrier mainly reflects inconsistent data collection standards, formats, and architectures, incompatible system designs, and difficult coordination of work and operation mechanisms involving multiple institutions.

4.3 Unclear data property rights hinder data circulation

The establishment of a credit market system needs to follow economic laws, and clear property rights are a prerequisite for the effective operation of the market economy. Currently, the rights of data ownership, usage, operation, and property have not formed a systematic data right binding. Institutions collect, analyze, and use personal identity and behavioral data of relevant users in actual operations, and even use and process data for profit. However, these data are closely linked to specific individuals, and the use and dissemination of data will inevitably lead to the disclosure of sensitive personal information, infringing on individuals' privacy. China's existing laws lack regulations on data property rights, and issues such as ownership of data information are blurred in practice, leading to controversies in information transactions and prominent problems such as user privacy violations, which hinder data sharing and transactions. As a critical element of the digital economy, the zero-cost replication and traceability difficulty of data also lead to the unsmooth trading and sharing of credit information[6]. Only when property rights are clearly defined, responsibilities are clear, and protection is strict, can data be shared and circulated.

5. Technical Basis and Characteristics of Blockchain

5.1 Data Structure and Anti-Tampering

First, anti-tampering of transactions. Each transaction in the blockchain is encrypted with a private key and can only enter the data pool and wait to be added to the blockchain after being verified by nodes. The reliability of data is determined by the encryption algorithm. Second, anti-tampering of blocks. Each transaction in a block is calculated using a hash function to generate a hash value. The hash values are then calculated pairwise, layer by layer, until a root hash of a Merkle tree is obtained and placed in the block header. Modification of the underlying data will cause a change in the root hash, which can be used to verify the correctness of the data storage. Third, anti-tampering of the blockchain. Each block in the blockchain contains the hash value of the previous block, forming a chain structure. Blocks are contested by a node for the right to bookkeeping, and are broadcast to other nodes for verification before they can be added to the blockchain, ensuring the correctness of the accounting data.

When data in a block is modified, the hash value changes, causing all subsequent blocks connected to it to also change their previous block hash values. To tamper with the data, all nodes must participate in the accounting process again and agree to modify the information in at least half of the nodes. However, nodes are typically controlled by different entities, making it extremely difficult to tamper with data in the blockchain. Based on these technical features, the hash value changes when the data content is tampered with, making it easy for the system to recognize during hash value verification. Therefore, the true reliability of blockchain data information can be effectively guaranteed, and trust relationships can be established between unfamiliar entities without the need for a third party.

ISSN 2616-5902 Vol. 5, Issue 7: 78-86, DOI: 10.25236/AJBM.2023.050712

5.2 Distributed Ledger Ensures Data Security

The servers in the blockchain network are called nodes, which provide storage space and computational support for the entire blockchain. The blockchain is a distributed database system that is participated in and maintained by nodes distributed in different locations. When a node in the blockchain adds a new block, each node will update the data in real-time. Dispersed nodes have complete records, thus avoiding the possibility of centralized single bookkeeping being controlled and falsified. A large number of nodes ensure the security of the data, and the ability to restore data is also stronger.

5.3 Asymmetric Encryption Provides Secure Identity Verification

Asymmetric encryption algorithm is the basis of the information verification mechanism in the blockchain system. The characteristic of the asymmetric encryption algorithm is that it simultaneously generates a pair of matching keys, one for encrypting files and the other for decrypting. The generated keys are generally divided into public keys and private keys, the former of which can be made public to relevant entities, while the latter must be carefully guarded. The information sent is usually encrypted with a private key, and the recipient uses the corresponding public key to decrypt it. Data encrypted with a hash algorithm generates a unique digital digest, and even if one number is changed, the data information will change completely. By comparing the digital digest, the integrity of the information can be directly confirmed, and the authenticity of identity information can be authenticated. In addition, the digital digest of asymmetric encryption cannot be deduced to the original data information, ensuring the security of identity data information.

In addition, the use of non-simultaneous encryption technology in blockchain, also known as digital signature, solves problems such as forgery, impersonation, denial, and tampering, similar to traditional seals and signatures. Transaction information stored on the blockchain is public, and anyone can query relevant data through public interfaces, while account identity information is highly encrypted. The digital signature mechanism ensures data security and personal privacy, and each data node in the blockchain can ensure the integrity of the queried data, improving the stability of the entire database.

5.4 Smart contracts have irreversible binding force.

Smart contracts are digital agreements that are defined and negotiated based on machine algorithms with predefined rules and terms, which are automatically executed without the intervention of third parties. First, smart contracts can effectively avoid central fraud and loss of control in institutional trust mechanisms without the presence of third parties. Secondly, smart contracts are based on standards and protocols that are agreed upon by all nodes, and are open, transparent, and visible. Thirdly, once triggered, smart contracts that are automatically executed are highly resistant to modification and have a high degree of readiness. Finally, smart contracts reduce the supervisory and coordination costs of managers and increase work efficiency. The above characteristics of smart contracts, which mitigate contract and operational risks, ensure the enforcement of transaction execution, not only benefit the credibility of data but also contribute to the establishment of a social credit system.

5.5 Timestamps provide data traceability protection

In the blockchain system, every new block generated is automatically loaded with a timestamp. The application of timestamp technology ensures that data is difficult to tamper with and can help locate and trace data. If the blockchain is a ledger, then a block is equivalent to a page in a ledger, and a timestamp is similar to the specific time recorded in the ledger. Each page in the ledger is connected in chronological order to form a decentralized distributed timestamp ledger. When a block is generated, the timestamp server automatically loads the time information, providing strong evidence of traceability for the existence or occurrence of data, ensuring the authenticity, integrity, and verifiability of data information. Timestamps increase the difficulty of changing records exponentially, and if data tampering is to occur, all subsequent blocks must be modified, which requires almost impossible resources to consume. Therefore, the older the data, the harder it is to tamper with. In addition, data traceability solves the important issue of ownership of data rights and interests, which is an important guarantee for realizing value sharing and fair distribution of interests.

ISSN 2616-5902 Vol. 5, Issue 7: 78-86, DOI: 10.25236/AJBM.2023.050712

5.6 Different types of blockchains construct basic ecosystems

Blockchain is divided into three types: public chain, alliance chain, and private chain. The public chain allows any node to freely join and exit the network without identity verification and has the widest application range. The alliance chain is created jointly by several institutions, is between the public chain and the private chain, and only allows authorized nodes to join the network. The alliance chain is maintained collectively by alliance members who formulate reading and writing permissions and accounting rules. The private chain is not publicly available, all nodes are held by the same institution, and only that institution has read and write permissions. The private chain has fewer nodes and a higher degree of privacy, with faster information transaction speeds. It is generally used for internal data management of companies that value data privacy. The alliance chain and the private chain are known as permissioned chains because they require authorization, while the public chain is known as an unpermissioned chain. Sidechains do not belong to the above-defined types of blockchains. Sidechains are like branches of the main road, connecting different blockchains to transfer digital assets between different blockchains and achieve interaction. Sidechains are independent of the main chain and can extend different functions, such as smart contracts and privacy, without affecting the performance of the main chain. On the other hand, sidechains can alleviate the burden of excessive data expansion on the main chain and improve transaction speed. In practical applications, public chains, alliance chains, and private chains each have their advantages and disadvantages. Organizational groups have different needs for privacy, security, and speed in different scenarios. Connecting different types of blockchains through cross-chain technology can construct a fully functional, cooperative, and communicative blockchain ecosystem.

6. Feasibility of Building a Digital Trust Mechanism Based on Blockchain Technology

In the era of the digital economy, information transmission and value transfer are closely intertwined. Blockchain provides an efficient and secure system for recording and transmitting information that can carry value movement[7]. Therefore, blockchain technology disrupts traditional trust mechanisms based on familiar social trust and institutional trust, and constructs more direct, efficient, and reliable trust relationships.

6.1 Technology maintains information authenticity and directly generates credit

Throughout the entire process of data information storage and transmission, the blockchain system utilizes a series of technical integrations such as block data structure design, distributed storage, and asymmetric encryption technology to prevent data from being tampered with and ensure data authenticity. Unlike third-party institutions designed based on institutional credibility, which authorize credit through information collection, processing, and issuing notarized documents, information on the blockchain can directly generate credit because it is authentic.

6.2 Data sharing reduces costs and quickly establishes trust relationships

In traditional society, secondary information transmission is the main way, and secondary information often has the defect of being difficult to distinguish between true and false. In addition, third-party institutions in institutional trust mechanisms generally have information monopolies, and information content collection is limited. If you want to establish a trust relationship, you need to involve many intermediaries, and the business process is too long, causing low collaborative efficiency. The high cost of establishing trust will also hinder the achievement of transaction cooperation. Blockchain technology realizes synchronous sharing of data information, and even direct information transmission between peers can be established without third-party involvement, constructing a network-centered multi-dimensional transmission. It not only avoids the falsification of third-party data but also achieves fast, lossless, and diversified information transmission. Moreover, smart contracts can achieve automated operation and management. Dependence on blockchain technology can effectively reduce time and cost for establishing trust relationships between unfamiliar entities, and improve overall operational efficiency. Trust is a dynamic process, and real-time, open, and frequent information sharing and communication between entities can promote and consolidate trust relationships.

ISSN 2616-5902 Vol. 5, Issue 7: 78-86, DOI: 10.25236/AJBM.2023.050712

6.3 Clarify data ownership and promote direct trust through information flow

One reason for the problem of information islands caused by the inability of institutions to share data is that data ownership is not clear, and each institution has no motivation to share data due to consideration of data information security and confidentiality. Blockchain can use encryption technology for digital asset signatures to determine ownership of digital assets and establish open permissions for information transactions through technology. The blockchain stores complete information flow records, and data can be traced back using its traceability technology, thereby realizing data ownership. Clarifying data ownership is a prerequisite for credit information to fully flow as a digital asset, and on this basis, maintaining the interests of all parties and participating in data sharing construction together.

On the other hand, after the information rights and obligations on the blockchain are clarified, information can flow independently of the entity. Based on blockchain technology, information can flow without time and space restrictions, and trust relationships can also be built across time and space. For example, the cooperation chain of trade is very long, involving many links such as production, logistics, and sales, and collaboration and transmission face many difficulties. Information can flow directly between various entities to generate trust, greatly improving corporate collaboration efficiency.

7. Thoughts on the Construction of Social Credit System under the Digital Trust Mechanism

With the development of the digital economy, the traditional acquaintance-based social credit and industrial economy-based contractual credit are gradually evolving into a system-based credit with digital technology as the foundation. The advantages of blockchain technology in information sharing, data rights confirmation, and automated transactions have been widely recognized. Its ability to solve problems coincides with the pain points of the social credit system, meeting the development needs of current social trust relationships. Therefore, it has attracted increasing interest from scholars both domestically and abroad, and it is widely agreed that its technological innovation in the trust mechanism can contribute to the sound operation of the socio-economic system. The digital trust mechanism provides a foundation for the construction of a new social credit system, but specific mechanisms and theoretical discussions are still in the early stages. Based on previous research, the following applications for constructing a new social credit system are proposed:

7.1 Building a fully functional digital network

Establish a public chain to record the basic information of social behavior subjects for identity verification, which is maintained by the state. Institutions involved in credit data collection and management establish a permissioned consortium chain based on a set of consensus mechanisms, relying on blockchain technology to build an information-sharing framework and construct a social credit system information data sharing platform. As nodes, each institution realizes secure, transparent, and efficient data flow in a controllable manner, effectively solving the current problem of information islands. Each node of the consortium chain establishes a private chain to record credit information data, ensuring the independence and security of credit resources. Each node is only responsible for recording and maintaining the information data within its own authority and cannot modify the content of other nodes. The database is updated in real-time to ensure the timeliness of credit information on the chain. Through sidechain technology and cross-chain technology, multiple chains are integrated and interact with each other to build a fully functional digital network for the social credit system.

7.2 Nodes record data and generate digital digests as information indexes

The characteristics of the distributed ledger of blockchain can surpass regional limitations and link and share credit data provided by widely distributed nodes. Each node formulates unified and standardized data collection standards, and the validity of data is verified through consensus before being entered into the node database. Institutions generate digital digests through asymmetric encryption as information indexes for specific credit information from their own databases, publish them, and broadcast them throughout the consortium chain. Other nodes verify and synchronize the updated information. Through the information traceability mechanism, a set of laws and regulations are established to ensure that information providers bear real and effective legal responsibilities for information resources.

ISSN 2616-5902 Vol. 5, Issue 7: 78-86, DOI: 10.25236/AJBM.2023.050712

7.3 Data Authorization Query

The demander of credit information needs to first verify their identity through the public chain and obtain authorization from the party being queried before submitting a query application to the nodes on the alliance chain. The digital digest of credit data is centralized on the alliance chain, where each node serves as both a provider and a querier of the data. When a query application is received, the alliance chain node first queries the digest information of its own node, then uses smart contracts to achieve digest information retrieval and automated queries, and returns the query results. If a match is found with the digest information, the node cannot directly access the specific credit information, but can only obtain the address of the index information and send a data query request to the data provider. After receiving the request, the data provider provides decryption permission for the authorized information. Finally, this query generates a transaction summary record chain on the platform[8].

7.4 Sound Incentive Mechanism

In addition to the support of blockchain technology, the construction of a social credit system also requires a set of incentive mechanisms to stimulate information owners to participate in the construction and sharing. In the design concept of blockchain technology, participating nodes in new blocks are rewarded, and transaction fees are also introduced as rewards. On the one hand, the more nodes participate, the more stable the system's security; on the other hand, fair economic incentives can maintain the normal operation and expansion of the blockchain ecosystem.

8. Problems and Risks of Blockchain Technology in Application

Blockchain technology can effectively avoid irrational intervention of human social variables, thereby simplifying social interaction mechanisms and improving social operational efficiency. However, as a whole, blockchain technology is still in the development stage, and there are still many problems and potential risks that need to be addressed in order to fully utilize its positive effects.

8.1 The authenticity of original information needs improved system design guarantees.

The blockchain storing the social credit system is an encrypted digital digest, not the actual data of the database, and the original data is still stored on the local server[9]. Although the on-chain data is difficult to tamper with, it can verify the integrity of the original data. However, if the original data before being put on the chain is forged or has already been tampered with, ensuring data reliability on the blockchain becomes meaningless, and instead endorses distorted data, which affects the credibility of the entire social credit system. In certain application scenarios, automatic identification, transaction verification, and transaction management of devices can be initiated through underlying IoT, and data collection and information processing can be guaranteed through smart contracts under unmanned intervention. However, the application scenarios of IoT and smart contracts are limited, especially in the early stages of development, and require improved system design, effective supervision, and legal regulations to regulate the behavior of all participating institutions.

8.2 Blockchain operations need to be expanded and accelerated.

In a distributed network lacking mutual trust, the design of the blockchain system focuses on data reliability and consistent updating, sacrificing transaction response performance. On the one hand, the design of the blockchain data structure, encryption, verification, and transmission are all relatively cumbersome, and the computational and storage burden is very heavy. On the other hand, all generated blocks are indiscriminately broadcasted to the entire network, resulting in high redundancy of transmission. Moreover, in order to ensure data consistency, all nodes need to perform complex verification before confirming data on the chain. The complex data structure of the blockchain and the repetitive verification to prevent tampering ensure the credibility of the data, but the low storage and transaction processing rate is the bottleneck for the promotion of its application scenarios. As blockchain develops, data storage will only increase rapidly, and corresponding storage computation will become increasingly significant. Blockchain expansion and acceleration is an important issue in current blockchain technology. The proposal and in-depth research of simple verification, side chains, lightning network protocols, and cross-chain technologies are providing possible solutions to the aforementioned problems.

ISSN 2616-5902 Vol. 5, Issue 7: 78-86, DOI: 10.25236/AJBM.2023.050712

9. Conclusions

The evolution of social trust has experienced a transition from trust in acquaintances to trust in institutions, and now to digital trust that seeks to leverage digital information technology. Blockchain technology, with its tamper-resistant distributed ledger features, has developed a digital trust mechanism that operates more efficiently, compensates for human and institutional deficiencies, and promotes the reconstruction of social credit systems. The innovation of digital trust mechanisms has also promoted the reconstruction of the social credit system, enriched the dimension of credit information, empowered social and economic development, and promoted the continuous innovation of credit services and application scenarios in the fields of housing rental, transportation, tourism, healthcare, and other social production and living areas, providing more convenient and high-quality services. However, behind digitization, destructive problems such as fraud, cheating, and attacks may also emerge. The ultimate goal of digital trust development is not to replace trust in acquaintances and trust in institutions, but to form a contemporary social trust system together. Digital information technology promotes the expansion of interpersonal relationships and makes institutional trust more reliable. The large-scale promotion of digitization advances social and technological progress, solves people's work and life problems, and also brings new problems. The forward-looking research of digital trust still has a long way to go.

Acknowledgments

This project is supported by Guangdong Province Youth Innovation Talent Project for Ordinary Colleges and Universities "Research on the Construction of Credit System for Small and Medium-sized Enterprises Based on Blockchain Technology" (Fund No. 2020WQNCX244), Guangdong Provincial Ordinary University Innovation Team Project "Cloud Accounting Big Data Intelligent Innovation Team" (Fund No. 2018GWCXTD002), Guangzhou Science and Technology Plan Project 'Research on Supply Chain Finance Risk Management Application Based on Blockchain Technology' (Fund No. 202201011685).

References

[1] Zhang W. Y., & Ke, R. Z. (2002). Trust and its explanation: An analysis of inter-provincial survey data from China. Economic Research, (10), 59-70+96.

[2] Zhang Z. (2022). Characteristics and Construction Path of Interpersonal Trust in Contemporary Chinese Society: An Empirical Study Based on the Seventh Wave of WVS Data. Zhejiang Social Sciences, (02), 59-69+157.

[3] Gong X. H. (2021). Human "Digital Attributes" and Their Legal Protection. Journal of East China University of Political Science and Law, 24(03), 71-81.

[4] Wu X. H. (2020). Digital Trust and the Reconstruction of Digital Social Trust. Learning and Practice, (10), 87-96.

[5] Xu Y. H., & Wu S. Q. (2022). Research on the Construction Mechanism of Blockchain Technology and Digital Trust: Taking Baidu Super Chain as an Example. Nanjing Social Sciences, No. 419(09), 55-64.

[6] Qin X. Y., Shen C., Chen G., et al. (2020). Construction of Internet Credit System Framework Based on Blockchain Technology. Credit Reference, 38(02), 12-17.

[7] Wang G. T., & Zhang Y. (2018). Discussion on the Credit System Embedded in the Blockchain Era. Credit Reference, 36(09), 13-17.

[8] Guo S. X., & Song Z. Q. (2018). Research and Application of Blockchain Mode Design for Credit Reference. Journal of Network and Information Security, 4(04), 63-71.

[9] Chen F., & Cai Z. (2020). The construction of social trust in the socialization of blockchain technology and social adjustment. Scientific Outlook, 38(12), 2124-2130.