Legal Issues Regarding Financial Data Security and Privacy Protection under Blockchain Technology

Manning Wang[1,a,*], Jiayi Zhu[1,b]

[1]University of Sanya, Sanya, China
[a]1928505556@qq.com, [b]739314551@qq.com
**Corresponding author*

Abstract: *With the advent of the digital era, and the Widespread Application of Blockchain Technology in the Financial Industry, financial data has become a crucial asset. However, financial data security and privacy have consistently been a societal concern. The emergence of blockchain technology provides a new solution for the security and privacy of financial data. This article starts by examining the role of blockchain technology in ensuring the security and privacy of financial data. It then explores the legal issues associated with financial data security and privacy protection under blockchain technology, offering corresponding recommendations.*

Keywords: *Blockchain Technology; Legal Issues; Data Security; Privacy Protection*

1. Introduction

In recent years, with the rapid development of technologies such as the internet and mobile internet, the digital economy has become a significant driver of economic growth. In the era of the digital economy, financial data has emerged as one of the most crucial assets, encompassing sensitive information such as personal identities, financial records, and credit ratings. However, concerns over the security and privacy of financial data have consistently been a focus of societal attention.

Liu, F.J.[1](2019), introduces the application of blockchain technology in the financial field, and also raises concerns about privacy protection. Block chain of openness and tamper-proof may lead to storage on the block chain transactions and personal information is easy to be accessed by the public, which causes the user's privacy concerns and put forward some possible solutions or Suggestions, to solve the block chain technology in the field of finance, and in the introduction of encryption algorithm, authentication mechanism, anonymity technology, etc., in order to improve the user's privacy protection level.Zhang Fei.[5](2017)analyzes the legal problems and challenges faced by the blockchain technology in the financial field. For example, there may be legal uncertainties and disputes in data privacy protection, legality of smart contract execution, digital assets supervision, etc., and the limitations and impacts of these issues on the application of blockchain technology in the financial industry are discussed.

Li Haoran.[2](2020),The importance of financial data security is discussed, especially in the digital age, where financial institutions are facing the threat of increasing data breaches and cyber attacks. These security threats can lead to financial loss and credibility damage for financial institutions and customers. Discuss the potential of blockchain technology for financial data security, such as improving data integrity, traceability, and resilience to tampering. It may also point to the challenges of blockchain technology in terms of scalability, performance, and legal compliance.

Jia Zhixiong.[3](2018),. It studies the legal provisions of financial data privacy protection under blockchain technology, emphasizing the importance of financial data privacy protection in the era of digital economy. This paper analyzes how the characteristics of blockchain may conflict with the traditional legal framework of privacy protection, such as personal information protection law and data protection law, and explores how to balance the relationship between the advantages of blockchain technology and the legal protection of financial data privacy.

Li Jianhua.[4] (2021),summarizes the application of blockchain technology in the financial field, introduces the practical application cases of blockchain technology in financial transactions, asset management, payment and settlement and other aspects, and points out that although blockchain technology has great potential in the financial field, the appropriate legal environment and regulatory mechanism still need to be further improved. The authors analyze the future trends, emphasizing that the interaction of technology and law will be the key to promoting the application of blockchain in the financial sector.

Cachin, C. (2016), for instance, introduced the design principles and components of the Hyperledger blockchain architecture, including consensus algorithms, identity verification, and access control mechanisms. The author proposed that Hyperledger provides a customizable and scalable blockchain platform suitable for financial data security and privacy protection. Meanwhile, studies by Hu Xiaoyan.[8] (2022) focused on the application of blockchain technology in securing financial data, using digital currencies as examples. The research explored the role of blockchain in protecting transaction records and individual privacy.

Additionally, Xu, X.[6] (2017), investigated attacks on decentralized consensus protocols, categorizing attack types such as double-spending and 51% attacks, along with corresponding defense measures. The study emphasized the need for appropriate protocol design and security mechanisms to ensure the security of financial data. T. T. A. Dinh [7](2018), analyzed the structure and functions of blockchain systems from a data processing perspective, highlighting challenges related to scalability and privacy protection. Lu Y.M.[9] (2021) reviewed the research progress in financial privacy protection based on blockchain technology, including the application and development direction of encryption techniques and zero-knowledge proofs.

Maesa, D. D. (2019), introduced the use of symbolic execution and attribute-based testing methods for the security verification of smart contracts, covering smart contract vulnerability classifications and verification technologies. These verification methods can help discover and prevent security issues in smart contracts, thereby enhancing the security of financial data.

From the literature review, it is evident that traditional methods of storing financial data face various issues, including susceptibility to attacks, tampering, and loss. The emergence of blockchain technology provides a new solution for the security and privacy of financial data. However, under blockchain technology, the legal issues surrounding the security and privacy protection of financial data become increasingly complex. This paper will explore the legal issues faced by financial data security and privacy protection under blockchain technology, starting from the role of blockchain technology in these domains, and will propose corresponding recommendations.

2. The Role of Blockchain Technology in Financial Data Security and Privacy Protection

Blockchain technology, as a distributed ledger technology, possesses characteristics such as decentralization, immutability, and anonymity, making it an ideal choice for safeguarding financial data security and privacy.

Firstly, the decentralized nature of blockchain technology effectively prevents data tampering. Traditional methods of financial data storage face a single point of failure issue, where an attack or tampering of the central server could compromise data security. Blockchain technology is a decentralized distributed database, where the data is no longer managed by a single central organization. By storing the data on multiple nodes, the attacker is unable to modify the data, so as to ensure the security of the data.

Secondly, the immutability feature of blockchain technology protects the integrity of data. In blockchain, each block contains the hash value of the previous block, forming an immutable chain. This ensures the integrity of financial data, guaranteeing its trustworthiness and authenticity.

Thirdly, Smart contracts: Blockchain technology can support smart contracts, an automated contract that can be defined and implemented in a programming language. Smart contracts can be used in financial transactions, asset management and other scenarios, which can improve the efficiency and security of transactions, but also protect the privacy of data.

Lastly, the anonymity feature of blockchain technology helps protect user privacy. Under traditional financial data storage methods, personal information is susceptible to leaks. In blockchain technology, users can use public and private keys for identity verification, enhancing user privacy.

3. Legal Issues in Financial Data Security and Privacy Protection under Blockchain Technology

Despite the significant impact of blockchain technology on financial data security and privacy protection, practical applications raise certain legal issues.

Firstly, the anonymity provided by blockchain technology may be exploited for illegal activities. Unlike traditional financial data storage, where authorities can trace user identities through banks, the anonymity of users in blockchain makes monitoring and tracking difficult.

Secondly, the decentralization feature of blockchain technology might lead to disputes. Traditional legal means can resolve disputes in traditional financial data storage, but in blockchain, the absence of a central server poses challenges in resolving conflicts.

Lastly, the immutability feature of blockchain technology presents legal challenges. Incorrectly recorded data on the blockchain is challenging to modify or delete, potentially questioning the legitimacy of certain data and leading to disputes.

4. Case Analysis

4.1. Data Ownership Issue:

The decentralized and distributed nature of blockchain technology creates ambiguity in data ownership, making it challenging to define data rights. Traditional financial institutions typically store customer data centrally in their databases, allowing for management and control. However, in blockchain technology, data is dispersed across various nodes in the network, complicating data ownership.

Specifically, the data ownership issue under blockchain technology involves the following aspects:

- Data Ownership: In blockchain technology, data can be simultaneously owned and used by multiple participants, leading to fuzzy boundaries in data ownership. In the financial sector, this ambiguity may result in disputes, such as data leaks or misuse.

- Data Access Permissions: Due to the decentralized nature of blockchain, anyone can access and view data on the public chain. Ensuring that only legitimate users can access sensitive data becomes a challenge.

- Legal Responsibility: In blockchain technology, due to the decentralized storage and sharing of data, determining the source and processing path of data becomes difficult. This complexity may make it challenging to hold financial institutions accountable for issues like data leaks or misuse.

In the context of blockchain technology, Bitcoin serves as an early application. In Bitcoin transactions, participants can engage in anonymous transactions, raising concerns about data privacy and security. For instance, individuals may use Bitcoin for illegal activities like money laundering and smuggling, posing challenges in determining the true owners of these transactions. Financial institutions may need to cooperate with relevant authorities to investigate such issues, but the unique characteristics of blockchain technology may involve challenges related to data privacy and ownership.

4.2. Dispute Resolution Mechanism Issue:

Due to the immutability of blockchain technology, resolving disputes becomes a challenge. Two primary solutions currently exist for this issue. The first involves using legally specified mediation and arbitration methods to resolve disputes. This approach is suitable for countries or regions with strong legal constraints, and agreements can include provisions specifying the use of these methods to resolve disputes. For example, the U.S. has recognized "smart contract" technology in its legal framework, facilitating the audit of applicant qualifications and the discovery of issues in the transfer process.In addition, the distributed storage and decentralized nature of blockchain technology make bitcoin data easy to be tampered with, but also make bitcoin data not easy to be managed and controlled. Secondly, because the blockchain data of Bitcoin is distributed, the security of Bitcoin data is also facing certain challenges, such as the security of Bitcoin nodes, the fork of Bitcoin blockchain and other issues.

The second solution involves community governance, where community members collectively resolve disputes. This approach is applicable in decentralized scenarios, where there is no centralized regulatory authority in the blockchain network, and participants collaborate based on consensus algorithms. An example is the Dubai Financial Services Authority's blockchain-based "Blockchain Will Management Plan," facilitating the transfer and governance of digital assets on the network. This model effectively addresses traditional inheritance management issues, assisting in handling cases where assets are inaccessible due to the absence or expiration of personal identities.

5. Recommendations

To address legal issues in financial data security and privacy protection under blockchain technology, several measures should be implemented:

5.1. Enhance Regulation of Blockchain Technology:

5.1.1. Strengthen regulatory oversight of blockchain technology, despite its decentralized nature.

Blockchain technology is known as the next generation of Internet technology, and its decentralized, non-tamper, traceability and other characteristics are widely used in finance, logistics, medical and other fields. But at the same time, the anonymity of blockchain technology and the difficulty of regulating it have also raised many concerns.

1) Development of regulatory policies

The government should strengthen the supervision of blockchain technology, formulate relevant policies and regulations, and ensure the healthy and orderly development of the market. Regulatory policies should formulate reasonable norms and standards from technology, security, privacy, compliance and other perspectives to ensure that the application of blockchain technology will not have a negative impact on society.

2) Formulation of technical standards

The development of technical standards is the key to ensure the safety and reliability of blockchain technology. Relevant standardization organizations should strengthen the standard formulation of blockchain technology to ensure the interoperability between different blockchains, while ensuring the security and reliability of blockchain technology.

3) Transparency of blockchain technology

The transparency of blockchain technology is the key to ensuring that it is not abused. Blockchain technology should be designed with transparency, so that all participants can see all the transaction records on the blockchain and prevent illegal activities such as transactions and money laundering.

4) Strengthen the research on regulatory technologies

With the development of blockchain technology, the regulatory technology should also be constantly updated and upgraded. Regulators should strengthen the research and development and application of regulatory technologies, regulate transactions on the blockchain through technical means, and ensure the healthy and orderly development of the market.

5) Industry self-discipline

Industry self-discipline is the basis for ensuring the healthy development of blockchain technology. Industry organizations should strengthen the regulation and supervision of blockchain technology, establish industry standards and rules, and ensure that the application of blockchain technology will not have a negative impact on the society.

Strengthening the supervision under the blockchain technology requires the joint efforts of the government, technical standards organizations, industry organizations, and blockchain technology developers. Only through collaboration in various aspects can blockchain technology develop in a healthy and orderly market environment.

5.1.2. Establish relevant legal frameworks and standards to guide its development.

1) Establish a legal framework

The legal framework is the key to ensure that the application of blockchain technology complies with laws and regulations. The legal framework should include the legal status, rights and obligations of blockchain technology. The establishment of the legal framework requires the participation of the government, lawyers, scholars and other experts.

2) Strengthening intellectual property rights protection

Intellectual property protection is an important guarantee to ensure the innovation and development of blockchain technology. Governments and regulators should strengthen intellectual property protection of blockchain technology to ensure that innovators' intellectual property rights are fully protected.

3) Strengthen network security protection

Network security protection is an important guarantee to ensure the security and reliability of blockchain technology. Governments and regulators should strengthen the cyber security protection of blockchain technology to prevent hacker attacks and cybercrimes.

5.2. Improve Dispute Resolution Mechanisms:

5.2.1. Develop effective dispute resolution mechanisms that consider the decentralized nature of blockchain technology.

1) Decentralized arbitration institutions

In the traditional dispute resolution mechanism, the arbitration institution is an important part. Under the blockchain technology, we can set up decentralized arbitration institutions that can use the blockchain technology to ensure its fairness and transparency. The decentralized arbitration organization can be composed of multiple nodes, each node can participate in the award and reach consensus through the consensus algorithm. Decentralized arbitration institutions can improve the speed and efficiency of dispute resolution, while also ensuring the fairness of adjudication.

2) Community governance

Community governance is a governance model based on blockchain technology, which can be applied in the dispute resolution mechanism. Community governance can be composed of multiple participants, each involved in decision-making and adjudication. Community governance can vote to determine the resolution of the dispute and record it on the blockchain. Community governance can improve the speed and efficiency of dispute resolution, while also ensuring the fairness of adjudication

5.2.2. Establish a framework ensuring timely resolution of disputes that may arise.

1) Smart contracts

Smart contracts are an application of blockchain technology that can be written in a programming language to automatically execute the terms in a contract. Smart contracts can be used in dispute resolution mechanisms. For example, when there is a dispute between two users, smart contracts can automatically enforce the terms, determine which party is correct, and give corresponding rewards or punishments. Smart contracts can improve the speed and efficiency of dispute resolution, reduce labor costs, and ensure the fairness of rulings.

2) Multiple signature technology

Multiple signature technology is an application of blockchain technology, which can be used to ensure the security and credibility of assets. In the dispute resolution mechanism, the multiple signature technology can be applied to the execution process of the adjudication. For example, when a party wins the dispute, the party needs to execute the award through the multiple signature technology to ensure the safe transfer of assets. Multiple signature technology can improve the security and credibility of dispute resolution and reduce the risk of asset transfer.

5.3. Enhance Data Management and Maintenance:

5.3.1. Strengthen management and maintenance of data on the blockchain.

Data backup and recovery: Data on the blockchain needs to be backed up and restored regularly to ensure data integrity and reliability. Distributed storage technologies, such as IPFS (InterPlanetary File System), can be used to store data on the blockchain to improve data security and availability.

Adopt a tiered architecture: The blockchain system can adopt a tiered architecture to divide data management and maintenance into different levels. This makes data management and maintenance more flexible and efficient, while also reducing the complexity of the system.

Strengthen authority management: On the blockchain, the access and modification of data requires authorization. Therefore, strengthening authority management can effectively control the access and modify authority to ensure the security and privacy of data.

Strengthen supervision and auditing: Data on the blockchain needs to be regulated and audited to ensure data transparency and compliance. Blockchain regulatory technologies and auditing technologies, such as smart contract auditing and blockchain data analysis, can be used to strengthen supervision and auditing.

5.3.2. Ensure the authenticity and legality of recorded data to avoid erroneous entries on the blockchain.

Blockchain technology is characterized by decentralization, tamper-proof, transparency and traceability, and is considered as an ideal technology to ensure the authenticity and legality of data. However, blockchain technology is not foolproof, and it can still make mistakes. To ensure the authenticity and legitimacy of the blockchain recording data and to avoid errors, the following measures can be taken:

Adopt authoritative consensus mechanism: Consensus mechanism is the core of blockchain technology and determines the authenticity and legitimacy of blockchain data. At present, the mainstream consensus mechanism includes proof of work (PoW), proof of equity (PoS), and certificate of entrustment equity (DPoS). Different consensus mechanisms have different advantages and disadvantages, requiring appropriate consensus mechanisms according to specific application scenarios. At the same time, in order to ensure the authority of the consensus mechanism, it is necessary to use multiple authoritative nodes for consensus and avoid the control of a single node.

Data encryption and privacy protection: Blockchain technology can ensure that data cannot be tampered with, but can not guarantee the privacy of data. In order to protect data privacy, it is necessary to adopt encryption technology in the blockchain, such as public key and private key encryption, homomorphism encryption and so on. At the same time, in order to prevent data leakage, sensitive data needs to desensitize and adopt a secure data transmission protocol, such as SSL / TLS.

Improve the quantity and quality of nodes: The quantity and quality of nodes are an important factor affecting the authenticity and legality of blockchain data. In order to ensure the authenticity and legitimacy of blockchain data, it is necessary to increase the number of nodes to avoid the manipulation of a single node. At the same time, the quality of nodes needs to be improved to ensure that they have high computational power and credibility.

In short, to ensure the authenticity and legality of blockchain recording data, it is necessary to start from multiple aspects and adopt a variety of technologies and means. Only in this way can we effectively avoid blockchain data errors and ensure the healthy development and application of blockchain technology.

6. Conclusion

This paper, starting from the impact of blockchain technology on financial data security and privacy protection, has explored the legal issues faced in these domains under blockchain technology and provided corresponding recommendations. While blockchain technology offers new solutions for the security and privacy of financial data, practical applications reveal existing legal challenges. It is crucial to take measures such as strengthening regulatory oversight, improving dispute resolution mechanisms, and enhancing data management and maintenance to ensure the healthy development of blockchain technology in the financial sector.

References

[1] Liu, F.J. (2019) The privacy protection issue of blockchain technology in the financial field. [J] Technology Perspective, 22, 148-149.

[2] Li Haoran.(2020) Application Analysis of Blockchain Technology in Financial Data Security. [J] Modern Financial Information, 06,122-123.

[3] Jia Zhixiong.(2018) Research on Legal Regulations for Financial Data Privacy Protection under Blockchain Technology. [J] Legal and Commercial Studies, 09, 132-133.

[4] Li Jianhua, Deng Kai, Liu Ziqian. (2021) Research on the Application and Legal Issues of Blockchain Technology in the Financial Field. [J] Modern E-commerce, 03,116-117.

[5] Zhang Fei. (2017) The Application of Blockchain Technology in the Financial Field and Legal Risk Prevention. [J] Business Era, 05,82-83.

[6] Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L.J., Pautasso, C., Rimba, P. (2017). A Taxonomy of Blockchain-Based Systems for Architecture Design. 2017 IEEE International Conference on Software Architecture (ICSA), 243-252.

[7] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi and J. Wang. (2018) Untangling Blockchain: A

Data Processing View of Blockchain Systems. Transactions on Knowledge and Data Engineering, 30(7),1366-1385.

[8] Hu, X.Y., Fu Y.H., (2022) Research on the Application of Blockchain Technology to Financial Data Security - Taking Digital Currency as an Example. [J] Economic Growth Guide, 9 (2), 47-48.

[9] Lu Y.M., Sun C., (2021) Research progress in financial privacy protection based on blockchain technology. [J] Computer Science, 48 (3), 204-212.