Research on Mobile Financial Crime Prevention Strategy Based on Blockchain Technology

Chengni Li[1*], Lanlan Wei[2]

2012010@ahsjxy.edu.cn[1*], 785181496@qq.com[2]

Auhui Audit College, Anhui Hefei 230601, China[1]
Anhui Provincial Public Security Department, Hefei 230031, China[2]

Abstract. Due to the difficulty of collecting evidence and supervision, mobile financial crimes face governance difficulties. By using the unique technical advantages of blockchain, such as decentralization and multiple digital signature, it can help with the punishment and evidence collection of mobile financial crimes and form a mutual trust mechanism of mobile financial ecosystem. When blockchain technology is applied to to prevent mobile financial crimes, it is essential to continuously optimize the prevention strategy through the construction of mobile financial supervision information application platform and a mobile financial crime early warning system, to improve the crime fighting strength and governance efficiency.

Keywords: mobile financial crime; blockchain technology; financial supervision; crime early warning system

1 Introduction

The report of the 20th National Congress of the Communist Party of China clearly states that it is necessary to improve the national security system, strengthen the construction of security systems such as economic, financial, network and data security, and enhance the development of the network security industry. In response to network security issues, China has successively enacted relevant laws and regulations such as Cybersecurity Law of the People's Republic of China and Data Security Law of the the People's Republic of China, and the construction of network security has achieved certain results. However, with the continuous popularization and increasing functionality of mobile terminals, the number of criminal cases caused by mobile clients has also increased, especially in the field of mobile financial clients. Innovative technologies need to be applied to solve the governance challenges in this area.

2 Background of Crime Governance in the Field of Mobile Finance

Currently, the number of internet users in our country ranks first in the world. According to the 50th Statistical Report on Internet Development in China released by the China Internet Net-

[1] Corresponding Author: Chengni Li, Ad: Auhui Audit College, Hefei 230601, China Tel-number: 18756038659, Email: 2012010@ahsjxy.edu.cn

ICBBEM 2023, May 19-21, Hangzhou, People's Republic of China

DOI 10.4108/eai.19-5-2023.2334430

work Information Center (CNNIC) in August 2022, as of June 2022, the number of internet users in China reached 1.051 billion, with mobile internet users accounting for 99.6%[1]. Against this background, an increasing number of netizens are using mobile financial clients on their phones to conduct related financial transactions, such as fund transfers and borrowing. Although a series of financial transactions can be completed quickly through mobile banking applications, at the same time, there are also potential financial risks. The stealth of the crime makes it difficult to prevent and control related cases, which poses challenges and difficulties for crime governance.

2.1 Regulating Mobile Financial Clients is Difficult, Risks are not Easily Prevented

First, there are many ways to download financial clients and it is difficult to ensure program security. There are many ways to download mobile financial clients, such as app markets, browsers, QR codes, etc. Among all these download methods, the app market is relatively safer. Therefore, downloading clients through the app market can to some extent prevent downloading fake or pirated mobile financial clients. The security of clients downloaded through other channels is relatively low. It cannot be guaranteed whether they have undergone security checks or whether there are backups, and security information related to these clients cannot be confirmed. Therefore, there is no effective guarantee in terms of security. When users download and install clients through unknown links or unreliable QR codes, there will be certain risks when using them. Therefore, diverse download channels for mobile financial clients provide opportunities for criminals to commit crimes, thereby causing high risks in the use of mobile financial clients[2].

Secondly, mobile financial clients themselves have insufficient protection capabilities. With the continuous expansion of the network financial market, more and more mobile financial clients have emerged, and these mobile financial clients are often developed and operated by different institutions with varying sizes. Some institutions are large in scale and strong in strength, and have good technology to prevent criminals from attacking the institution's clients. However, smaller institutions lack corresponding capital investment and technical applications, making it easy for criminals to attack by exploiting vulnerabilities in the client, stealing registered user information or even stealing user property.

Finally, it is difficult to defend against counterfeit and phishing mobile financial clients. Counterfeit and pirated mobile financial clients are mostly highly similar to the genuine financial clients. When producing such fake clients, criminals will imitate the interface and content of the genuine financial client to achieve a lifelike effect. Then, they induce users to download these fake clients through browser links or QR code scans. Once users use these fake clients, criminals can directly steal user information and account funds. In addition to producing fake clients, criminals will also launch attacks on some smaller, less defensive genuine financial clients, tampering with their content, such as planting phishing interfaces in genuine financial clients. Once users log in, personal information is easily stolen.

2.2 Difficulties in Obtaining Evidence and Investigating Mobile Financial and Other Network Crimes Have Created Difficulties in Addressing the Problem of Criminal Governance

Firstly, insufficient evidence is commonly found in mobile financial crime cases. In relation to cases involving mobile financial and other network crimes, the electronic evidence obtained is

often numerous due to the digital characteristics of network financial crime. However, these numerous pieces of electronic evidence generally have low probative value in judicial trials and cannot independently prove the events waiting for evidence. Secondly, it is difficult to determine the amount of losses suffered by victims in mobile financial crime cases. To determine the specific amounts suffered by victims during illegal transaction activities, it is necessary to first obtain evidence such as information provided by the victims and transfer records. In most cases, however, this type of crime involves team efforts and factors that can affect the determination of the amount of money involved include the existence of some criminals who are still at large, which may result in missing evidence; and deliberate destruction of evidence, which makes it impossible to form a complete and effective chain of evidence, making it difficult to calculate the actual loss amount suffered. Thirdly, the identification of "causal relationships" in mobile financial crime cases is difficult. The causality relationship refers to a cause-and-effect relationship between a specific behavior and a specific result. The confirmation of any crime cannot be separated from the identification of the causal relationship. In the governance of mobile financial crimes, it is often necessary to confirm whether there is a causal logic relationship between suspected mobile financial client software and the criminal results. Criminals may argue that there is no causal relationship between the financial client software involved in the case and the criminal results based on the difficulty of tracing mobile financial client software. Fourthly, determining criminal jurisdiction is difficult in handling mobile financial crime cases. In current criminal procedural laws and other regulations, there are inconsistent interpretations regarding the jurisdiction of mobile financial and other network financial cases, which often leads to conflicts in dealing with these cases[3].

3 Description of the Advantages and Application of Blockchain Technology

The above-mentioned issues have caused serious obstacles to the investigation and management of financial crimes such as mobile finance and network finance by public security departments, which have harmed the vital interests of the masses, disrupted the network security environment, and affected social stability. Based on this, in addressing how to prevent and crack down on the use of false mobile finance client crimes, blockchain technology can play its powerful governance advantage. On the one hand, it records all transaction behaviors to provide complete criminal information for relevant case handling in the later stage. On the other hand, it can also give early warning to possible illegal transaction behaviors to maximize the protection of users' fund security.

3.1 Technical Advantages of Blockchain Technology

With the booming development of the financial market, traditional offline capital transactions have been transformed into online financial transaction models. The status of traditional banks and other financial institutions has been affected and impacted, and many Internet financing platforms have emerged like mushrooms. Although the emergence of internet financial platforms greatly improves people's convenience, their overall development time is not long, and government supervision is inadequate, which gives illegal elements an opportunity to take advantage of. To improve the security of these financial platforms, it is necessary to pay attention to a characteristic they share, namely "centralization". When the platform is "centralized",

illegal elements can obtain relevant control over the financial platform through various means and steal user information[4]. After using blockchain technology, the "centralized" characteristics of these platforms will be transformed into "decentralized", and illegal elements will find it difficult to obtain relevant control over the financial platform, thus increasing the difficulty and effectiveness of governance.

3.1.1 Decentralization and Distribution

The dynamic warning of mobile financial crimes aims to identify potential hidden network financial crimes in advance through the application of related technologies. The decentralized and distributed chain recording technology in blockchain technology is helpful for the application of dynamic warning of mobile financial and other network financial crimes. Blockchain refers to a chain composed of a certain number of blocks arranged in chronological order. During the transaction process, when the transaction information changes, the transaction information will not directly modify the information of the previous block in the blockchain. Specifically, when there is information change, all blocks in the blockchain will participate in the transaction information change. To modify transaction information, it is necessary to modify all blocks on this blockchain, which means that if illegal elements want to tamper with financial data, they need to modify at least 51% or more of the blocks on the blockchain before they have the opportunity to complete the modification of financial data. The number of blocks itself is very large. In theory, it is almost impossible to modify more than 51% of the blocks. Therefore, using blockchain technology can greatly ensure the security of mobile finance clients, and the essence of this technology is decentralization[5].

Distributed recording refers to the fact that all information on the public chain of the blockchain will be recorded in the designated area of the block. Once all financial transaction information of the mobile finance client is uploaded to the chain, the transaction information of the client on the public chain will be stored in all blocks on the chain. Before a financial client goes on the chain, it must be reviewed by relevant departments, and approved only after meeting the conditions. With more and more entities participating in the transaction chain, the constructed transaction information database will become increasingly large. In this huge database, specialized verification algorithms can enable all qualified financial clients on the chain to have corresponding verification mechanisms. Through the screening of the verification mechanism, some false financial clients can be detected and tracked. As the database grows larger, the number of blocks in the blockchain will increase, making it more difficult for illegal elements to tamper with data and conduct illegal transactions.

Moreover, false financial clients are mostly induced to download and use through browser links or QR codes. In order to help users better identify false financial clients, after applying blockchain technology, a specialized identification mechanism can be introduced for all qualified financial clients on the chain. For example, after downloading the relevant financial client, users can click on the verification link to check whether the client has a special "certified record" label. This can quickly identify whether the client is a legal client. For users, with this technology, they can download mobile finance clients with greater peace of mind and reduce the probability of account theft. Users only need to verify whether the financial client is legal through a special verification link after downloading it. If the client cannot provide relevant verification paths, it largely means that the client may carry hidden risks and belong to counterfeit or fake mobile finance clients. According to statistics, since the first half of 2022, the

Ministry of Industry and Information Technology has promoted a special campaign to crack down on client-side infringement of user rights. After conducting full coverage inspections on client applications that are mainly available in app stores, the number of users who have encountered network security issues has significantly decreased. It can be seen that detecting mobile financial clients is very necessary. Currently, China has made certain progress in blockchain technology. Some financial clients have actively tried to apply blockchain technology and have completed corresponding filings in the Internet Finance Association, effectively improving transaction security[6].

3.1.2 Multi-Signature Technology

Multi-signature technology has the function of independent signature authentication, as well as effectively preventing data tampering and ensuring data integrity. By using blockchain technology, effective smart contract codes can be developed to constrain all records stored on the chain, as well as requiring all mobile financial clients participating in the chain to undergo real-name registration, which can form a certain amount of pressure on fake financial clients.

Since the production difficulty of such fake clients is very high, illegal elements often involve multiple people to form a complete black industry chain when making counterfeit or fraudulent financial clients, ultimately achieving the theft of user information and funds. First, illegal elements will imitate and design based on legitimate mobile financial clients. In order to achieve the effect of being faithful to the original, this fake financial client will be very similar to the legitimate financial client in terms of interface and various modules, making it difficult for users to detect its differences. At the same time, some illegal elements with certain network technical capabilities can even imitate the financial functions of legitimate financial clients on their illegal financial clients. Secondly, after making an illegal financial client, illegal elements need to establish corresponding payment channels to steal user information and funds. At the same time, in order to effectively solve the problem of high-frequency fund transfer, illegal elements will use various channels and methods to obtain multiple accounts unaffected by risk control. After illegally obtaining the funds, because regulatory provisions cannot complete withdrawals through ATM machines without any restrictions, other means must be used for money laundering. After applying multi-signature technology of blockchain, during the process of transferring funds or conducting related transactions, illegal elements need to involve multi-signature of blockchain, which requires authorization through signature. During the authorization process, the system will send warning messages about abnormal transactions of illegal elements to law enforcement personnel, who can promptly trace the source of information and obtain relevant information about illegal elements[7]. For example, Zhongke lianan (Beijing) Technology Co., Ltd. independently developed the "Wuni" virtual currency crime early warning and tracking platform. With just one virtual currency "address" involved in the case, it can analyze and restore the complete virtual currency fund flow and locate the identity of the suspects through "one-click certification".

3.2 The Effectiveness of Blockchain Technology in Mobile Financial Crime Governance

3.2.1 Assisting in the Investigation and Punishment of Mobile Financial Crime

Firstly, the decentralized and distributed chain recording mode of blockchain technology can enable real-time tracking and recording of illegal transaction activities, lock specific amounts involved in the transactions, and effectively combat network financial crimes such as mobile finance. In addition, once the relevant information is recorded in the blocks of the blockchain, it cannot be erased. Therefore, as long as the illegal trade activity is completed within a block, the criminal record of the perpetrator will be recorded in the block. Once the criminal record of the criminal is recorded in the block, relevant departments can use the information stored in the block as evidence to effectively crack down on the illegal behavior of the criminals. Furthermore, the decentralized and distributed chain recording mode preserves detailed information about the criminal, including the time and method of the crime.

Secondly, by using blockchain technology, electronic evidence can be effectively improved in terms of tracing and self-proving, solving the problem of insufficient electronic evidence in network financial crimes such as mobile finance. After all the amounts involved in the case are put on the chain, automatic settlement can be realized, and this automatic settlement method can completely record the specific situation of fund transfers, becoming a powerful evidence for handling the case, and effectively improving the efficiency of handling cases, to a certain extent, safeguarding the legitimate rights and interests of victims. It can also record all transactions that occur on the blockchain, trace them, and restore the entire process of financial crime, which can effectively prove the relationship between the implicated financial clients and the crime results. Moreover, it can accurately determine the geographical location data of all parties involved in mobile financial crime cases, clarifying the issue of jurisdiction. In 2021, the Chain Eye Pro of OKLink assisted in cracking down on more than 80 cases of various crimes such as gambling, pyramid schemes, fraud, drugs, money laundering, theft, etc. and assisted the police and victims in freezing and recovering assets of more than 30 billion yuan.

Finally, when dealing with cases of mobile financial crimes such as counterfeit or imitation mobile financial clients, combining blockchain technology can greatly enhance the legal deterrence and effectively suppress the increase in related mobile financial crime cases.

3.2.2 Establishing a Mutual Trust Mechanism for Mobile Financial Ecosystem through Blockchain Technology

With the continuous in-depth research of blockchain technology, it will greatly promote the formation of mutual trust mechanisms in the mobile financial ecosystem and gradually reduce the space for mobile financial crimes such as counterfeiting and impersonating mobile financial clients. Currently, China has shown some initial progress in building the mobile financial ecosystem, and on this basis, further research is needed on how to promote the establishment of mutual trust mechanisms. In combating and controlling criminal cases of counterfeiting and impersonating mobile financial clients, it is not enough to rely solely on financial regulatory authorities. Instead, multiple parties should be mobilized to participate in forming a good cooperative mechanism. In this process, reasonable use of blockchain technology can help establish mutual trust mechanisms. Therefore, in the construction of public chains in blockchain, it is

required to maintain absolute trust between all blocks on the chain. The combination of public and private chain technologies can solve the trust issue in shared data on the chain. In the construction of blockchain, the participation of multiple parties such as government departments, financial institutions, and enterprises can build a mobile network financial alliance chain, thereby transforming the original bilateral trust or central trust mechanism into a multilateral trust mechanism, effectively solving the problem of "credibility", and based on the premise of controllable data, solving the barrier problem of data transmission through a multilateral trust mechanism[8].

4 Application Strategies of Blockchain Technology in Preventing Mobile Financial Crimes

4.1 Build a Platform for Mobile Financial Regulatory Information Application

4.1.1 Make full use of blockchain technology for information collection and build an information collection module

By utilizing timestamp technology, public chain technology, private chain technology and other technologies in blockchain, it is possible to record all transaction behaviors on the mobile financial client and trace these transactions to form a special information collection module. With the use of blockchain technology in mobile finance clients, when all legitimate mobile finance clients have completed registration on the chain, the transaction data generated in the mobile finance client will be stored in the block summary, creating a huge financial information database. At the same time, by using the information collection module function, it is possible to collect and store in real-time all users' financial account information and transaction records appearing in counterfeit or fake mobile financial clients in blocks, forming unmodifiable information. Once the regulatory department encounters relevant financial crime cases, based on the data stored in the information collection module, through intelligent analysis technology, all records of criminal activities can be obtained in a timely manner, providing strong evidence for mobile financial crime cases.

In the actual construction of the information collection module, the following issues need to be emphasized. First, it is necessary to consider that the collection equipment is easily attacked by external factors, especially criminals. To address this issue and ensure the security of collected data, a dedicated identity authentication function can be designed for the information collection module. Specifically, a public-private key pair is generated in the IOT gateway. First, the public key is sent to the terminal based on the IP information. After receiving the public key, the terminal encrypts the information of the corresponding IP and sends it back to the gateway. Then, the gateway decrypts the public key according to the private key information. If the decryption is successful, the terminal will receive the corresponding approval message and start collecting information. If decryption fails, the terminal will remain inactive after receiving the message [9]. Second, due to the inherent instability of the information collection module, problems such as data loss and abnormality may occur during practical applications. To effectively reduce the probability of such risks, multiple information collection modules can be designed to collect all transaction information that occurs in the mobile financial client that is uploaded to the blockchain through simultaneous operation of multiple devices. Third, to ensure the in-

formation transmission security of the information collection module, encryption methods can be designed for information transmission.

4.1.2 To build an information analysis module, analyze the data that has already been collected

In the construction of mobile financial regulatory information application platform, the information collection module is the most basic module, responsible for collecting all information, but it does not have the function of analyzing this information. Therefore, there needs to be corresponding analysis modules to better identify abnormal information. Through the function of the information analysis module, the transmitted information can be analyzed, and problematic data can be monitored. It can also realize real-time monitoring. If there are abnormal transaction behaviors, a warning will be issued in a timely manner, and real-time tracking of the transaction activities will be conducted. For example, when there are transaction activities in a false mobile financial client, the information analysis module will track the transaction, record relevant information such as the counterparty and transaction amount, and issue a warning. This allows relevant department personnel to track and capture criminals involved in such anomalous transactions in the shortest possible time. Since the information analysis module has recorded the transaction amount and locked relevant information regarding the transaction personnel, it provides strong evidence for subsequent case handling.

4.1.3 Design visual function modules to display data

To monitor the transaction information of counterfeit mobile finance clients, a specially designed visualization module (shown in Fig. 1) is needed to display the monitored data. In the module structure design, the first layer is the infrastructure layer, which mainly includes perception facilities and network facilities. Network facilities such as dedicated networks, wireless networks, and mobile networks can effectively transmit data based on these network facilities. The perception facilities mainly include image and graphics recognition and GPS positioning. Combined with perception facilities, each transaction can be automatically tracked and located. Then, in the database layer, data transmission, storage, and sharing are mainly performed. In the application service layer, data is managed and analyzed, and finally presented in the user display layer. Based on the construction of the visualization function module, regulatory personnel can understand the specific financial transactions in real-time and directly view any potential issues that may exist.

Fig. 2. Visualization of Function Module Structure Design

4.2 Building a Mobile Financial Crime Early Warning System

Building a mobile financial crime early warning system is to proactively detect and identify illegal transactions that may occur in counterfeit and fake mobile financial client, effectively protecting the safety of users' funds. In the construction of traditional online financial crime

early warning systems, it requires the participation of multiple departments to provide corresponding intelligence data to improve the effectiveness of early warning. Due to the lack of top-level design in the system construction, it is difficult to coordinate the participating departments, which can lead to difficulties in departmental organization and coordination. Therefore, by combining blockchain technology, the top-level design of the system can be improved to better coordinate the participation of various departments. Based on blockchain technology, the implementation of multi-department real-time data sharing, real-time data recording, and prevention of data leakage can ensure the security of data. At the same time, under the background of blockchain technology, each department can be responsible for their own intelligence data, ensuring the security and reliability of the data, and enabling better cooperation among departments. After improving their own intelligence data, each department can upload the standardized intelligence data in a unified format to the final management department. The management department can more effectively predict possible financial crimes and improve the accuracy of predictions after obtaining these aggregated intelligence data. Specifically, as shown in Figure 2, in the design of the mobile financial crime early warning system, it mainly consists of the chain-side business layer, the edge-side computing layer, and the terminal data resource layer, with the following details:

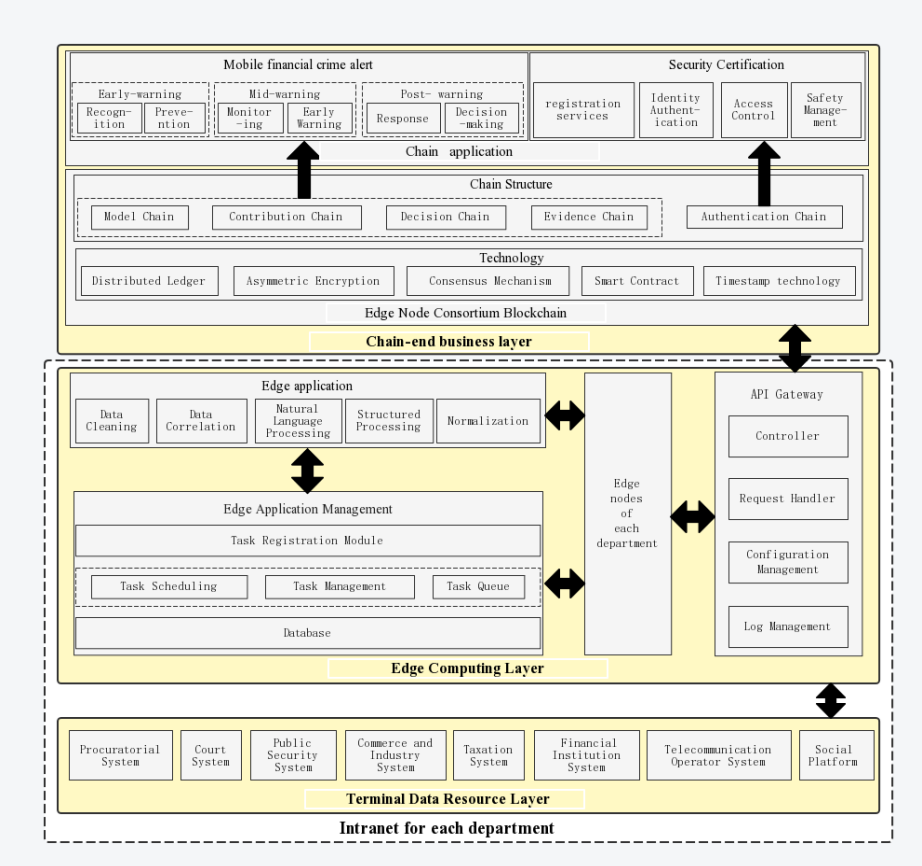

Fig. 3. Design of Mobile Financial Crime Warning System

4.2.1 Building Terminal Data Resource Layer

The terminal data resource layer mainly consists of internal systems from various departments. By involving multiple departments, massive intelligence data can be obtained. Based on these rich intelligence data such as illegal records, administrative penalty records, and fund flow records, the work of the warning system can be effectively supported. Possible hidden cases of mobile financial crimes can be identified in real-time[10].

4.2.2 Building the edge computing layer

In the edge computing layer, EdgeX Foundry technology is mainly used as a support. Through the construction of multiple microservices, it can effectively process large-scale intelligence data transmitted by various departments at the same time, and analyze these data separately by department.

4.2.2.1 API Gateway

The microservice interfaces in the API gateway are mainly used to process task content transmitted from various ports. In the case of receiving a task request, the controller in the gateway is responsible for parsing the task and then routing the parsed information to the request handler for microservice organization, thereby meeting the task request. The function of the configuration management module is mainly used to store relevant configuration information. The log management is mainly used to record the running status of each component. When a component encounters a problem during operation, it will be stored in the log management module. When technicians check the system, they can quickly analyze the problems existing in the system based on the records in the log management module and solve them.

4.2.2.2 Edge Application Management

Edge application management is mainly responsible for handling task requests sent by corresponding modules. Among them, the task registration module belongs to the top-level module. Through this module, staff can add new tasks or perform operations such as deleting, modifying, and querying existing tasks. When using the task registration module, the task information will be correspondingly saved in the database. The task scheduling module will check all the transmitted tasks, and after checking the legality of the tasks, the tasks that meet the requirements will be assigned an ID number. The role of this ID number is to queue the task in the task queue and facilitate subsequent queries by staff. The main function of the task management module is to read the queued task IDs and begin executing the task after loading the task content. Edge application management mainly performs operations such as numbering, scheduling, and queuing on requested tasks[11].

4.2.2.3 Edge Applications

Edge applications include functions such as data cleaning, data correlation, and normalization. Firstly, each department collects corresponding data based on its own advantages. Then, for these collected massive data, each department can perform corresponding cleaning or correlation operations on it, and then further analyze the data by combining natural language processing and statistical analysis methods. Finally, the analyzed data features are normalized, so that these originally scattered data, which are responsible for by various subject departments, can form standardized and unified data content, and uploaded to the alliance chain for sharing.

4.2.3 Building the Chain-end business layer

4.2.3.1 Chain Structure

The chain structure mainly includes authentication chain, model chain, etc. Specifically as follows:

Firstly, the authentication chain. The role of the authentication chain is to provide related services for all participating entities to register accounts, such as registering new employees' accounts and verifying personal information when logging in. Secondly, the model chain. It verifies and shares the data uploaded by departments to the blockchain and effectively prevents data tampering. Thirdly, the contribution chain. The contribution chain calculates and records the contribution value of each department through the use of smart contracts. Fourthly, the evidence chain. The evidence chain stores all the data uploaded by the departments, and these evidence can only be viewed by the public security department. By adopting this form, on the one hand, because only the public security department has the power to view all data, it can ensure the security of data and help mobilize other departments to actively share relevant data; on the other hand, the evidence chain is not used to save all intelligence data but only stores evidence data, which can greatly reduce the amount of data and prevent problems caused by excessive data volume[12].

4.2.3.2 Chain Application

In the chain application module, it is mainly divided into early warning stage, mid-warning stage, and post-warning stage. Among them, in the early warning stage, based on the experience of mobile financial criminal governance, a mobile financial crime early warning index system is constructed to provide corresponding references for work development. In the mid-warning stage, based on the existing feature set, relevant objects are monitored, and potential crimes are warned during the monitoring process. In the post-warning stage, it refers to after obtaining the alarm signal, relevant departments review the criminal case indicated by the signal and formulate corresponding control measures according to the specific situation of the case. Through the implementation of the chain application module, it can effectively identify and prevent possible criminal cases of counterfeiting and imitation of mobile financial clients, and prevent the occurrence of cases in advance.

5 Conclusion

In the regulatory governance of mobile financial crimes targeting mobile financial clients, the application of blockchain technology can effectively retain records of illegal transactions suspected of crimes. This provides corresponding evidence for handling mobile financial crime cases such as counterfeiting and impersonation of mobile financial clients. On the other hand, it can greatly prevent the occurrence of illegal transaction behaviors. Specifically, by combining blockchain technology, a specialized mobile financial regulatory information application platform can be constructed to record all transaction behaviors and identify transaction activities that may contain hidden risks. Additionally, the use of blockchain technology can establish a mobile financial crime early warning system. Based on the blockchain technology, multiple departments participate in it to build a huge intelligence database, monitor the possible illegal transaction activities in real time, and take timely measures to prevent the loss of user funds.

This enhances the crime-fighting strength and governance efficiency of the mobile financial field.

Acknowledgments. This study was sponsored by Anhui Provincial University Scientific Research Project in the Year 2022 (2022AH052947).

References

[1] China Internet Network Information Center.(2022) The 50th Statistical Report on Internet Development in China[R]. Beijing：China Internet Network Information Center, 2022: 25-28.

[2] Mx A , Hl B , Yzc D . (2020) Blockchain financial investment based on deep learning network algorithm [J]. Journal of Computational and Applied Mathematics,2020：372(C).

[3] Wei J. (2020)Study on the Jurisdiction of Internet Financial Crimes [D].Guangxi University for Nationalities,2020.DOI:10.27035/d.cnki.ggxmc.2020.000412.

[4] Hu Y. (2020) Applying blockchain technology to solve the governance challenge of financial crimes in cyberspace [N]. Procuratorial Daily, 2020-12-29 (003). DOI:10.28407/n.cnki.njcrb.2020.006111.

[5] He H, Li C .(2022) Network Security Analysis Based on Blockchain Technology [J].Network Security Technology& Application,2022(09):23-25.

[6] He C, Dong J, Ma Y, Zeng Y. (2022)Study on Coupling Method of Blockchain Technology and Public Project Fund Security Management Database with the Purpose of Transparency and Traceability[J].Technology Wind,2022(32):80-83+87. DOI:10.19392/j.cnki.1671-7341.202232027.

[7] Hao Z, Sun B. (2022)Research on the Application of Blockchain Technology in Police Jointoperation Command [J].Journal of China People's Police University,2022,38 (09):85-89.

[8] Hua X. (2020)Strengthening collaboration and front-end governance together to combat online financial crimes Summary of the Network Financial Crime Governance Summit[J].People's Procuratorial Semimonthly,2020(20):55-58.

[9] Liu W. (2022)The Application of Blockchain Technology in Network Security [J].China CIO News,2022(10):66-69.

[10] Li R. (2013)Risk and Prevention Suggestions for Cooperation Between Commercial Banks and Third-party Payment Institutions[J].Huabei Finance, 2013(8):28-30.

[11] Jiang Y. (2021)Prevention and Effectiveness Evaluation of Cyber Financial Crime Victi-mization[J].Journal of Nanjing University((Philosophy, Humanities and Social Sciences), 2021,58(05):112-124.

[12] Zarpala L , Casino F . (2020)A blockchain-based Forensic Model for Financial Crime Investigation: The Embezzlement Scenario[J]. 2020. https://doi.org/10.1007/s42521-021-00035-5