Jurnal IUS Kajian Hukum dan Keadilan
Volume 12 Issue 3, December 2024, E-ISSN 2477-815X, P-ISSN 2303-3827
Indexing: Scopus, DOAJ, Sinta 2, open access at : https://jurnalius.ac.id/

Application of Blockchain Technology in Cross-Border Telecommunications Network Fraud to Ensure China's Judicial Justice

Chen Siqi[1], Ramalinggam Rajamanickam[2], Nazura Abdul Manap[3], Zamre Mohd Zahir[4].
[1]Universiti Kebangsaan Malaysia, Malaysia, adam47chen@gmail.com.
[2]Universiti Kebangsaan Malaysia, Malaysia, rama@ukm.edu.my.
[3]Universiti Kebangsaan Malaysia, Malaysia, nazura@ukm.edu.my.
[4]Universiti Kebangsaan Malaysia, Malaysia, zamre@ukm.edu.my.

Abstract

Cross-border telecommunication fraud involves criminals abroad using network technology to remotely defraud Chinese citizens. China is currently facing more severe problems in combating cross-border telecommunications network fraud, including the easy destruction of electronic evidence during the process of collecting and storing evidence, low investigation efficiency in cross-border judicial cooperation, and the difficulty in tracing stolen money involved in cases located abroad. In order to combat crime and achieve judicial justice, investigators need to use the latest science and technology to improve case handling efficiency, and blockchain technology is exactly what they are paying attention to. Blockchain technology, as an emerging technology, has the characteristics of decentralization and non-tampering, and has unique advantages in the acquisition, storage and circulation of data. Therefore, this article aims to explore the necessity and feasibility of applying blockchain technology to combat cross-border telecommunication network fraud. This article adopts qualitative approaches to analyze the current Chinese legal provisions and research literature on the field of cross-border telecommunication network fraud, and provides a comprehensive understanding of blockchain technology. This article proposes leveraging the characteristics of blockchain technology to prevent telecommunication network fraud by establishing a personal information protection mechanism and a suspicious fund flow supervision mechanism through blockchain technology. Furthermore, the efficiency of investigation can be improved by establishing an internal communication and cooperation mechanism. The authenticity and integrity of evidence can be ensured by establishing blockchain forensics and evidence storage system.

Keywords: Blockchain Technology; Cross-border telecommunications network fraud; Decentralization; Electronic Data; Electronic Evidence.

1. INTRODUCTION

In recent years, under the unified leadership of the Ministry of Public Security of the People's Republic of China, public security bureau around the country coordinated and cooperated in taking special actions to crack down on telecommunication fraud on several occasions and have achieved certain results. The Fourth Procuratorate Director of China's Supreme People's Procuratorate Zhang Xiaojin said in an interview that from January to November 2023, the

 DOI: http://dx.doi.org/10.29303/v12i3.1554

public prosecutor's office prosecuted more than 42,000 people for telecommunication network fraud, accounting for 42.4% of the number of people prosecuted for fraud and 2.8% of the number of people prosecuted for criminal offences. However, the current situation of combating telecommunication network fraud is still severe and complex. Firstly, fraudulent gangs are showing a trend towards cross-border and monopolization. Secondly, fraudulent methods are diverse and complex, more confusing, and also give rise to serious violent crimes such as intentional injury. Thirdly, the organizations involved in crime are becoming more numerous, more closely co-operating, and the division of labor more clearly defined, and criminal tools and software are becoming simpler and easier to use, leading to more people involved in crime. Fourthly, funding channels have become intertwined and hidden, virtual coins have become a mainstream method of money-laundering, low-income groups have been exploited to assist perpetrators in transferring funds related to these crimes, and funding pathways have become more complex, difficult to recover and extremely harmful.[1]

With the development of the Internet, as well as the popularity of computers, mobile phones and other electronic products, perpetrators began to use the combination of Internet technology and deception to cheat others of their property.[2] perpetrators gradually combine telecommunication fraud tactics with the Internet, this type of fraud that has left investigators at their wits' end and countless victims duped. On 4 March 2016, this type of crime was formally named telecommunication network fraud by the official.

Hou Zhi, Yang Jie, Feng Xiangjun and Liu Xiaomei pointed out that in terms of its nature, cross-border telecommunication network fraud offences are no different from ordinary fraud offences in terms of their criminal composition, except that the intervention of telecommunication networks has made telecommunication network fraud have new characteristics compared with traditional fraud offences, which has led to many new types of difficult problems in judicial practice.[3] Xie Ling pointed out that with the progress and development of science and technology, network communications to achieve global coverage, information technology into all aspects of real life, the perpetrators use telecommunications network to crime, for the victim's daily use of mobile phones, online shopping, online social networking, online banking payments and other specific scenes to carry out fraudulent acts and access to the victim's property.[4]

In terms of cross-border, Kang Xinjian proposed that the so-called cross-border refers to the connection across the border.[5] Cross-border telecommunication network fraud crime has the distinctive features. Wu Zhiting and Zhi Shiyong pointed out in the study that with the use of network technology, the main body of this type of crime are grouped, with a tight organizational structure.[6] Li Xinmin pointed out that, as an emerging crime,

1 Xiaotian Jiang and Man Liu, "Interview with Zhang Xiaojin, Director of the Fourth Procuratorial Department of the Supreme People's Procuratorate: The Cross-Borderisation of Wire Fraud Crimes, with a Focus on Criminal Syndicates and the Masterminds behind Them," Southern Metropolis Daily, May 4, 2024, https://www.spp.gov.cn/spp/zdgz/202403/t20240304_647113.shtml.

2 Henny Saida Flora, "Criminal Sanctions toward False Criminal Actors through the Internet," *The International Journal of Humanities & Social Studies* 7, no. 9 (September 30, 2019), https://doi.org/10.24940/theijhss/2019/v7/i9/HS1909-081.

3 Zhi Hou et al., "Research on the Dilemma View and Practical Response of Crime of Telecommunication Network Fraud——Take 137 Cases as Breakthrough," *Tianjin Legal Science* 34, no. 2 (August 16, 2018): 83–89.

4 Ling Xie, "Research on Information Investigation of Telecom Network Fraud," *Journal of People's Public Security University of China(Science and Technology)* 26, no. 3 (2020): 85–93, https://doi.org/10.3969/j.issn.1007-1784.2020.03.013.

5 Xinjian Kang, "Research on the Investigation and Prevention of Cross-Border Telecom Fraud in Yunnan Border Area in the Era of Big Data," *The Journal of Yunnan Police College*, no. 1 (2020): 92–97, https://doi.org/10.3969/j.issn.1672-6057.2020.01.017.

6 Zhiting Wu and Shiyong Zhi, "Characteristics of Telecom Network Fraud Crime and Prevention and Control Measures," *Journal of Hebei University of Economics and Business(Comprehensive Edition)* 21, no. 2 (2021): 77–81, https://doi.org/10.3969/j.issn.1673-1573.2021.02.013.

cross-border telecommunications network fraud breaks the traditional characteristics of fraud restricted by the regional bureau, cross-border telecommunications network fraud is not affected by geography, the victims are widely distributed, and the scope of harm is wide.[7] Lou Yongtao and Tang Xiang pointed out that with the advancement of intelligent communication technology and the development of big data, perpetrators are becoming more and more covert, and the criminal means are constantly renovated with the advancement of technology, and the prevention and control of telecommunications fraud is a very serious situation.[8]

In telecommunication network fraud cases, most of the evidence exists in the form of electronic data, which puts higher requirements on investigation and evidence collection.[9] Ma Zhonghong pointed out that perpetrators use intelligent criminal means to commit crimes, and it is extremely difficult to investigate. Fraud perpetrators set servers and Internet IP addresses outside of China, so it is difficult to obtain evidence directly related to the case, and it is not possible to get a glimpse of the whole picture of the case without forming a chain of evidence.[10] The research of Wu Chengjie and Chen Wen shows that cross-border telecommunications network fraud as a typical new type of cybercrime, different from the physical space of the fraud crime, perpetrators use communication and Internet technology to contact the victim, perpetrators are always hidden behind the scenes, due to the network for the virtual space, the main evidence of the crime can only be in the form of electronic data retained in the electromagnetic media. Generally speaking, in addition to CDR (Call Detailed Record) data query, SKYPE (instant messaging software) record data, disks, communication records and other electronic data, almost no trace will be left behind.[11] Cross-border telecommunications network fraud perpetrators use the Internet, data communications and other high-tech means to commit crimes, and it is difficult for investigators to obtain relevant clues. Even if investigators obtain relevant criminal clues through various channels, the evidence is stored in electromagnetic media and is easy to delete and tamper with. As a result, the evidence obtained by investigators may not be used as evidence to substantiate the charges.[12]

With the deepening process of globalization, telecommunication network fraud has also shown a cross-border trend. According to statistics, the number of cases of fraud dens outside China has now exceeded 60 % of all fraud cases. In terms of investigation and arrest, although China has achieved some success, the high mobility of perpetrators and the gap between the law enforcement capabilities of other countries and China have led to many difficulties in police co-operation.[13] Liu Yang points out that China currently faces some problems in entrusting other countries with criminal judicial assistance,

7 Xinmin Li, "Research on the Development and Countermeasures of Cross-Border Crime of Telecom and Online Fraud," *Journal of Western*, no. 1 (2024): 78–81.

8 Yongtao Lou and Tang Xiang, "The Prevention, Control and Reflection of Telecom Network Fraud Crime in the Big-Data Age," *Journal of Chongqing University of Technology(Social Science)*, no. 3 (2020): 121–28.

9 Evgenii Khramtcov, "Optimization of Criminal Procedure Legislation in the Field of Evidence in Criminal Cases on Crimes against Property Committed Using Information and Telecommunication Technologies," *Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia* 2022, no. 2 (July 6, 2022): 239–43, https://doi.org/10.36511/2078-5356-2022-2-239-243.

10 Zhonghong Ma, "The Difficulties and Countermeasures about the Investigation of the New Network Crimes Taking Telecommunications Fraud as the Representativesed——Research Based on W Survey," *Journal of People's Public Security University of China: Social Sciences Edition*, no. 3 (2018): 78–86.

11 Chengjie Wu and Wen Chen, "Discussion on Difficult Issues in Telecommunication Network Fraud Cases," *Journal of Law Application*, no. 21 (2017): 40–50.

12 Tongyu Xiao, "Discussion on the Investigation Dilemma and Countermeasures of Telecommunication Fraud Cases," *Network Security Technology & Application*, no. 1 (2023): 131–33, https://doi.org/10.3969/j.issn.1009-6833.2023.01.064.

13 Zicheng Huang, "Research on International Co-Operation in Combating Transnational Telecommunication Network Fraud Offences in the Lancang Subregion," *Network Security Technology & Application*, no. 2 (2022): 160–62, https://doi.org/10.3969/j.issn.1009-6833.2022.02.094.

including the fact that China may not have signed a treaty on criminal judicial assistance with the requested country, or that the provisions on evidence extraction in the assistance treaty are not specific, and that the request for evidence collection is inefficient, leading to delays in the timing of the investigation or the extraction of evidence that does not comply with the requirements of Chinese law.[14] Chen Longxin pointed out that there are objective differences between China and ASEAN countries in terms of social systems, ideologies, customs and cultural traditions. There are also differences between ASEAN countries in terms of legal systems and judicial systems. Differences in legal systems lead to conflicts of jurisdiction in criminal cases, and different judicial systems can cause obstacles to the connection of relevant functional departments in specific investigative cooperation, which in turn affects the efficiency of investigative cooperation.[15] Some scholars also believe that judicial assistance between ASEAN countries and Australia should be strengthened to combat cross-border crime.[16]

One of the challenges China needs to face is the difficulty of recovering stolen funds. There are many criminal organizations involved cross-border telecommunication network fraud. These organizations have developed a complete criminal process. Perpetrators can use the network to transfer stolen money and evade detection by public security authorities.[17] Under the non-contact mode of crime, the fraud can be very insidious. Perpetrators, money-laundering organizations and victims did not have direct contact. These aspects mentioned above not only increase the fraud crime, but also the difficulty of evidence collection and recovery of stolen property.[18]

Currently, there have been a large number of studies on cross-border telecommunication network fraud, and comprehensively these studies can be found that, compared with traditional fraud crimes, cross-border telecommunication network fraud is a criminal offence committed by perpetrators with the purpose of illegal possession, using the Internet, telecommunications or other modern media of communication, as well as financial exchange services, and other means to commit criminal acts of fraud across different countries or regions. Currently, the problems faced in the management of cross-border telecommunication network fraud offences mainly include the easy destruction of electronic evidence during forensics and depositing, the inefficiency of cross-border judicial cooperation, and the difficulty of tracing the stolen money involved in cases located outside the country.

Blockchain technology, one of the most significant technological innovations in recent years, has garnered extensive attention from both industry and academia. As a distributed ledger technology, it is transforming business practices across various industries, including banking and financial services, healthcare, food, transportation, and public services. Research in this field highlights its growing potential for practical applications. For instance, Ana □ui□ Tankovi□, Marina Periši□ Prodan, and Dragan Benazi□ discuss the segmentation of consumer adoption in blockchain technology in

14 Liu Yang, "On the Forensics of Cross-Border Telecom Network Fraud Crime--Taking Southeast Asian Countries as the Object of Analysis," *Journal of Political Science and Law*, no. 6 (2023): 5–11.

15 Longxi Chen, "Research on China's International Investigative Co-Operation" (Doctoral dissertation, East China University of Political Science and Law, 2011).

16 Ika Yuliana Susilawati, "PERAMPASAN ASET HASIL TINDAK PIDANA KORUPSI DI LUAR NEGERI MELALUI BANTUAN TIMBAL BALIK (MUTUAL LEGAL ASSISTANCE)," *Jurnal IUS Kajian Hukum Dan Keadilan* 4, no. 2 (2016): 138–51, https://doi.org/10.12345/ius.v4i2.281.

17 Alexander Mikhaylov and Richard Frank, "Cards, Money and Two Hacking Forums: An Analysis of Online Money Laundering Schemes," in *2016 European Intelligence and Security Informatics Conference (EISIC)* (IEEE, 2016), 80–83, https://doi.org/10.1109/EISIC.2016.021.

18 Fei Pan and Chang Liu, "Governance and Prevention of Telecommunication Network Frauds," *Journal of Guangxi Police College* 32, no. 5 (2019): 48–52, https://doi.org/10.19736/j.cnki.gxjcxyxb.2019.0509.

their study. They emphasize its wide-ranging influence and adoption trends.[19] However, the application of blockchain technology in criminal case investigations remains relatively underexplored, with research mainly focusing on areas such as investigation and forensics, intelligence sharing, and collaborative investigations. Some scholars propose building a synthetic investigation intelligence collaborative sharing system based on blockchain technology to enhance investigative processes.[20] Additionally, theories such as front-end control, judicial presumption, unfavorable self-identification, and supplementary corroboration have been suggested to address challenges related to the authenticity of electronic evidence. These theories are often combined with blockchain deposition technology to improve evidence storage and authentication.[21] Further advancing the field, Chen Peixin proposed a blockchain-based cloud forensics solution using the Changan Blockchain platform and China's national encryption algorithms (SM2, SM3, and SM4). This approach aims to enhance the security, integrity, and functionality of blockchain forensics through experimental verification and security analysis.[22] Anand Karambe proposed the development of a global criminal database and application leveraging blockchain technology. This system would enable investigative agencies, police, and other organizations to access global crime data through distributed blockchain nodes within their respective countries. Authorities could instantly and efficiently retrieve comprehensive criminal histories, including identifying details of anonymous individuals, to address cases involving foreign nationals suspected of antisocial activities in their countries of origin. By streamlining the process of obtaining information from a suspect's home country, this solution would significantly reduce delays. Furthermore, the blockchain-based system would ensure the integrity and authenticity of criminal records, effectively eliminating the risk of forgery or tampering.[23] Obviously, there have been some relevant researches and explorations on the application of blockchain technology in the work of public security organs, but the research on the application in the investigation of criminal cases is still relatively small. Blockchain, as an emerging technology, has great advantages in the acquisition, preservation and circulation of data, etc. This article aims to study how to apply blockchain technology to solve the current problems in the investigation of cross-border telecommunication network fraud cases.

Therefore, this article will start from the perspective of the application of blockchain technology, use a qualitative research methodology to analyze in detail the literature related to cross-border telecommunication network fraud. In this article, the existing literature was collected by searching academic websites for keywords such as cross-border telecommunication network fraud and blockchain technology and using libraries to find laws and literature on cross-border telecommunication networks. By understanding the concepts and characteristics of cross-border telecommunication network fraud and blockchain technology, this article addresses the difficulties faced in the process of combating cross-border network fraud, discusses the role that blockchain

19 Ana Čuić Tanković, Marina Perišić Prodan, and Dragan Benazić, "Consumer Segments in Blockchain Technology Adoption," *South East European Journal of Economics and Business* 18, no. 2 (December 1, 2023): 162–72, https://doi.org/10.2478/jeb-2023-0025.

20 Shuxiang Qiu and Haobo Jin, "Synthetic Investigative Intelligence Management with the Application of Blockchain Technology," *Journal of Zhejiang Police College*, no. 4 (2018): 28–34, https://doi.org/10.3969/j.issn.1674-3040.2018.04.005.

21 Pinxin Liu, "On the Institutional Value of Electronic Data's Storage and Authentication Based on Blockchain," *Archives Science Bulletin*, no. 1 (2020): 21–30.

22 Peixin Chen, "Cloud Forensics Solution Based on Blockchain," *Network Security Technology & Application*, no. 3 (2024): 124–26, https://doi.org/10.3969/j.issn.1009-6833.2024.03.046.

23 Anand Karambe, "Blockchain-Based Approach for Tracking Global Criminals," *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT* 07, no. 06 (June 12, 2023), https://doi.org/10.55041/IJSREM19377.

technology can play in combating cross-border network fraud, and then puts forward suggestions for applying blockchain technology.

2. ANALYSIS AND DISCUSSION

Aiming at the current problems faced in the fight against cross-border telecommunication network fraud, such as the difficulty of evidence collection, the ease of destruction of electronic evidence, the low efficiency of investigation and collaboration, the many limitations faced by international cooperation, and the difficulty of recovering stolen money. This article provides an in-depth understanding of blockchain technology, discusses the role that blockchain technology can play in combating cross-border telecommunication network fraud and puts forward suggestions for its application.

2.1. The Concept and Characteristic of Blockchain Technology

Blockchain is in essence a decentralized distributed ledger database, which is a chain of data blocks arranged in a certain order through cryptographic correlation, and contains stored data information in each data block, which contains a data record, the hash value of the current block, the hash value of the previous block, timestamps, and other information.[24] Blockchain is not just a single technology, but is the result of the integration of multiple technologies, including distributed storage technology, asymmetric encryption technology, smart contracts, etc., which combine to form a decentralized data recording and storage system.[25] The blockchain contains every transaction that has ever been executed in the system, and based on this transaction information, people can find information at any time and at any address.[26] The blockchain as a state machine, each transaction is an attempt to change the state, and each consensus-generated block is the result of the participants' confirmation of the result of the transaction in the block resulting in a change of state.[27] Each node within the blockchain network can independently record data information and perform various network operations, ensuring the authenticity and reliability of the data information through the network's publicity mechanism, and making the stored data information impossible to be tampered.[28]

Decentralization is the most basic feature of blockchain. Due to the application of distributed storage technology, the data in the system is stored and maintained by the nodes of the whole network, no longer relying on the central processing node, and the blockchain nodes follow the unified rules to update the data. Each network node is equal to each other, and no node is in a central position or has control or management authority over other nodes.[29] In the traditional centralized storage model, an attack on the central node can cause damage to the entire system, while in the decentralized

24 Craig S Wright, "Bitcoin: A Peer-to-Peer Electronic Cash System," *SSRN Electronic Journal*, 2008, https://doi.org/10.2139/ssrn.3440802.

25 Zibin Zheng et al., "Blockchain Challenges and Opportunities: A Survey," *International Journal of Web and Grid Services* 14, no. 4 (2018): 352–75, https://doi.org/10.1504/IJWGS.2018.095647.

26 Subiramaniyan S D et al., "A Novel Decentralized Product Verification Using Blockchain Technology," in *2023 7th International Conference on Trends in Electronics and Informatics (ICOEI)* (IEEE, 2023), 642–46, https://doi.org/10.1109/ICOEI56765.2023.10125833.

27 Kenji Saito and Hiroyuki Yamada, "What's So Different about Blockchain? — Blockchain Is a Probabilistic State Machine," in *2016 IEEE 36th International Conference on Distributed Computing Systems Workshops (ICDCSW)* (IEEE, 2016), 168–75, https://doi.org/10.1109/ICDCSW.2016.28.

28 Suyash Gupta and Mohammad Sadoghi, "Blockchain Transaction Processing," in *Encyclopedia of Big Data Technologies* (Cham: Springer International Publishing, 2019), 366–76, https://doi.org/10.1007/978-3-319-77525-8_333.

29 Remya Stephen and Aneena Alex, "A Review on BlockChain Security," *IOP Conference Series: Materials Science and Engineering* 396 (August 29, 2018): 012030, https://doi.org/10.1088/1757-899X/396/1/012030.

blockchain network, an attack on a single node cannot damage the entire network, resulting in a qualitative improvement in security and stability.[30]

Information storage into the blockchain cannot be tampered. Inside the blockchain, data information cannot be changed after being stored after verification, and the security of data is greatly improved through the application of cryptography technology, distributed storage and consensus mechanism. Blockchain shifts people's trust in centralized intermediaries to trust in systems and algorithms, and as long as the systems and algorithms are trustworthy, then the stored data is secure.[31] For the blockchain, the attacker is ineffective in modifying the database on a single node only, but also needs to modify all the remaining nodes as well as the subsequent storage records, which is not yet successful enough with the current technological means, and the changes in the data will make the hash value on the block change dramatically, and it is difficult to hide the traces of tampering.[32]

2.2. Functions Played by Blockchain Technology in Combating Cross-border Telecommunication Network Frauds

2.2.1. Strengthening The Security Protection of Personal Information Data

The issue of citizens' personal data security is very important, and the leakage of personal data is a determining factor affecting crime.[33] Obviously in cross-border telecommunications network fraud, the security of citizens' personal data is also very important. Although the law stipulates that users have ownership of their own information, citizens' personal privacy data are held by perpetrators through illegal channels, and citizens have no way of knowing whether their information has been leaked or not, and no way of preventing the leakage of their own information.[34] Protecting citizens' personal data should therefore be a legal priority.[35]

The data stored in blockchain is open and verifiable, and users can check by themselves whether their data has been leaked or tampered with. Through the application of asymmetric encryption technology, the users can hold their personal information by themselves and prevent personal information being used maliciously by others. The application of asymmetric encryption technology has higher security in data storage, and it can better protect the private data, especially the public security organs can play a great advantage in the protection of the database network security.[36]

2.2.2. Constructed The Fund Flow Supervision System Based on Blockchain Technology

Suspicious fund flows can be monitored based on data information such as the size of transactions, the type of transactions involved, and the frequency of transactions in a short period of time as screening conditions. Regardless of whether the perpetrators

30 Van-Duy Pham et al., "B-Box - A Decentralized Storage System Using IPFS, Attributed-Based Encryption, and Blockchain," in *2020 RIVF International Conference on Computing and Communication Technologies (RIVF)* (IEEE, 2020), 1–6, https://doi.org/10.1109/RIVF48685.2020.9140747.

31 Zehua Kang, "Research on the Application of Blockchain in Smart Policing," Legal and Economy, no. 7 (September 15, 2020): 160–62, https://doi.org/10.3969/j.issn.1005-0183.2020.07.066.

32 Neelam Badhani and Sachin Sharma, "Blockchain-Based Financial Enterprises Credit Value Information System Using Federated AI," in *2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)* (IEEE, 2023), 1–7, https://doi.org/10.1109/ICBDS58040.2023.10346298.

33 E. A. Russkevich, "Personal Data in the Mechanism of Criminal Law Protection," *Proceedings of Southwest State University. Series: History and Law* 13, no. 5 (December 5, 2023): 75–86, https://doi.org/10.21869/2223-1501-2023-13-5-75-86.

34 Dragana B. Petrović, "PRIVACY AND PROTECTION OF PERSONAL DATA – CRIMINAL LAW ASPECT," *Strani Pravni Život* 66, no. 4 (January 26, 2023): 469–89, https://doi.org/10.56461/SPZ_22407KJ.

35 Fenty Usman Puluhulawa, Jufryanto Puluhulawa, and Moh. Gufran Katili, "Legal Weak Protection of Personal Data in the 4.0 Industrial Revolution Era," *Jambura Law Review* 2, no. 2 (June 20, 2020): 182–200, https://doi.org/10.33756/jlr.v2i2.6847.

36 Valeriia Balatska and Ivan Opirskyy, "ENSURING THE CONFIDENTIALITY OF PERSONAL DATA AND SUPPORTING CYBER SECURITY WITH THE HELP OF BLOCKCHAIN," *Cybersecurity: Education, Science, Technique* 4, no. 20 (2023): 6–19, https://doi.org/10.28925/2663-4023.2023.20.619.

withdraws cash, transfers money or uses money to consume, the channels for transferring the funds involved must rely on the various means of financial services provided by financial institutions.[37] The advantage of relying on blockchain to strengthen the supervision of suspicious fund flows is that it can help public security organs from information and data monitor, lower supervision costs.[38] Within the blockchain system, the autonomous operation of smart contracts eliminates the cost of direct human involvement, and computer programmers can improve the efficiency and economy of contractual relationships, reducing the problems of errors, misunderstandings, delays or disputes. Combining blockchain to establish a regulatory system also solves the conflict between data collection and privacy. On the one hand, investigators cannot interfere with the operation of the system, on the other hand, any access records of investigators to the system will be recorded by blockchain and cannot be deleted or altered, which effectively guarantees privacy and security within the enterprise, and is conducive to public security organs and social enterprises to reach a consensus more quickly in this regard. By automatically monitoring whether the capital flow data meets the regulatory standards of the public security authorities, it will not only reduce the regulatory burden of enterprises and administrative departments, but also strengthen the quality of the data obtained, so as to achieve timely control of suspected illegal acts.

2.2.3. Constructed The Investigation Record System Based on Blockchain Technology

Relative to traditional physical evidence, there is a great difference in the way electronic evidence is generated and exists, mainly reflected in the symbolic, easily tampered with, inseparable, easily replicated, and easily destroyed electronic evidence, making the authenticity of electronic evidence in the process of collection and use will change.[39] With the increasing quantity and variety of electronic evidence, the improvement of the investigation and evidence collection process should take into account the professional quality of investigators and try to adopt a convenient and fast way to extract electronic evidence, so the blockchain-based investigation record system end should be integrated with a variety of factors, such as easy to grasp the operation method, higher extraction efficiency, and stronger security.[40] Therefore, in order to improve the quality of evidence, public security organs should strengthen the upgrading and transformation of evidence collection equipment, promote the development of evidence collection equipment in the direction of intelligence, and try to exclude the interference of human factors in the process of evidence collection, so as to prevent the evidence extracted by investigators from being "contaminated" due to their operational errors or other factors.

For evidence collection, such as on-site audio and video recordings by investigators during evidence collection, the combination of law enforcement recording devices with the blockchain application system should be considered. Law enforcement recording devices should be used to record the behavior of investigators at the scene, and the data should be automatically transferred to the blockchain system at the end of the on-site investigation. In addition, for the scene of physical evidence, such as documentary evidence and other physical evidence, fixed preservation of records, site photos, and other data should also ensure synchronous upload to the blockchain to facilitate later

37 Jun Xiong and Li Li, "The Trial-Centred Perspective of Telecommunication Network Fraud Crime Investigation and Evidence Collection Path," *Legal System and Society*, no. 31 (2020): 23–24, https://doi.org/10.19387/j.cnki.1009-0592.2020.11.012.

38 Shusong Ba, Wei Wei, and Haifeng Bai, "From Data Driven to Embedded Supervision: Prospects of Financial Supervision Based on Blockchain," *Journal of Shandong University(Philosophy and Social Sciences)*, no. 4 (2020): 161–73.

39 Pinxin Liu, *Dianzi Zhengjufa*, 1st ed. (Beijing: China Renmin University Press, 2021).

40 Aleksandrs Brīvers, "UNDERSTANDING OF ELECTRONIC EVIDENCE, ITS ACQUISITION AND STRENGTHENING IN CRIMINAL PROCEEDINGS," *INDIVIDUAL. SOCIETY. STATE. Proceedings of the International Student and Teacher Scientific and Practical Conference*, January 11, 2023, 156–62, https://doi.org/10.17770/iss2021.6913.

access and review. Investigators should use forensic devices to collect electronic data generated at the time of the crime. So that the case-related electronic data and information, such as case-related web pages, victims' transfer information, case-related chat information, and case-related IP addresses, etc., can be intelligently identified for forensics. Before uploading the data to the blockchain, artificial intelligence technology should be used to assist in analyzing the legitimacy of the evidence involved in the case, such as the legitimacy of the investigator's identity, the time of the forensics, the place of the forensics, the completeness of the forensics process, and other aspects of the authentication process, and then, after passing the verification, the system automatically generates the forensics report containing the information of time, place, forensics personnel, data format, data type and other data information, and finally, the forensics equipment automatically identifies the collected electronic evidence. Finally, the collected electronic evidence is automatically uploaded to the blockchain system by the evidence collection device, and in the process of uploading, the intelligent contract is applied to verify the uploaded data standards. And the system judges whether the evidence collected by the investigators meets the standards prescribed by law, so as to decide whether the extracted evidence can be stored in the blockchain as the basis for subsequent judicial activities.

2.2.4. Constructed The Cross-border Judicial Collaboration System Connecting Investigators of Different Areas Based on Blockchain Technology

In combating cross-border telecommunication fraud crimes, Chinese public security authorities need to collaborate with police agencies in other countries in many aspects such as evidence collection, data exchange, search and arrest, and recovery of stolen money, so the optimization of cross-border collaboration mechanisms should focus on the following aspects.[41] Firstly, countries should focus on building a secure and trustworthy communication platform based on blockchain technology, so as to improve the construction of cross-border collaboration mechanism.[42] Secondly, after the establishment of the platform, law enforcement agencies of various countries can promote the implementation of offline law enforcement collaboration through the operation of online rules, and improve the efficiency of law enforcement cooperation through the blockchain platform by providing an automatic online collaboration mode for multinational police forces. At the same time, the blockchain system can provide judicial appraisal services for documents, certificates and assets involved in the process of international law enforcement cooperation. Finally, through the platform built by technical means that can provide open and transparent information, all parties can query the data and information within the blockchain system to understand the source and trajectory of all kinds of materials, providing a foundation of trust for multi-party collaboration.[43]

The operation of the blockchain system is conducive to reaching consensus faster due to the decentralized nature of the blockchain, all parties involved are equal participants in the main body, jointly involved in maintaining the operation of the system, none of the parties do not hold the right to control the system, all parties can independently interact with the information under the condition of equal status, and reach a consensus

41 AiJiao Liu, "The Strategy of Fighting for the Telecommunications Fraud with I Iternational Police Cooperation," in *Proceedings of the 2016 4th International Conference on Management, Education, Information and Control (MEICI 2016)* (Paris, France: Atlantis Press, 2016), https://doi.org/10.2991/meici-16.2016.19.

42 Cheng-Yong Liu, Tian-Yu Dong, and Ling-Xing Meng, "Cross-Border Credit Information Sharing Mechanism and Legal Countermeasures Based on Blockchain 3.0," *Mobile Information Systems* 2022 (July 1, 2022): 1–12, https://doi.org/10.1155/2022/6972647.

43 Luo Wanhua, "Research and Application of Blockchain Technology in Transportation Administrative Law Enforcement," in *2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC)* (IEEE, 2020), 766–70, https://doi.org/10.1109/ITOEC49072.2020.9141836.

faster in the extraction of evidence, the apprehension of suspects and other aspects of the process.[44] The establishment of technical rules can ensure that the identity and expression of the subject of consultation are more equal, the participation of the subject of consultation is more direct, the consultation process is more open and interactive instantly and conveniently, and the results of the consultation are more effective. Blockchain technology standards and composition structure have common technical specifications at home and abroad, and blockchain technology as the underlying technology of public security information resources can narrow the technical gap between different data systems, strengthen mutual articulation, and eliminate the problem of system exclusion.[45] In order to ensure that all parties will act in accordance with the results reached through consensus, the blockchain can transform the multi-party agreement into online rules to supervise the implementation of all parties, and according to the implementation results of all parties to be rated and open to the whole network, according to the rating results can be decided by the system to give or deprive of a certain degree of authority, to achieve the whole network to supervise the common governance of the joint efforts to combat telecom fraud crimes. In addition, based on the blockchain technology architecture of self-confidence different countries' police departments can exchange sensitive data with each other within a certain range, get rid of the problem of lack of trust between different countries and regions, so as to enhance the executive power of international investigation collaboration and build a more complete international investigation collaboration system.[46]

3. CONCLUSION

Although China's public security organs have carried out special actions to combat cross-border telecom network fraud many times, cross-border telecom network fraud has a low threshold, high returns and low risk, which constantly tempts more people to embark on the road of crime, especially when various hot events break out, the suspects are even disregard the law and morality to try to obtain illegal benefits. In this context, the application of blockchain can play an important role in the fight against cross-border telecommunication network fraud. Compared with technologies such as big data and artificial intelligence, the advantage of blockchain lies in its ability to guide multiple parties to carry out actions together, so as to achieve the optimization of the allocation of resources for investigative information and solve the problems in the investigation process. The public security organs need to keep abreast of the times, change their own thinking concepts, and promote the use of blockchain technology in the investigation work. So that the blockchain technology can be applied in the process of combating cross-border telecommunication fraud and achieve more results. This article adopts the method of qualitative analysis to combat cross-border telecommunication network fraud as the

44 Anand Karambe, "Blockchain-Based Approach for Tracking Global Criminals," *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT* 07, no. 06 (June 12, 2023), https://doi.org/10.55041/IJSREM19377.

45 David Wood, "A Future History of International Blockchain Standards," *The Journal of the British Blockchain Association* 1, no. 1 (July 4, 2018): 1–10, https://doi.org/10.31585/jbba-1-1-(11)2018.

46 Rameshwar Dubey et al., "Blockchain Technology for Enhancing Swift-Trust, Collaboration and Resilience within a Humanitarian Supply Chain Setting," *International Journal of Production Research* 58, no. 11 (June 2, 2020): 3381–98, https://doi.org/10.1080/00207543.2020.1722860.

core of the relevant research, to explore the concept of cross-border telecommunication fraud, as well as the predicament faced in the process of combating. By studying the technical characteristics of blockchain, it elaborates on the countermeasures to combat cross-border telecommunication network fraud, and explores the feasible application scenarios of blockchain in combating cross-border telecommunication network fraud from the perspectives of strengthening the protection of personal information, constructing the fund flow supervision system, blockchain investigation record system, and the cross-border judicial collaboration system, and so on. With the help of blockchain technology, it promotes the modernization and intelligence of the investigation mode.

ACKNOWLEDGEMENTS

First of all, I would like to thank Prof. Ramalinggam Rajamanickam, Prof. Nazura Abdul Manap and Dr. Mohd Zamre Mohd Zahir for their guidance and advice while writing this article. Secondly, I would also like to thank the University Library for providing me with a wealth of study materials and a comfortable study environment where I could concentrate on my research. I would like to thank all the scholars and seniors in the related fields whose experience and research have provided me with good reference value.

REFERENCES

Ba, Shusong, Wei Wei, and Haifeng Bai. "From Data Driven to Embedded Supervision: Prospects of Financial Supervision Based on Blockchain." *Journal of Shandong University (Philosophy and Social Sciences)*, no. 4 (2020): 161–73.

Badhani, Neelam, and Sachin Sharma. "Blockchain-Based Financial Enterprises Credit Value Information System Using Federated AI." In *2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, 1–7. IEEE, 2023. https://doi.org/10.1109/ICBDS58040.2023.10346298.

Balatska, Valeriia, and Ivan Opirskyy. "ENSURING THE CONFIDENTIALITY OF PERSONAL DATA AND SUPPORTING CYBER SECURITY WITH THE HELP OF BLOCKCHAIN." *Cybersecurity: Education, Science, Technique* 4, no. 20 (2023): 6–19. https://doi.org/10.28925/2663-4023.2023.20.619.

Br□vers, Aleksandrs. "UNDERSTANDING OF ELECTRONIC EVIDENCE, ITS ACQUISITION AND STRENGTHENING IN CRIMINAL PROCEEDINGS." *INDIVIDUAL. SOCIETY. STATE. Proceedings of the International Student and Teacher Scientific and Practical Conference*, January 11, 2023, 156–62. https://doi.org/10.17770/iss2021.6913.

Chen, Longxi. "Research on China's International Investigative Co-Operation." Doctoral dissertation, East China University of Political Science and Law, 2011.

Chen, Peixin. "Cloud Forensics Solution Based on Blockchain." *Network Security Technology & Application*, no. 3 (2024): 124–26. https://doi.org/10.3969/j.issn.1009-6833.2024.03.046.

D, Subiramaniyan S, Mohamed Fayas M P, Selva Bharathi S M, Sasikala K, R. Reshma, and S. P. Sasirekha. "A Novel Decentralized Product Verification Using Blockchain Technology." In *2023 7th International Conference on Trends in Electronics*

and Informatics (ICOEI), 642–46. IEEE, 2023. https://doi.org/10.1109/ICOEI56765.2023.10125833.

Dubey, Rameshwar, Angappa Gunasekaran, David J. Bryde, Yogesh K. Dwivedi, and Thanos Papadopoulos. "Blockchain Technology for Enhancing Swift-Trust, Collaboration and Resilience within a Humanitarian Supply Chain Setting." *International Journal of Production Research* 58, no. 11 (June 2, 2020): 3381–98. https://doi.org/10.1080/00207543.2020.1722860.

Flora, Henny Saida. "Criminal Sanctions toward False Criminal Actors through the Internet." *The International Journal of Humanities & Social Studies* 7, no. 9 (September 30, 2019). https://doi.org/10.24940/theijhss/2019/v7/i9/HS1909-081.

Gupta, Suyash, and Mohammad Sadoghi. "Blockchain Transaction Processing." In *Encyclopedia of Big Data Technologies*, 366–76. Cham: Springer International Publishing, 2019. https://doi.org/10.1007/978-3-319-77525-8_333.

Hou, Zhi, Jie Yang, Xiangjun Feng, and Xiaomei Liu. "Research on the Dilemma View and Practical Response of Crime of Telecommunication Network Fraud——Take 137 Cases as Breakthrough." *Tianjin Legal Science* 34, no. 2 (August 16, 2018): 83–89.

Huang, Zicheng. "Research on International Co-Operation in Combating Transnational Telecommunication Network Fraud Offences in the Lancang Subregion." *Network Security Technology & Application*, no. 2 (2022): 160–62. https://doi.org/10.3969/j.issn.1009-6833.2022.02.094.

Jiang, Xiaotian, and Man Liu. "Interview with Zhang Xiaojin, Director of the Fourth Procuratorial Department of the Supreme People's Procuratorate: The Cross-Borderisation of Wire Fraud Crimes, with a Focus on Criminal Syndicates and the Masterminds behind Them." Southern Metropolis Daily, May 4, 2024. https://www.spp.gov.cn/spp/zdgz/202403/t20240304_647113.shtml.

Kang, Xinjian. "Research on the Investigation and Prevention of Cross-Border Telecom Fraud in Yunnan Border Area in the Era of Big Data." *The Journal of Yunnan Police College*, no. 1 (2020): 92–97. https://doi.org/10.3969/j.issn.1672-6057.2020.01.017.

Kang, Zehua. "Research on the Application of Blockchain in Smart Policing." *Legal and Economy*, no. 7 (September 15, 2020): 160–62. https://doi.org/10.3969/j.issn.1005-0183.2020.07.066.

Karambe, Anand. "Blockchain-Based Approach for Tracking Global Criminals." *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT* 07, no. 06 (June 12, 2023). https://doi.org/10.55041/IJSREM19377.

———."Blockchain-Based Approach for Tracking Global Criminals." *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT* 07, no. 06 (June 12, 2023). https://doi.org/10.55041/IJSREM19377.

Khramtcov, Evgenii. "Optimization of Criminal Procedure Legislation in the Field of

Evidence in Criminal Cases on Crimes against Property Committed Using Information and Telecommunication Technologies." *Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia* 2022, no. 2 (July 6, 2022): 239–43. https://doi.org/10.36511/2078-5356-2022-2-239-243.

Li, Xinmin. "Research on the Development and Countermeasures of Cross-Border Crime of Telecom and Online Fraud." *Journal of Western*, no. 1 (2024): 78–81.

Liu, AiJiao. "The Strategy of Fighting for the Telecommunications Fraud with I Iternational Police Cooperation." In *Proceedings of the 2016 4th International Conference on Management, Education, Information and Control (MEICI 2016)*. Paris, France: Atlantis Press, 2016. https://doi.org/10.2991/meici-16.2016.19.

Liu, Cheng-Yong, Tian-Yu Dong, and Ling-Xing Meng. "Cross-Border Credit Information Sharing Mechanism and Legal Countermeasures Based on Blockchain 3.0." *Mobile Information Systems* 2022 (July 1, 2022): 1–12. https://doi.org/10.1155/2022/6972647.

Liu, Pinxin. *Dianzi Zhengjufa*. 1st ed. Beijing: China Renmin University Press, 2021.

———. "On the Institutional Value of Electronic Data's Storage and Authentication Based on Blockchain." *Archives Science Bulletin*, no. 1 (2020): 21–30.

Lou, Yongtao, and Tang Xiang. "The Prevention, Control and Reflection of Telecom Network Fraud Crime in the Big-Data Age." *Journal of Chongqing University of Technology (Social Science)*, no. 3 (2020): 121–28.

Ma, Zhonghong. "The Difficulties and Countermeasures about the Investigation of the New Network Crimes Taking Telecommunications Fraud as the Representativesed——Research Based on W Survey." *Journal of People's Public Security University of China: Social Sciences Edition*, no. 3 (2018): 78–86.

Mikhaylov, Alexander, and Richard Frank. "Cards, Money and Two Hacking Forums: An Analysis of Online Money Laundering Schemes." In *2016 European Intelligence and Security Informatics Conference (EISIC)*, 80–83. IEEE, 2016. https://doi.org/10.1109/EISIC.2016.021.

Pan, Fei, and Chang Liu. "Governance and Prevention of Telecommunication Network Frauds." *Journal of Guangxi Police College* 32, no. 5 (2019): 48–52. https://doi.org/10.19736/j.cnki.gxjcxyxb.2019.0509.

Petrovi□, Dragana B. "PRIVACY AND PROTECTION OF PERSONAL DATA – CRIMINAL LAW ASPECT." *Strani Pravni Život* 66, no. 4 (January 26, 2023): 469–89. https://doi.org/10.56461/SPZ_22407KJ.

Pham, Van-Duy, Canh-Tuan Tran, Thang Nguyen, Tien-Thao Nguyen, Ba-Lam Do, Thanh-Chung Dao, and Binh Minh Nguyen. "B-Box - A Decentralized Storage System Using IPFS, Attributed-Based Encryption, and Blockchain." In *2020 RIVF International Conference on Computing and Communication Technologies (RIVF)*, 1–6. IEEE, 2020. https://doi.org/10.1109/RIVF48685.2020.9140747.

Puluhulawa, Fenty Usman, Jufryanto Puluhulawa, and Moh. Gufran Katili. "Legal Weak Protection of Personal Data in the 4.0 Industrial Revolution Era." *Jambura*

Law Review 2, no. 2 (June 20, 2020): 182–200. https://doi.org/10.33756/jlr.v2i2.6847.

Qiu, Shuxiang, and Haobo Jin. "Synthetic Investigative Intelligence Management with the Application of Blockchain Technology." *Journal of Zhejiang Police College*, no. 4 (2018): 28–34. https://doi.org/10.3969/j.issn.1674-3040.2018.04.005.

Russkevich, E. A. "Personal Data in the Mechanism of Criminal Law Protection." *Proceedings of Southwest State University. Series: History and Law* 13, no. 5 (December 5, 2023): 75–86. https://doi.org/10.21869/2223-1501-2023-13-5-75-86.

Saito, Kenji, and Hiroyuki Yamada. "What's So Different about Blockchain? — Blockchain Is a Probabilistic State Machine." In *2016 IEEE 36th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, 168–75. IEEE, 2016. https://doi.org/10.1109/ICDCSW.2016.28.

Stephen, Remya, and Aneena Alex. "A Review on BlockChain Security." *IOP Conference Series: Materials Science and Engineering* 396 (August 29, 2018): 012030. https://doi.org/10.1088/1757-899X/396/1/012030.

Susilawati, Ika Yuliana. "PERAMPASAN ASET HASIL TINDAK PIDANA KORUPSI DI LUAR NEGERI MELALUI BANTUAN TIMBAL BALIK (MUTUAL LEGAL ASSISTANCE)." *Jurnal IUS Kajian Hukum Dan Keadilan* 4, no. 2 (2016): 138–51. https://doi.org/10.12345/ius.v4i2.281.

Tanković, Ana Čuić, Marina Perišić Prodan, and Dragan Benazić. "Consumer Segments in Blockchain Technology Adoption." *South East European Journal of Economics and Business* 18, no. 2 (December 1, 2023): 162–72. https://doi.org/10.2478/jeb-2023-0025.

Wanhua, Luo. "Research and Application of Blockchain Technology in Transportation Administrative Law Enforcement." In *2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC)*, 766–70. IEEE, 2020. https://doi.org/10.1109/ITOEC49072.2020.9141836.

Wood, David. "A Future History of International Blockchain Standards." *The Journal of the British Blockchain Association* 1, no. 1 (July 4, 2018): 1–10. https://doi.org/10.31585/jbba-1-1-(11)2018.

Wright, Craig S. "Bitcoin: A Peer-to-Peer Electronic Cash System." *SSRN Electronic Journal*, 2008. https://doi.org/10.2139/ssrn.3440802.

Wu, Chengjie, and Wen Chen. "Discussion on Difficult Issues in Telecommunication Network Fraud Cases." *Journal of Law Application*, no. 21 (2017): 40–50.

Wu, Zhiting, and Shiyong Zhi. "Characteristics of Telecom Network Fraud Crime and Prevention and Control Measures." *Journal of Hebei University of Economics and Business(Comprehensive Edition)* 21, no. 2 (2021): 77–81. https://doi.org/10.3969/j.issn.1673-1573.2021.02.013.

Xiao, Tongyu. "Discussion on the Investigation Dilemma and Countermeasures of Telecommunication Fraud Cases." *Network Security Technology & Application*, no. 1 (2023): 131–33. https://doi.org/10.3969/j.issn.1009-6833.2023.01.064.

Xie, Ling. "Research on Information Investigation of Telecom Network Fraud." *Journal of People's Public Security University of China (Science and Technology)* 26, no. 3 (2020): 85–93. https://doi.org/10.3969/j.issn.1007-1784.2020.03.013.

Xiong, Jun, and Li Li. "The Trial-Centred Perspective of Telecommunication Network Fraud Crime Investigation and Evidence Collection Path." *Legal System and Society*, no. 31 (2020): 23–24. https://doi.org/10.19387/j.cnki.1009-0592.2020.11.012.

Yang, Liu. "On the Forensics of Cross-Border Telecom Network Fraud Crime--Taking Southeast Asian Countries as the Object of Analysis." *Journal of Political Science and Law*, no. 6 (2023): 5–11.

Zheng, Zibin, Shaoan Xie, Hong Ning Dai, Xiangping Chen, and Huaimin Wang. "Blockchain Challenges and Opportunities: A Survey." *International Journal of Web and Grid Services* 14, no. 4 (2018): 352–75. https://doi.org/10.1504/IJWGS.2018.095647.