Journal of Research in Science and Engineering (JRSE)
ISSN: 1656-1996 Volume-4, Issue-6, June 2022
DOI: 10.53469/jrse.2022.04(06).06

Exploring the Applicability of Blockchain Technology in the Judicial Deposit of Electronic Evidence

Bo Zhang

Hainan Vocational College of Political Science and Law

Abstract: ***In the era of electronic data, the form of evidence in the judicial evidence chain is also increasingly iterative, and at this stage electronic evidence has become a form of evidence that cannot be ignored. The storage, inspection, authentication and analysis of electronic evidence are all possible to be tampered with. The main feature of Blockchain technology is tamper-proof, which realizes the verification needs of electronic evidence itself at the technical level, ensures data authenticity and completes the tasks of electronic evidence in the judicial appraisal process more efficiently.***

Keywords: Electronic data, Blockchain, Judicial deposition**.**

1. Introduction

With the digital development of electronic information, electronic data has become an important part of the evidence to replace the traditional meaning of the judicial appraisal or criminal technical investigation of electronic evidence in the activities of the world is increasingly prominent, electronic evidence has become an indispensable part of the evidence system of public security, prosecution, law and other departments. Begin to enter the “electronic proof of the era”. Today, electronic evidence in the litigation law is classified as a single piece of evidence, the status of the case in the exponential increase year by year. Using electronic evidence as a keyword, we searched the Chinese Judicial Documents website and found that.

During the decade from 2012 to 2021, the volume of relevant case data climbed year by year, including 51.22% and 65.75% year-on-year growth in 2017 and 2018, respectively. Since the era of physical evidence “scientific evidence” has become the basis for objective determination of the case, which in terms of technological content, whether in breadth or depth, electronic evidence is greatly exceeded the level of general physical evidence.

Now according to the Blockchain technology of medical, financial, file management and other fields of research has emerged, between the public prosecution and justice related evidence, there is a certain sensitivity, so the judicial deposition of Blockchain technology has not been fully developed, the research can not only promote the theoretical development of electronic evidence forensic related fields, but also even further for the efficient application of electronic evidence to clear the obstacles, greatly enhance the value and use of Blockchain electronic evidence space, can play a greater role in the public prosecution and justice in the field of electronic evidence.

2. The Development Status of Electronic Evidence

The positioning of electronic data in litigation has been clarified with the actual needs. In the early work, most of the electronic data were transformed into documentary evidence or recognized as other forms of evidence such as audio-visual materials for litigation. First, converting electronic data into documentary evidence is a way to undermine the probative value of electronic data. Electronic data itself is fallible, easily tampered with, and easily destroyed. In many cases, the original electronic data already has errors, and because the documentary evidence cannot fully reflect the content of the original electronic data, storage methods and other key features, increasing the electronic data is not recognized as no valid evidence.

Second, because the coverage and expansion of electronic data with the continuous development of information technology and gradually expand, has long exceeded the scope of audiovisual data, it is not appropriate to identify electronic data through the identification of audiovisual data. Species gradually becomes stronger. The formulation of electronic data-related procedural rules has undergone a transformation from principle-based provisions to detailed provisions, gradually refined from vague programmatic provisions to operational and reference industry standards, and continuously improved with the development of technology. At the same time can adapt to the needs of current legal practice, keep pace with the times, so that judicial personnel have the law to follow.

3. Electronic Evidence Judicial Process

Electronic evidence in China’s legislation, after gradually improving the construction of mechanisms, has achieved a legal status. At this stage has begun to intervene in the formal judicial case process on a large scale, playing an unprecedented role in a wider and wider range of cases, and the data of the judicial appraisal center in recent years shows that electronic evidence identified more and more demand. The reason why Blockchain technology is chosen is that through Blockchain technology, case files, evidence deposition system in the business collaboration platform with mutual trust identity, mutual trust time, mutual trust environment, mutual trust technology, etc. for the business critical process of fair, fair and open records, forming a platform for the complete evidence chain, the whole process is traceable, auditable and non-tamperable to ensure that electronic evidence, electronic files, electronic archives Electronic data, such as electronic evidence, electronic files, electronic archives, in the collection, transmission, storage, flow and other processes of the real and credible, to achieve anti-tampering, anti-repudiation and other functions. Electronic evidence forensic process, as shown in Figure 1.

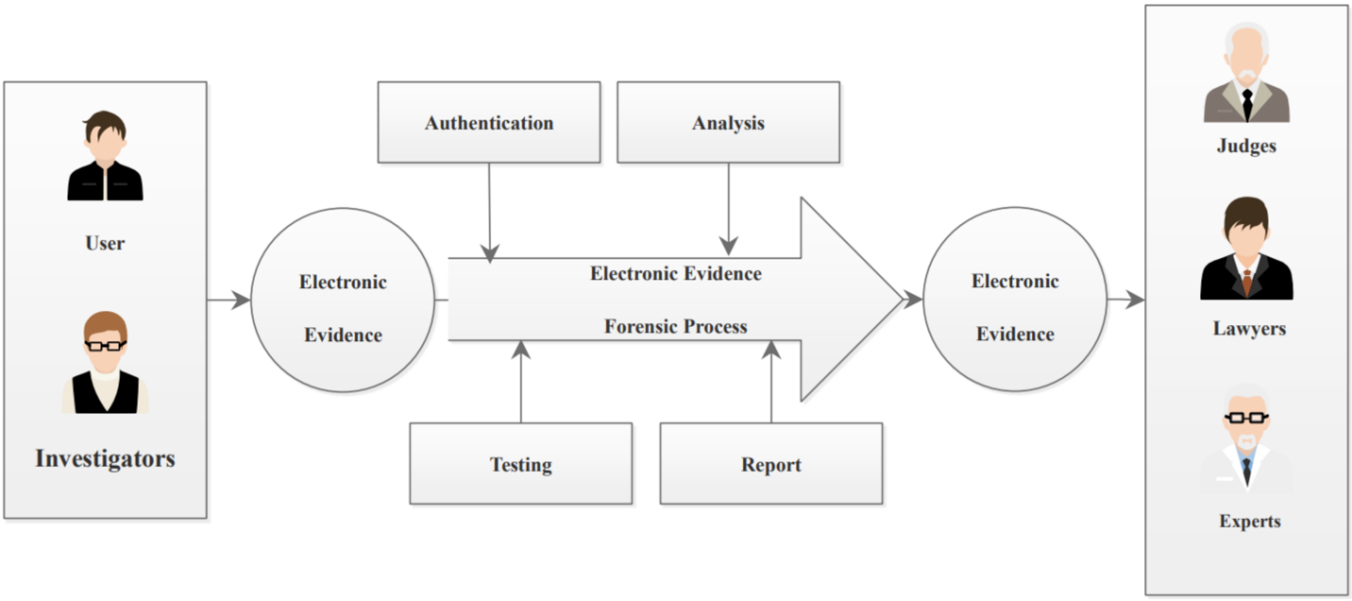

Figure 1: Electronic evidence judicial appraisal process

4. The Existence of Electronic Evidence Problems

At present, the relevant public prosecutors, judges and other units in the regulations, or in the law, judicial interpretation and other content, domestic and foreign electronic evidence of the scope, the original form, means of forensics, etc. have made some relevant provisions, but the provisions set generally not comprehensive nor can be effectively implemented. And electronic evidence in the actual operation of various departments, for example, in the specific evidence storage links, evidence collection links, evidence presentation links, evidence burden, evidence identification and other links, there are still obvious pain points. As electronic data has the characteristics of large data volume, real-time, reliance on electronic media, easy to tamper, easy to lose, etc., it is difficult to have standardized means to solve the above-mentioned evidence storage problems. The following key issues exist at this stage.

4.1 Electronic Evidence Authenticity Proof is Difficult

For example, the authenticity of the evidence can not be copied: some locally generated electronic data for forensics, the original can only be saved in the generation of electronic data equipment, and the original evidence and equipment are inseparable. Once the original evidence leaves the device, it becomes a copy and cannot be used as a basis for judgment.

Therefore, it is necessary to study a set of case files and evidence retention system to ensure that the whole process is traceable, audible, and untamperable, and to ensure the transmission of electronic data such as electronic evidence, electronic files, and electronic archives. authenticity and credibility of the stored and circulated information, and to achieve anti-tampering and anti-repudiation functions. Electronic data storage is a potentially important application area of Blockchain technology, and the combination of Blockchain and electronic data storage can reduce the cost of electronic data storage, facilitate the identification of electronic data evidence, and improve the evidence storage capacity of various political and legal departments.

4.2 Electronic Data is Easy to be Tampered with and Difficult to be Evidenced

Electronic evidence or digital case materials, the biggest problem is that electronic data is easy to be tampered with, whether it is documents, pictures or audio and video, modify are very easy to do, which is usually the case, offline to the forensic appraisal, notary and other relevant institutions to issue electronic data related to the certification of documents, notary or forensic institutions are generally required to provide the original proof of the underlying cause.

Data easy to lose difficult to forensics, according to the traditional way, usually in the event of legal disputes to retrieve electronic data, but many times, the original data will appear lost and inaccessible. Such as WeChat chat records, especially the pictures in WeChat, often over time will not be able to access; and then WeChat group, QQ group was kicked out of the group we can no longer get the original chat records in the group; if there is a third-party platform or storage media (CD, U disk, hard disk) data, will be due to rent storage space due to clean up, media damage, or manually deleted by mistake can easily cause data loss. Data migration, transfer, and misuse by others can also easily cause data tampering.

The original proof is difficult to obtain, in the Supreme Court provisions of Article 15 clearly states: the parties to electronic data as evidence, should provide the original. The original proof is a necessary condition for electronic data as evidence, but in many cases it is difficult to produce effective proof of the original, especially if there has been a data transfer or data re-deposit. If the original data is generated on a third-party platform, you need to contact the platform to obtain the original proof, which depends on the platform’s operating mechanism. If the originals are in the hands of the other party in a legal dispute, the helpless situation of difficulty in obtaining proof of originals may also occur[4].

4.3 Information Security is Difficult to Ensure Low Credibility

Some of the traditional data sharing platforms established by the relevant units of advanced public prosecution, law and justice are using centralized storage of special data, and there is no way to prevent external or internal factors from tampering with the existing data, which makes the credibility of judicial data submitted across departments doubtful. In addition, the centralized storage method is an easy target for hackers, making it difficult to ensure data security. Departmental compartmentalization makes system duplication serious. Moreover, the premise of ensuring security to keep the data of each system separately, its need to invest huge hardware and software, with the addition of intrusion detection and other system protection, the cost increases while increasing the difficulty of operation.

Lack of trust in information sharing, reluctance to share between judicial departments, and fear of responsibility due to the potential hidden dangers of information sharing security issues, many departments are afraid to share among themselves, resulting in a low level of information sharing. At present, the domestic research platforms for Blockchain deposition include Tianping chain, Huayu chain, Guangzhou Netcom law chain, Yangtze River Delta judicial chain, etc. The current Blockchain for judicial applications is mainly developed by third-party companies, with relatively independent systems and difficult business collaboration, and the deposition and proof itself is a process that requires the collaboration of multiple departments of politics and law[5].

Traditional judicial systems are built according to the corresponding policy standards of their respective departments, and the lack of coordinated deployment at the digital information level in a consistent pace leads to easy conflicts in the execution of affairs between departments; in addition, although the government system has improved the efficiency to a certain extent, even if the conditions are met, it still relies on manual processing of a large number of transactional work, and there is no way to automatically execute business and thus improve efficiency. Duplicate construction of systems and duplicate data entry also lead to difficulties in connecting information sharing channels. It is difficult to integrate each system in each department using independent databases; it is difficult to converge systems across cities, provinces and departments; and it is even more difficult to retrieve because of the massive amount of information stored centrally.

For example, population information system, ID card information system, information system for criminal offenders, information system for people at large, and anti-drug information system require that the information must be accurate and can be used as a judicial basis, but at present, problems such as incorrect identity information, multiple identities of a person, and inaccurate information on case records are widespread, and information errors are almost inevitable due to human or error, in addition, the people’s Some personal identity information collected and stored in the public security department is not shared with other departments, or is not updated and stored in a timely manner, resulting in the people still need to issue various certificates when handling business in the relevant departments, making the accuracy, real-time, and consistency of electronic data poor.

4.4 The Existing Approach is Costly and Difficult

To solve the above problems, at this stage there are also some solutions, such as the early issuance of proof of documents is an effective way to solve the data can not be obtained in a timely manner, but in the actual case investigation or identification process the feasibility of this method is very low, the main reason is that in all electronic data storage, there is a dispute is, after all, a small number of cases, advance pre-judgment to ensure that all the data to issue proof of documents is too costly Moreover, the proof instruments need to go to the notary or forensic institutions to open, which requires a lot of time and effort, in addition, the original proof still need to provide, if the third-party platform to open, the difficulty of its issuance has not been reduced.

In general, research in independent business systems existing electronic evidence forensic research is mainly immature in application, and relatively little research is invested in the theory and application of Blockchain. There are such as electronic data easily tampered with, data easy to lose difficult to forensics, information security is difficult to ensure; original proof is difficult to obtain, the feasibility of advance notarization is low; information accuracy, real-time, consistency is poor; judicial business synergy efficiency is low, the communication between the departments of mutual trust is difficult and a series of problems.

5. The Blockchain Technology Applicability Analysis

5.1 For the Pain Points of Electronic Evidence

For the above analysis of the problems and pain points of electronic data, combined with the essential characteristics of Blockchain technology, from the following aspects.

1) To solve the problem of easy data tampering and loss in the judicial appraisal of electronic evidence, it is proposed to propose asymmetric encryption algorithms and hash algorithms with a trusted execution environment to reduce the redundancy between data and improve the security of data. Based on the SGX executable environment and the commonly used K-mean algorithm, it is proposed to derive the mathematical models of asymmetric encryption algorithm and hash algorithm with matrix parametric regularization and design efficient algorithms to solve the corresponding security optimization problems.

2) In order to solve the Blockchain multi-source electronic evidence forensic fusion problem, it is proposed to propose a multi-core Blockchain data fusion approximation algorithm based on deep neural network to enhance mutual trust among business systems. Based on the commonly used deep learning network, it is proposed to derive the mathematical model of

Blockchain multi-source electronic evidence fusion algorithm and analyze its characteristics, and design an efficient algorithm to solve the corresponding system data fusion optimization problem.

3) To solve the robustness problem of Blockchain multi-source electronic data forensic fusion based on the spatio-temporal correlation of the kernel matrix (similarity matrix), it is proposed to theoretically elaborate the impact of the spatio-temporal variation of the kernel matrix on the performance of Blockchain multi-source electronic data fusion to ensure the real-time and consistency of the model[6].

5.2 Constructing A Complete System Model

The Blockchain key technology-based electronic evidence forensic model is constructed, by which the Blockchain network's electronic evidence forensic fusion system is designed step by step to ensure that the system's has the ability of efficient, secure, real-time, and scalable processing. In order to achieve the purpose of solving practical problems, it is necessary to systematically analyze the information of electronic evidence type elements in the Blockchain network environment, base on the process of judicial appraisal, propose rigorous feature selection means and methods, study the spatial and temporal characteristics of Blockchain network electronic evidence judicial appraisal, and establish a multi-level and multi-scale Blockchain feature electronic evidence judicial appraisal model based on spatial and temporal correlation. The hierarchical structure is shown in Figure 2.

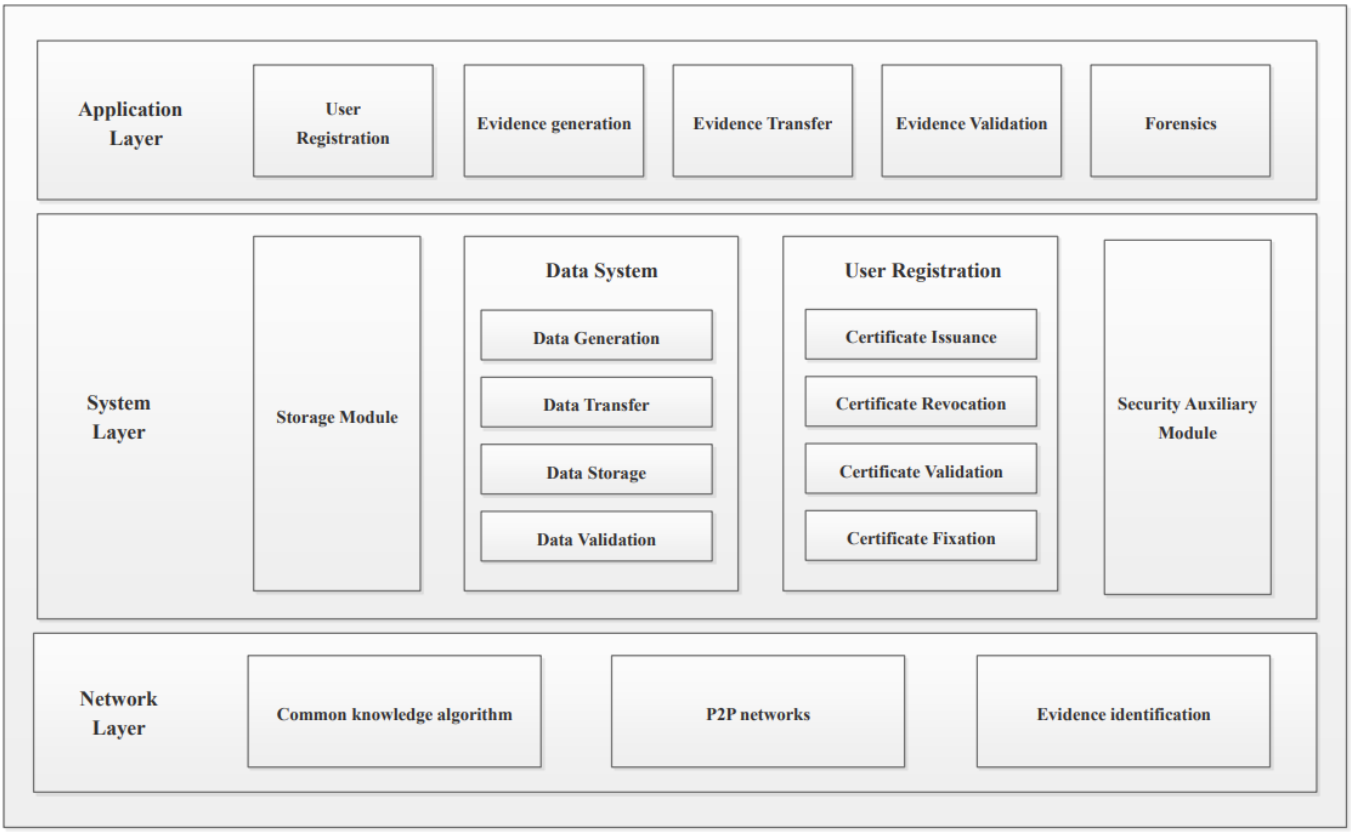

Figure 2: Multi-level multi-scale Blockchain feature electronic evidence forensic appraisal model

5.3 Scientific Problems to be Solved

In order to ensure the effective application of Blockchain technology in the judicial deposition of electronic evidence, so that the existing Blockchain technology means applied in other fields can be more applicable to the link of judicial deposition, the specific key scientific issues that need to be solved are as follows.

1) In the Blockchain multi-source electronic data forensic fusion, how to design the regularization term to make the selected electronic data have less redundancy and higher security trustworthy execution environment between.

2) When dealing with Blockchain multi-source electronic evidence forensic fusion problem, how to design the objective function so that the Blockchain electronic evidence can be better applied to the network trained from the down-sampled data.

3) Analyzing the properties of the optimization problems corresponding to Blockchain multi-source e-evidence forensic fusion algorithms with matrix parametric regularization and Blockchain multi-source e-evidence forensic fusion approximation algorithms based on deep neural networks, and designing efficient algorithms to solve them.

4) Defining suitable metrics to analyze the robustness and consistency of the temporal variation of electronic data on Blockchain data fusion results.

The next step is to design a novel set of efficient algorithms for Blockchain multi-source data fusion with correlation among electronic data, combining the hierarchy of existing models, supported by the already existing relevant technologies, to effectively deal with the series of problems of isolation, easy tampering, and poor consistency of electronic data or electronic evidence itself[7]. The key scientific issues are used as refined implementation targets to break the technical barriers one by one.

6. Conclusion

In line with Moore’s law of the rapid development of electronic data informatization today, Blockchain technology has been integrated into various industries, existing such as medical, financial, human resources, archives management and other various industry sectors, but instead, it is not properly applied in the relevant fields such as public prosecution and justice where evidence is king. Although there is a small amount of research in theoretical or practical application of electronic evidence forensics, but again, it does not adequately address the problems of electronic evidence, and does not reasonably integrate the technical advantages of Blockchain technology into electronic evidence.

This paper intends to analyze the method of Blockchain-based electronic evidence forensic appraisal, use such as asymmetric encryption and redundant distributed storage to achieve information tamper-proof, use chain data structure to achieve data information traceability, through distributed data storage, peer-to-peer transmission, consensus mechanism, encryption algorithms to ensure the trustworthiness of forensic evidence and other more mature Blockchain technology features at this stage, analyze the applicability of Blockchain technology in solving the judicial deposit of electronic data, and research concludes that Blockchain technology fusion electronic evidence can better solve the problems of mutual trust and tamper-proof of business sector evidence, so as to improve the efficiency and fairness of judicial trial.

References

[1] Cao Ruolin. Thinking on the civil evidence law of Blockchain evidence storage technology[J]. Legal System and Economics, 2021, 30(07): 26-32.

[2] Ruan Xiao, Wang Yue. The application status and rule exploration of Blockchain evidence[J]. Journal of Guiyang University (Social Science Edition), 2021, 16(05): 51-55.

[3] Li Jingjing. Analysis on the technical characteristics and judicial practice optimization of the Blockchain certificate deposit system[J]. Journal of Shangqiu Vocational and Technical College, 2021, 20(03): 22-28.

[4] Mai Xiaoyu. Distributed accounting and Blockchain technology in financial accounting[J]. Journal of Physics: Conference Series, 2021, 1881(2).

[5] Manish Verma. Credible and non-corruptible supply chain management using Blockchain technology[J]. Journal of Trend in Scientific Research and Development, 2021, 5(3).

[6] Shi Guanbin, Chen Quanzhen. On the advantages and judicial review paths of electronic data stored in Blockchain[J]. Journal of Southwest University for Nationalities (Humanities and Social Sciences Edition), 2021, 42(01): 67-73.

[7] Zheng Yujie, Fong BOH Wai. Value drivers of Blockchain technology: A case study of Blockchain-enabled online community[J]. Telematics and Informatics, 2021(prepublish).

[8] Bai Xuetong, Wang Qiuyun, Chen Ying. Application Research of electronic evidence platform based on Blockchain technology[J]. Cyberspace Security, 2020, 11(10): 104-109.

[9] Jin Du, Liping Ding, Guangxuan Chen. Research on the rules of electronic evidence in Chinese criminal proceedings[J]. International Journal of Digital Crime and Forensics (IJDCF), 2020, 12(3).

[10] A.S. Aleksandrov, A.A. Yunusov, N.N. Rybushkin. Current legal organization of judicial evidence and “independent, objective” judges[J]. Uchenye Zapiski Kazanskogo Universiteta Seriya Gumanitarnye Nauki, 2020, 162(2).

[11] Shijie Chen, Chengqiang Zhao, Lingling Huang, Jing Yuan, Mingzhe Liu. Study and implementation on the application of Blockchain in electronic evidence generation[J]. Forensic Science International: Digital Investigation, 2020, 35.

[12] Jong-Min Sin, Hye-Ryon Son. Dealing with the problem of collection and analysis of electronic evidence[J]. Int. J. of Electronic Security and Digital Forensics, 2019, 11(3).

[13] Baek Jae Hyeon. The limitation of search and seizure of electronic evidence under existing legislation &amp; a scheme for improvement[J]. The Journal of Legal Studies, 2019, 27(1).

[14] R Borges Blázquez. Electronic evidence in criminal procedure and probative value of conversations maintained through instant messaging third party programs[J]. Revista Boliviana de Derecho, 2018, s/v(25).

[15] --. About the normative and tendentiously binding nature of the rules of sound criticism in the weighing of judicial evidence[J]. Revista de derecho (Valparaíso), 2018, s/v(50).