

Blockchain Depository Technology in Litigation Activities

-- Introduction with the Way of Defending the Right in the Case of Network Infringement

Yueyao Feng *

School of Humanities and Development, China Agriculture University, Beijing, China

* Corresponding Author Email: 15647932324@163.com

Abstract. The development of the Internet has made the dissemination of information on the Internet much faster than before, and consequently caused the occurrence of cyber violence. In this series of events, the difficulty of the parties to defend their rights is regarded as a very prominent problem. A large part of the difficulty in defending the rights of the parties concerned is due to the difficulty in collecting evidence. According to the principle of "whoever claims, whoever produces evidence", the infringer needs to bear the unfavorable consequences of proof, thus making it difficult for infringers to defend their legitimate rights and interests in cyber violence infringement cases. With the development of blockchain technology, the problem of traditional electronic data forensics will be solved by blockchain technology. This paper will take the main logic of how blockchain evidence solves the dilemma of applying traditional electronic data in litigation activities, and take the way of defending rights in network infringement cases as the entry point to elaborate the application of blockchain deposit technology in litigation activities.

Keywords: Electronic Data; Online Infringement Incidents; Ways to Defend Rights; Blockchain Deposits.

1. Introduction

In recent years, with the popularization and development of the Internet, incidents of cyber-violence have occurred frequently. 15-year-old Liu Mouzhou chose to kill himself in Sanya after a successful search for his family, due to cyber-violence because of the conflict with his biological parents. 24-year-old prospective postgraduate student Zheng Mouhua suffered cyber-violence because of a head of powdered hair, and ultimately committed suicide after a depressive episode. The mother of a child who was run over in a school in Wuhan was criticized by netizens for wearing overalls while rushing to school, and eventually chose to end her young life. The dead can't come back to life. However, in the face of a series of cyber violence infringement incidents, public opinion only saw the side of the victim to be pitied, the abuser as the infringer is hidden behind the network mask, tap the delete button can cover up their own crimes. These abusers hold the law is not responsible for the fluke, the use of network violence, low cost, difficult to obtain evidence and other characteristics, wantonly trample on the legitimate rights and interests of others, but in the use of the keyboard indirectly "take" another person's life, and still get away with it. The reason for the existence of this persistent problem is one of the symptoms of the judicial authorities' difficulties in applying traditional electronic data.

2. Dilemmas in the Application of Traditional Electronic Data

Blockchain forensics is a combination of blockchain technology and traditional evidence (mainly electronic data evidence) and does not constitute a new type of evidence. Blockchain technology can be a good solution to the problem of electronic data evidence being restricted from use in litigation activities due to traditional technology. There are a series of limitations on traditional electronic data in terms of depositing, obtaining, adducing and validity of evidence.

2.1. Deposit of Traditional Electronic Data

The deposit of electronic data has the characteristic of centralization, whether it is a third-party deposit, notary public deposit or local deposit is faced with the problem of one party controlling the content of the deposit with the help of cell phones, computers or other electronic devices. [1] In the unilateral centralized depository mode, on the one hand, due to the lack of external supervision, the depository subject can be tampered with the evidence without being detected, resulting in the loss of electronic evidence of its authenticity; on the other hand, a single depository equipment, once a network attack, system failure, or equipment failure, destruction and loss and other unforeseen circumstances will lead to the tampering and loss of electronic data. This consequence is often irreversible, to the storage of electronic data has caused great security risks.

2.2. Traditional Electronic Data Forensics

At present, China's judicial interpretation of electronic data forensics means of provisions can be summarized as follows nine: 1, seizure, sealing of the original storage media; 2, on-site extraction of electronic data; 3, the network online extraction of electronic data; 4, freezing of electronic data; 5, access to electronic data; 6, book-type fixation; 7, photographs and video cameras; 8, copying and reproduction; 9, entrusted to the analysis of [2]. Among them, the seizure of the original carrier of electronic data is often first adopted by the judicial organs in practice. From the above nine forensic methods, we can see that the current forensics for electronic data evidence is more of the data stored in the electronic media for documentary or physical evidence processing. Based on the traditional electronic data centralized storage mode, in the forensics of locally produced electronic data, due to the original can only be retained in the production of electronic data in the equipment, so the need to store the data of the original equipment for seizure, sealing, which will cause inconvenience to the parties to the normal work, life. Moreover, the electronic data through snapshots, printing, justice and other ways to paper processing, will also increase the party's time and capital costs, thus hindering the improvement of litigation efficiency. After transforming electronic data into documentary evidence, the flexibility of electronic evidence will be lost, and then lose its unique existence value. In addition, in the case of network violence infringement, for example, many infringement evidence is stored in the infringer's mobile device and the backend of the Internet operating vendors, which belongs to the category of electronic data. Unlike the judicial organs, as ordinary citizens, the infringer can hardly achieve the same effect of evidence collection with the traditional electronic evidence collection means.

2.3. Evidence of Traditional Electronic Data

Electronic data is stored in electronic equipment, and its content needs to be read and displayed in the courtroom, which will cause difficulties in the presentation of evidence. First of all, some of the contents of the electronic data (such as electronic signatures, time information, etc.) can not be visualized in the court; Secondly, by the parties to complete the electronic data screenshots, video and snapshots of printing and other evidence, it is difficult to verify with the original electronic data, the parties are very easy to tamper with the data, which affects the authenticity of the electronic data evidence. And in the litigation process, because both parties based on their respective positions issued by the electronic data will occur in the discrepancy between the evidence and even contradict each other, resulting in electronic data (even as the key evidence of the case) can not be used as the basis for the case, resulting in the party bearing the burden of proof to lose the case.

2.4. Effectiveness of Traditional Electronic Data Evidence

In judicial practice, the use of electronic evidence is still facing many difficulties, mainly manifested as follows: first, electronic evidence is easy to be tampered with; second, in the forensics, electronic evidence and related equipment, if the separation occurs, the effectiveness of the electronic evidence will be greatly reduced; once again, in the presentation of the evidence, it is necessary to convert the electronic evidence into documentary evidence, this operation may not only destroy the content of

the electronic data, but also the judicial determination of the Higher cost; Finally, in the evidence, due to the characteristics of electronic evidence easy to tamper with, so there will be inconsistency between the two sides of the electronic data content, resulting in the court on the authenticity of electronic evidence, relevance, legality of the determination of the three sexes has become exceptionally difficult, so that the electronic evidence to lose its original evidence of the effectiveness of the evidence.[3]

The above reasons cause electronic data, although recognized by the legislation as the statutory eight types of evidence, but in practice the chances of being admitted by the judiciary are generally not high, and the emergence of blockchain technology can effectively solve the above problems.

3. Concept and Introduction to Blockchain Forensics

3.1. What is Meant by Blockchain Technology

The so-called blockchain is a bookkeeping technology that is maintained by multiple parties and uses cryptography to ensure the security of data transmission and access, thus realizing that data can be stored consistently, difficult to tamper with and protected against repudiation, which is also known as distributed ledger technology. A typical blockchain is a "block-chain" structure for data storage. As a new computing paradigm and collaboration model to establish trust at low cost in an untrustworthy competitive environment, blockchain is changing the application scenarios and operation rules of many industries with its unique trust establishment mechanism, and is one of the indispensable technologies for the development of digital economy and the construction of a new type of trust system in China in the future. [4]The core technologies of blockchain include: consensus mechanism, storage structure, communication method, etc., which are used to guarantee the multi-party participation of blockchain, with the characteristics of difficult to tamper and difficult to lose. The related technologies of blockchain include: trusted storage, electronic identity and trusted time, etc., which provide effective support for various application scenarios of blockchain system. Blockchain is stored in a "block-chain" data structure, and the uploaded data and transaction records are recorded in blocks, and each block will be hash-operated on all the data in the block to get a hash value and stamped with a timestamp, which will form a back-to-back connected chain according to the time sequence, thus forming a chain of blocks. Time sequential, thus forming a "chain" connected to the front and back. [5]The next block contains the hash value of the previous block in addition to the newly entered data, which can be verified before and after. All of the above nodes can be updated synchronously, thus enabling trusted, low-cost "peer-to-peer" transactions.

3.2. Characteristics of Blockchain Deposits

Blockchain forensics and depositions have the following characteristics:

First, Immutability; Blockchain is a distributed database consisting of multiple nodes, each of which keeps a complete copy of the data. This decentralized nature means that no single central node can control or modify the data. Moreover, each block of data is encrypted using a hash function to encrypt its contents, which in turn generates a unique hash value. Any modification to the data results in a change in the hash value. In addition, each data block contains the hash value of the previous data block to form a continuous chain, which makes the data blocks dependent on each other. Once the previous data block is artificially modified, the hash values of all its subsequent data blocks will change. Therefore, once data is written into the blockchain, its content cannot be modified or deleted by human beings, because modifying the data will cause the hash value to change, thus breaking the consistency and integrity of the chain.[6]

Combining the above features of blockchain, its depository technology can ensure that the stored data has a high degree of security and trustworthiness, preventing the data from being tampered with or forged.

Second, decentralization; blockchain is a distributed network where data is stored on multiple nodes rather than centralized within a single server, thus improving the security and reliability of stored data. The decentralized feature of blockchain depository technology refers to its characteristic of not relying on a single centralized institution or individual control. This feature is mainly reflected in the following aspects: blockchain is a network of multiple nodes, each of which keeps a complete copy of the data. Since there is no single centralized node, all nodes can participate equally in the process of data verification and transaction confirmation. To ensure the trustworthiness and consistency of the data, blockchain uses a consensus mechanism to decide which node has the right to add a new block of data to the chain. Consensus mechanisms can be in the form of proof of workload, proof of entitlement, authoritative authentication, etc., but all ensure that no single entity can manipulate the entire network[7]. Due to the decentralized nature of the blockchain, even if some nodes fail or are attacked by the network, other nodes can continue to operate normally, thus ensuring the stability and continuity of the entire system.

In traditional centralized systems, it is necessary to rely on a third-party agency to verify and control data. In the decentralized blockchain depository technology, however, it is no longer necessary to trust a single intermediary, but rather rely on mathematical algorithms and network consensus to guarantee the security and authenticity of data.

Taken together, the decentralization of blockchain depository technology makes it a highly trusted, attack-resistant and tamper-proof depository suitable for a variety of scenarios that require trusted storage and verification of data.

Third, openness and transparency; the blockchain is open and transparent, and each participant can view transactions or records, which in turn increases the credibility of the data. The open and transparent feature of blockchain depository technology refers to the fact that the technology adopts the blockchain architecture when storing data, so that all transaction records and data operations are publicly recorded on the blockchain and cannot be tampered with, and every participant can view and verify these transactions, which can effectively ensure the transparency of the data. Moreover, blockchain uses cryptography to ensure data security and protect data from unauthorized access or tampering. Overall, blockchain depository technology provides strong support for trustworthy storage and verification of data through its open and transparent features.

In addition, blockchain depository technology also has the following characteristics: 1. Provide accurate time stamps for each transaction or record to ensure and record data at the same time as well as in the same order of sequence; 2. Allow the exchange of information and cooperation between multi-party organizations, so that multi-party subjects can participate in the whole process of forensics; 3. Automate the recording of data, and once the data has been written, it will be permanently preserved not to be erased or Deleted. Encryption algorithms can be utilized to protect the data. These features above make blockchain forensics and depositions a powerful tool for ensuring the reliability, security and traceability of electronic evidence, providing new possibilities for judicial practice and the forensics process.

3.3. The Applied Value of Blockchain Forensic Technology

Blockchain depository can solve the problem of difficult evidence collection by parties, as it provides a decentralized and tamper-proof data recording system. Parties can upload important evidence onto the blockchain, thus ensuring the integrity of its timestamp and content. In this way, the evidence will be permanently recorded on the blockchain and no party will be able to unilaterally modify or delete this information, which eliminates the reliance on intermediaries and ensures the credibility and accuracy of the evidence. At the same time, the parties only need to use their private keys to access their deposited evidence, thus ensuring the security and privacy of the data.

Blockchain depository can ensure the integrity and inerrancy of evidence by recording electronic evidence on the blockchain in an encrypted manner. In this way, when we need to use electronic evidence, we can easily avoid the risk of data tampering or forgery by verifying the authenticity of

its source, thus solving the problem of difficulty in using electronic evidence. In addition, the distributed nature of the blockchain increases the credibility and reliability of the evidence.

At the same time, blockchain depository can effectively improve the efficiency of court trials. Once recorded, the data on the blockchain cannot be deleted or modified, which ensures the authenticity and credibility of the evidence and reduces disputes and controversies, thus speeding up the process of trial. Moreover, blockchain technology enables smart contracts and automated execution, which reduces red tape and paperwork, improves the efficiency of information transfer, and allows all participants to view and verify the data, ensuring transparency and fairness. [8]In addition, data on the blockchain can be shared by multiple courts and relevant departments, reducing the time and workload for information collection and enabling related cases to be processed and resolved more quickly. Overall, blockchain depository technology can improve the credibility and transparency of evidence, reduce disputes, speed up the trial process, and effectively enhance the efficiency of court trials.

3.4. Blockchain Depository Technology in China

In 2018, Article 11 of the Provisions of the Supreme People's Court on Several Issues Concerning the Trial of Cases by Internet Courts made it clear that if the electronic data submitted by the parties can prove its authenticity through technical means of evidence collection, fixation and tamper-proofing such as electronic signatures, credible timestamps, hash value verification, blockchain, etc., or through authentication by the e-discovery and deposit platforms, the Internet court shall confirm[9]. introduced in 2021 Articles 16-19 of the Online Litigation Rules of the People's Courts introduced in 2021 have made further provisions on blockchain evidence[10]. In recent years, multi-tiered courts, led by China's Internet Court, have established a judicial blockchain alliance system. At the same time, blockchain deposit platforms of commercial nature have also emerged in large numbers, and with the Internet Court as a pilot, China's judicial organs have begun to try to apply blockchain deposit in judicial practice and realize the blockchainization of judicial activities.

Blockchain deposit technology has the following applications in the judicial field; first, the deposit of electronic evidence; blockchain can be used to store electronic evidence, such as contracts, transaction records, audio and video footage, and so on. By uploading the hash value of the electronic file with the deposit information, it ensures the integrity and inerrancy of the electronic evidence, which can be used as credible evidence in court. At present, the field where this kind of new technology is utilized more is the case of intellectual property protection disputes. Blockchain deposit technology can be used to protect intellectual property rights, including copyrights, patents and trademarks. By depositing information about a work or invention, it is possible to prove the point in time at which it was created, submitted or registered, thus ensuring that the legitimacy of the rights and interests of the parties concerned is effectively safeguarded.

In addition, there are a number of uses that are worth promoting that need to be further improved in practice. The first is the deposit of judicial documents; judicial documents such as court judgments and arbitration awards can be deposited using blockchain deposit technology to ensure that their contents are not tampered with and to provide reliable evidence. The second is the deposit of appraisal results; judicial appraisal results can be deposited through blockchain to ensure the independence, objectivity and authenticity of appraisal results, thus strengthening the credibility of the judicial field. The last is the legal contract; by depositing the content of the legal contract on the blockchain, the non-tamperability and non-repudiation of the contract can be ensured. In the course of contract disputes or enforcement, blockchain deposits can provide legally valid evidence.

Overall, blockchain depository technology in the judicial field can provide more secure, transparent and credible depository services, effectively reduce the risk of data tampering, strengthen the reliability of evidence, and improve the effectiveness of judicial decisions. With its technical advantages, blockchain deposit technology is expected to be further promoted and popularized in litigation activities, thus enhancing the level of judicial intelligence, effectively solving the problem

of difficulty in defending rights in the previously mentioned network violence infringement events, further improving the dilemma of the traditional use of electronic data, and enhancing the efficiency of the trial. At the same time, we should also rationally view the use of this emerging technology. At present, there is a lack of uniform legal regulation of blockchain depository technology, and the differences in the application of blockchain technology in various places in the process of using it are also due to the existence of different local policies and technical levels.

4. Problems in the Application of Blockchain Depository Technology

4.1. Issues of Qualification of Evidence

In law and in the course of judicial practice, the qualification of blockchain deposited evidence as evidence may face a number of problems and challenges, mainly involving the following aspects:

First of all, it is the problem of blockchain deposit evidence being recognized by law and legitimacy; blockchain deposit evidence currently exists in the case of legislation lagging behind the judiciary, regarding the legitimacy of blockchain deposit evidence, at this stage, only the relevant judicial interpretation issued by the supreme people's court to provide for it, and it has not been confirmed at the legislative level. The Supreme People's Court, as the highest judicial adjudicative organ in China, will inevitably reflect the relevant interests of the court as a litigation subject, and there are native interests (such as the efficiency and economy of the trial). Although other litigation subject will also pursue the efficiency of litigation, but the specific implementation of the content and mode and its own position in the litigation has a close relationship. [11]The courts are therefore improperly assuming the role of rule-maker while being the subject of litigation. If the legitimacy of blockchain deposits is to be confirmed at the level of the legal system, it is necessary for the National People's Congress to intervene as a legislature and regulate it through the introduction of relevant legal provisions, and the author believes that the relevant content can be revised on the basis of the existing civil procedure law.

Secondly, there is the issue of the credibility of the data source and technology and the authenticity of the evidence; although blockchain technology can ensure that the data after uploading and the data generated in the blockchain are not tampered with, it is difficult to guarantee the reliability and authenticity of the electronic data before uploading. This also leads to the authenticity of blockchain evidence, the need to further distinguish and verify. The author searched for blockchain evidence on China Judicial Instruments Network (CJIN), and found that in Beijing, for example, among the 55 cases using blockchain deposit technology that could be searched for, 52 of them were ex post facto depositions (i.e., the electronic data was uploaded to the blockchain after generation to be preserved). Among the cases involving blockchain depository, about 90% or more of the cases follow the order of first generating electronic data and then uploading the electronic data to the blockchain. This shows that the percentage of ex post facto storage models for blockchain of electronic data is in a high category. One of the dilemmas of the ex post facto storage model is that the electronic data may have been artificially tampered with or added to or subtracted from before it is uploaded to the blockchain, and there is no way to ensure that the uploaded electronic data is true and legitimate. If there are problems with the data itself or the source of the data is not credible, the authenticity and validity of the evidence may be affected.

Finally, while the tamperability and decentralized nature of blockchain gives greater credibility to deposited data, the technology itself may be vulnerable or subject to the risk of attack. Therefore, for the application of this emerging technology, we should not blindly give unconditional trust to it and ipso facto give it a supreme legal status. In the current judicial interpretation, individual provisions violate the principle of technological neutrality, giving blockchain evidence a status beyond the normal scope, such as Article 11, paragraph 2 of the Provisions on the Hearing of Cases in the Internet Court, which not only lists the provisions related to "blockchain" and other technological means, but also explicitly stipulates that the court "shall" confirm its authenticity[12] . However, in the author's

view, there is still a need for specialized technical appraisal and assessment of blockchain technology in the courtroom, so as to ensure the authenticity of electronic data.

4.2. Problems with the Subject of the Depository

The subject of a blockchain deposit is the owner or submitter of the electronic data deposited on the blockchain. In a blockchain depository, the subject of the depository may be an individual, an organization or other entities, who upload the data onto the blockchain and record its timestamp in order to achieve the purpose of data tampering, storage and proof of the existence of the data. The identity and rights of the subject of the deposit are one of the key issues of blockchain deposit, and currently the subjects of blockchain deposit in China include: the parties, the judicial authorities, and the third party subjects. There are some common issues about the subject of blockchain deposit. The first is identity verification; when uploading data to the blockchain depository system, the identity of the subject of the depository needs to be verified to ensure that they have the right to deposit the data, and to prevent the emergence of malicious storage behaviors and false certificates. The second issue is the authority to upload data; the depositing subject needs to ensure that they have the right to upload data to the blockchain, where the right can be based on the ownership of the data and the relevant authorization, or based on the needs of the infringed person to deposit the data. Otherwise, data deposited without the owner's consent may lead to relevant legal disputes. The last is the authority of data access: blockchain depository systems usually have different authority settings to control the access authority of the depository subject and other users to the data, as it is necessary to protect the privacy and security of the deposited data.

In addition, for the three different types of subjects mentioned above, there are also some personalized aspects of the problem, specifically manifested as follows: first, it is difficult for the parties to become eligible subjects for depositing evidence; firstly, because the parties do not have the ability to master the blockchain technology by themselves, and secondly, because the parties do not have a neutral litigation position. The parties as the subject of the deposit, on the one hand, it is difficult to complete the process of blockchain deposit by themselves, on the other hand, it is difficult to be adopted by the judge to a certain extent by the evidence deposited. Secondly, the judiciary as the subject of the deposit, due to its credibility, can effectively endorse the authenticity of the evidence, on the one hand, the authority of the judiciary for the blockchain deposit of evidence to provide a guarantee of national credibility; on the other hand, such a practice will lead to the judiciary to participate in the process of litigation in advance, which may result in the loss of the trial of its neutral position. Moreover, since the judicial organs themselves are the depository subject of the evidence, they will inevitably give the evidence a supreme legal status in the determination process, thus unconsciously lowering the standard of determination of the evidence, which may result in some level of judicial injustice. Finally, the third party as a depository subject; compared to the first two subjects, is the most feasible. In this regard, this subject will be further discussed in the next part of this paper.

4.3. Problems with Third-Party Qualification

As a third party of blockchain depository, the qualification issue of its depository subject is an important consideration. The reason is that the credibility and professionalism of the third-party depository subject directly affects the validity and acceptability of the deposit results. The qualification of the third party depository subject mainly involves the following aspects:

First, In terms of legal qualifications; third-party depository entities should have legal operating qualifications as well as compliance licenses. When choosing a depository service provider, it should be ensured that it has been registered and operates in compliance with the law, and can provide continuous and reliable depository services. In this regard, China's qualifications for third-party depository subjects currently do not have more systematic and comprehensive provisions.

Second, in terms of technical level; the third-party depository subject should have sufficient technical capabilities and expertise to be able to use blockchain technology to realize secure storage and non-tampering of data and ensure the authenticity and integrity of the deposited data.

Thirdly, the independence and impartiality of the third party is also the most important issue in the author's view; independence is an important factor in ensuring the objectivity and credibility of the depository. Therefore, the third-party depository subject should maintain its independence from the influence of other stakeholders, in order to ensure the impartiality of the results of the deposit.

Fourth, privacy protection; when processing data, the subject of the depository should strictly observe the principle of privacy protection, ensure data security during the depository process, and clearly specify the scope and purpose of data use.

Fifth, in terms of user acceptance and credibility; checking the customer reviews and word-of-mouth of third-party depository subjects can help to understand the credibility of their services. Choosing a reputable and credible depository service provider can effectively improve the acceptability of the depository results.

When conducting a blockchain depository, users and enterprises should carefully select a suitable third-party depository subject and understand its qualifications, technical capabilities and measures for privacy protection. Choosing a trusted depository subject can increase the reliability and legal validity of the deposited data and ensure the validity of the deposit results in the judicial and legal fields.

5. Concluding Remarks

As an emerging technology, blockchain is quietly changing the layout of traditional industries. Many objects that have long been taken for granted have become new because of the integration of this technology. This paper takes the way of defending rights in online violence infringement events as an entry point to discuss how blockchain technology can better play the role it should play in judicial litigation activities. Blockchain deposit technology innovates the preservation of evidence, by virtue of its untamperable, decentralized and open and transparent characteristics, it can effectively solve the traditional electronic data in the past there is too high a cost of deposit, the evidence identified difficulties and the data is prone to be tampered with and other applicable aspects of the dilemma, and effectively enhance the efficiency of the use of electronic evidence, so that the electronic data can really play its due role in litigation activities. At the same time, we need to dialectically view the application of blockchain deposit technology. At present, the application of this new technology of blockchain deposit in our country is still in the beginning stage of development, there are still deficiencies in the legislative level, and the system regulation level has not yet been unified. This paper mainly discusses the qualification of evidence, the subject of deposit and the conflict between blockchain technology and citizens' privacy, and all the above problems need to be gradually solved in practice through the construction of technology and system. Looking into the future, the application of blockchain technology has a long way to go, and we need to contribute to its standardized and reasonable application by every legal person.

References

- [1] Chen, Y. S. Legal regulation of electronic data search and seizure[J]. *Modern Law*, 2014, 36(05): 111-127.
- [2] See White Paper on Blockchain Judicial Deposit Application (Version 1.0), June 2019, guided by the Information Center of the Supreme People's Court, with the participation of 25 units, including multi-provincial high courts, Internet courts, and the China Judicial Big Data Research Institute.
- [3] See Liu Pinxin, "On the authenticity standard of electronic evidence", *Social Science Journal*, No. 1, 2021.
- [4] See September 5, 2018, when the China Academy of Information and Communications Technology released the Blockchain White Paper (2018).
- [5] Yang Dong. Chain gold has the law [M]. Beijing: Beijing University of Aeronautics and Astronautics Press, 2017: 12.

- [6] ZHANG Yujie. Judicial application of blockchain technology, systemic dilemmas and evidence law innovation[J]. *Oriental Law*, 2019(03):99-109. doi:10.19404/j.cnki.dffx.20190129.002.
- [7] Chen, Xiuhui. Why blockchain decentralization is important[J]. *Computer and Network*,2018(21):38[5]He Pu, A forward-looking overview of blockchain technology and applications[J]. *Computer Science*,2017(4) :4.
- [8] Liu Xuezai,Ruan Chongxiang. Research and thinking on blockchain electronic evidence[J]. *Journal of Northwest University for Nationalities (Philosophy and Social Science Edition)*,2020(01):52-59.DOI:10.14084/j.cnki.cn62-1185/c.20191206.002.
- [9] See Provisions of the Supreme People's Court on Several Issues Concerning the Trial of Cases in Internet Courts [N]. *People's Court News*, 2018-09-08(003).
- [10] See People's Court Online Litigation Rules Law Interpretation [2021] No. 12 (Adopted by the Trial Committee of the Supreme People's Court at its 1838th meeting on May 18, 2021, effective August 1, 2021).
- [11] Liu Pinxin. On blockchain evidence[J]. *Legal Research*,2021,43(06):130-148.
- [12] Xi Zhehan. Judgment on the evidence of "triality" of electronic data deposited on blockchain[J]. *Social Scientist*,2022(07):126-132.
- [13] Article 107 of the Civil Code of the People's Republic of China provides that a natural person may, in accordance with the law, inspect or copy his or her personal information from an information processor; if he or she discovers that there are errors in the information, he or she has the right to object to the information and to request that corrections and other necessary measures be taken in a timely manner. If a natural person discovers that an information processor has handled his or her personal information in violation of the provisions of laws or administrative regulations or the agreement between the two parties, he or she has the right to request the information processor to delete the information in a timely manner.
- [14] Wen Zhanting. Research on the Application of Blockchain Depository in the Field of Civil Litigation [D]. *Three Gorges University*,2023.DOI:10.27270/d.cnki.gsxau.2022.000022.