**Electronic Data Preservation and Storage of Evidence by Blockchain**

Hua Shang¹, Hui Qiang²

¹School of Humanities and Law, North China University of Technology, Beijing, China, ²Institute for Chinese Legal Modernization Studies, School of Law, Nanjing Normal University, Nanjing, Jiangsu, China

**Abstract**

In the face of the era of big data, how to ensure the authenticity of electronic data has become an important practical issue. Online preservation methods based on hash operation, time stamp, and blockchain technology can effectively guarantee the authenticity and security of electronic data. Blockchains are inherently traceable, de-centralized, and difficult to tamper with, which can be enough served as the basic technology of electronic data certification. Preservation by blockchain mainly includes the following links: platform registration and identity authentication, generation and transmission of electronic data, and storage of electronic data. Preservation by blockchain has higher security than centralized online security because of distributed storage. However, it should be acknowledged that the preservation by blockchain is not without risk. The court should adhere to the principle of individual review of each case and review the electronic data from its generation, transmission, reception, storage, and collection.

**Keywords:** Electronic data, online evidence preservation, preservation by blockchain

**INTRODUCTION**

With the advent of the Internet Age, more evidence is reflected in the form of electronic data. Electronic evidence preservation is of great significance in judicial practice. First of all, electronic data preservation is of great significance to the effective proof of the parties. Electronic data is easy to be deleted, modified, and lost in practice. In order to effectively protect the rights of parties, it is necessary to ensure the authenticity and integrity of electronic evidence. Second, electronic data preservation is of great significance for judges to find the fact of the case. Finally, electronic data preservation is of great significance for improving the efficiency of litigation. A large number of cases in the judicial practice show that an important focus of litigation dispute often is the authenticity of electronic evidence, and the parties and the judge spend a lot of time to solve this problem. Electronic evidence preservation can guarantee its authenticity, thereby reducing litigation costs and time and improving litigation efficiency. In summary, electronic data preservation has become an unavoidable practical problem.

**OVERVIEW OF ELECTRONIC DATA PRESERVATION**

**The concept of electronic evidence preservation**

There are four different views on the concept of evidence preservation: “fixed custody,” “measures,” “procedures,” and “behavior.” Although the four viewpoints are different, they basically express the core meaning of evidence preservation. The preservation of evidence is essentially through preinvestigation (premeasures), which determines the evidence that can be used to prove the facts of a case so that it does not lose its validity. The purpose of evidence preservation is to properly fix and preserve the evidence that has been discovered or extracted to prevent its destruction or loss, so as to ensure the evidential value. “Evidence preservation includes the fixation and custody of evidence, which means to fix evidence in an appropriate way and keep evidence safely so that judicial personnel, parties, and lawyers can prove the fact of a case.”

**Address for correspondence:** Dr. Hua Shang, No. 5 Jinjumang Road, Shijingshan District, 100144 Beijing, P.R. China. E-mail: hshang103@163.com

Submitted: 04-May-2019 Revised: 11-Feb-2020 Accepted: 13-Feb-2020 Published: 17-Mar-2020

This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 License, which allows others to remix, tweak, and build upon the work non-commercially, as long as appropriate credit is given and the new creations are licensed under the identical terms.

For reprints contact: reprints@medknow.com

How to cite this article: Shang H, Qiang H. Electronic data preservation and storage of evidence by blockchain. J Forensic Sci Med 2020;6:27-36.
From the perspective of proving the fact, electronic data has a different role from other evidences such as material evidence and documentary evidence. Material evidence plays the role of proving the fact with its external characteristics, existence, and attributes. Moreover, the preservation of the material evidence is mainly to prevent its loss or difficult to obtain in future. The electronic data has a special high-tech carrier, which is easier to modify in the practice. Its preservation should pay more attention to how to ensure its authenticity. Electronic data is more likely to be tampered with in practice, and more attention should be paid to how to ensure its authenticity. In view of this, this article believes that electronic evidence preservation has broad and narrow meanings. The broad sense of electronic evidence preservation refers to the act of fixing and keeping the original data evidence or its auxiliary data such as hash values and abstracts in an appropriate way in the case where electronic data may be deleted or modified. In the narrow sense, electronic evidence preservation only refers to the fixation and preservation of the original electronic data itself.

Regardless of the broad concept or the narrow concept, the main purpose of electronic evidence preservation is to ensure the true existence of electronic data and to ensure the smooth progress of litigation. German scholar Hans-Joachim Muzerak believes that the preservation of evidence (procedure) means that “an investigation of evidence can be carried out according to the application of one party in addition to the procedure or even before the commencement of the proceedings, with the purpose of preserving the evidence for litigation.”\(^{(4)}\)

**Legislative provisions on electronic evidence preservation in China**

At present, there is no centralized and comprehensive legal norm for electronic evidence preservation in China, and the relevant provisions are scattered among some laws and judicial interpretations.

In criminal proceedings, “Provisions of the Supreme People’s Court, the Supreme People’s Procuratorate, and the Ministry of Public Security on Extracting and Reviewing Electronic Data in Criminal Case” is a relatively comprehensive provision of electronic data in criminal proceedings in China. Article 8 of this provision stipulates: “When electronic data is collected and extracted, and the original storage medium of electronic can be seized, the original storage medium should be seized and sealed, and a record should be made to record the storage status of the original storage medium. When sealing the original storage medium of electronic data, it shall ensure that electronic data cannot be added, deleted or modified without removing the sealing state. Before and after sealing, photographs of the sealed original storage medium shall be taken to clearly reflect the state of sealing. If storage media such as mobile phones with wireless communication functions are stored, measures such as signal shielding, signal blocking, or power-off should be taken.” Articles 10 and 11 of this provision, respectively, provide for other methods of evidence collection and fixation, that is, “the relevant evidence may be fixed by means of printing, photographing or video recording, and explaining the reasons in the written record,” and “the electronic data can be frozen with the approval of the person in charge of the public security organ or the chief procurator at or above the county level.”

In civil litigation and arbitration, the preservation of electronic evidence is extremely important. Article 81 of the Civil Procedure Law\(^{(5)}\) and Article 46 of the Arbitration Law\(^{(6)}\) stipulate the conditions and procedures for the preservation of evidence. Articles 23 and 24 of Several Provisions of the Supreme People’s Court on Evidence in Civil Procedures further clarify the conditions and methods for the preservation of evidence. Article 24 of this provision stipulates: “When preserving evidences, the people’s court may, according to the specific circumstances, adopt the ways of preservation like sealing up, detaining, taking photos, make sound recordings or visual recordings, making reproductions, authenticating, taking transcripts, etc. When preserving evidences, the people’s court may demand the parties concerned or the litigation agent to be present.”

Some local or departmental regulations clarify the procedure for the preservation of electronic evidence. In 2009, “Answers to Several Issues Concerning Site Investigation and Electronic Evidence Preservation of Computerized Digital Devices in Intellectual Property Cases by the People’s Court of Shanghai High Court (1)” stipulates the specific process of electronic evidence extraction and preservation, namely “(1) Preparation for investigation. The court determines the investigators, discusses the investigation plan, and develops an investigation plan. (2) Protect the site. After the investigators arrive at the scene, they implement effective isolation to protect the site and prevent electronic evidence from being destroyed. (3) Find evidence. Investigators look up all possible electronic evidence on the spot. (4) Preserve evidence. The investigators immediately fix the electronic evidence found in the investigation. (5) Extract evidence. Investigators extract evidence containing electronic evidence from the scene. (6) Remote inspection. In some cases, remote target systems need to be inspected through the network to extract and fix the state of the remote target system and the remaining electronic data.” In 2012, All-China Lawyers’ Association issued “lawyer’s guide on handling electronic data evidence business.” It stipulates how to collect and preserve the evidence of electronic data, such as “can apply for a notary office to carry out the whole process of video notarization, the whole process of documentary notarization or the deposit of mirror report notarization, etc.” “You can use professional electronic data forensics equipment or software, or seek technical services such as electronic data evidence collection and fixation provided by professional technical service organizations such as identification agencies.” In 2012, the China Notary Association issued “Guidance on Handling Notarization of Internet Electronic Evidence Preservation,” which stipulates the scope, procedure, and specific operating rule of Internet electronic evidence preservation by notarial organs.
**Method and Problem of Electronic Data Preservation**

**Nononline preservation of electronic data evidence**

From the above relevant regulations and practice, the main methods of electronic data evidence preservation include: (1) sealing and detaining the original storage media; (2) printing, taking photographs, and making sound recordings or visual recordings; (3) making inquests, inspections, and on-site transcripts; (4) authenticating; (5) cyber notary authority; (6) time stamp; and (7) preservation by blockchain. According to whether it belongs to remote online operation, these main preservation methods can be divided into nononline preservation method and online preservation method. The former pays more attention to the storage medium of electronic data and focuses on how to select the information carrier and fix the electronic data through physical space operation, including sealing and detaining the original storage media, printing, taking photographs, making sound recordings or visual recordings, and making transcripts. The latter pays more attention to the content of electronic data and the authenticity of evidence content in network links such as generation, transmission, storage, and collection of electronic data. The online preservation methods include cyber notary authority, time stamp, and preservation on blockchain. Here are some common nononline security methods.

First, seal and detain the original storage media. Sealing and detaining are the common methods of evidence preservation, which are widely used in the preservation procedure of material evidence, documentary evidence, and other kinds of evidence. For electronic data evidence, the evidence information is generated in the original storage medium. If the original storage media can be promptly and effectively sealed and detained, the authenticity and integrity of electronic data evidence can be ensured.

Second, print, take photographs, and make sound recordings or visual recordings. These methods are simple and cost-effective, and are used by judicial personnel. China’s notary agencies also use this method more commonly. In 2012, Article 9 of the China Notary Association, that is, “Guidance on Handling Notarization of Internet Electronic Evidence Preservation,” stipulates: A notary office may, in handling the procedures for the preservation of Internet electronic evidence, extract and fix evidence by downloading, screenshot, real-time printing, storage printing, video recording, photography, synchronous video recording with software, text recording, and other methods. If the command input process such as login, download, screen capture, and save can be printed in real time, it is recommended to use the “real-time print + video” method to extract and fix the evidence. Although these preservation methods have played a positive role, it should be noted that these preservation methods have transformed electronic data into other forms of expression, which will affect the authenticity and proof value of electronic evidence to a certain extent.

Third, make inquests, inspections, and on-site transcripts. This method is a common traditional method, which is stipulated in the procedural law, and is widely used by judicial organs and notary agencies. In Articles 7, 10, and 11 of the Guiding Opinions of the China Notary Association for the Preservation of Internet Electronic Evidence in 2012, the requirements for making transcripts are specified, that is, “cleaning inspection of the computer used should be performed” and “The notary office shall handle the electronic notarization of the Internet and shall make an on-site record.”

From a practical perspective, the nononline preservation of electronic data has a positive effect and is often used in judicial practice. However, there are some problems in practice as follows:

First, the effect of guaranteeing the authenticity of electronic data is greatly affected by the operator. For example, sealing and detaining the original storage media is a commonly used method of evidence collection and preservation in practice. However, the reliability of this method is greatly affected by human operation. In practice, it may not play an effective role in guaranteeing authenticity, but may be questioned by relevant parties. The doubt mainly arises from two aspects: first, the operator’s ability and equipment reliability and second, whether the operator can really follow the legal procedures strictly, whether it can be objectively neutral without any bias.

Second, most of the nononline preservation methods lag behind. Electronic data has the characteristics of being easily falsified, and the shorter the time between generation and preservation, the better the preservation effect. If the time is long, the evidence preservation may cause some problems, such as how to ensure that the electronic data before the evidence preservation has not been deleted and how to ensure the reliability of its storage medium. These problems have emerged in practice, which has become the focus of disputes between the parties and the key points of court review.

Third, nononline preservation is less efficient. The nononline preservation method needs to operate the specific data evidence one by one, to seal and detain the original storage media, print, take photographs, make sound recordings or visual recordings, and make inquest and inspection transcripts. In practice, it takes more workforce, material resources, and time than the online preservation method. In particular, in the current environment of large amount of data and remote transaction, traditional nononline preservation methods are difficult to cope with these situations, such as Taobao shopping dispute and network fraud, which in practice often present a “small amount and multiple transactions” form. Therefore, it is more necessary to improve the efficiency of electronic data evidence preservation.

**Online preservation of electronic data evidence**

**Cyber notary authority**

Cyber notary authority is a system of specific cyber notary organization that uses advanced network technology and specific computer programs to prove relevant legal facts on
the Internet and to preserve relevant electronic evidence in the Internet.\(^7\) "Cyber notarization refers to the act of providing enhanced certification and evidence preservation for electronic identity, electronic transaction behavior, data files, etc., on the Internet by using computer and Internet technologies."\(^8\)

In the European Union, cyber notary authority is commonly used in electronic data evidence preservation. The whole process of notarization is completed in the network, without the face-to-face communication between the parties and the notary, which can greatly shorten the distance of physical space. By issuing instructions from the applicant’s computer, the notary can receive encrypted data messages through the Internet. The notary shall verify the relevant electronic data information and make corresponding digital notary certificate. In order to ensure the reliability and security of cyber notary, it is inseparable from technical support such as digital encryption and digital authentication. It is a combination of multiple technologies such as identity authentication technology and hash algorithm.

In China, the notarization preservation of electronic data is not simply an online evidence preservation method; rather, it includes some nononline preservation methods. The China Notary Association’s “Guidance on Notarization of Evidence Preservation” stipulates how the notary office handles the real-time electronic evidence preservation of the Internet. Article 15 stipulates “Notarization for the preservation of real-time data evidence on the Internet should be carried out using a computer of a notary office or a computer of a third party without interest. The notary or the party shall operate in accordance with the written operating procedures provided by the party. The notary shall record the entire process of logging into the network, entering the relevant website (web page), downloading, printing (or burning a CD) and the name and version of the operating software used, and pay attention to whether the downloaded content matches the content of the webpage. The preservation process can be made visual recordings if necessary.” In 2012, the China Notary Association’s “Guidance on Handling Notarization of Internet Electronic Evidence Preservation” further clarified the scope, procedures, and specific operating rules of notary office for the preservation of electronic evidence.

From the comparison of practice between China and foreign countries, there are the following problems in China’s cyber notary authority: first, pay attention to fixing and ignore custody. Article 2 of the Guidance on Handling Notarization of Internet Electronic Evidence Preservation clearly stipulates that the term “Internet electronic evidence preservation” as mentioned in the guidance opinions refers to the activities of notary institutions to fix and extract electronic evidence by accessing wide area network through computer equipment and technology. The custody of electronic data services does not fall within the scope of these guidelines. Second, preservation technology is relatively traditional. The China Notary Association’s “Guidance on Handling Notarization of Internet Electronic Evidence Preservation” stipulates in Article 9 that A notary office may, in handling the procedures for the preservation of Internet electronic evidence, extract and fix evidence by downloading, screenshot, real-time printing, storage printing, video recording, photography, synchronous video recording with software, text recording and other methods. If the command input process such as login, download, screen capture, and save can be printed in real time, it is recommended to use the “real-time print + video” method to extract and fix the evidence. Some new technologies are not fully applied to notarization preservation, such as data encryption technology, time stamp technology, blockchain technology and so on. Although a few notary offices in China have carried out new exploration of online preservation of data evidence and achieved positive results, there are still some problems in the majority of electronic evidence notarization, which are in urgent need of innovation and development.

**Time stamp certification**

Time stamp is a complete and verifiable data which has already existed at a specific point in time. Time stamp is an encrypted voucher document, which includes the following three parts: (1) digest of the document that needs to be time stamped; (2) date and time when digital time-stamp (DTS) receives the document; and (3) digital signature of DTS. The process of time stamp generation is as follows: The user first encrypts the file to be time stamped with a Hash code to form a digest and then sends the digest to DTS, which encrypts the file (digital signature) after adding the date and time information of receiving the digest and then sends it back to the user.\(^9\) An electronic data can prove the generation time by time stamping, thus exerting its further proof value.

In judicial practice, time authentication is as important as identity authentication, which is directly related to the proof value of electronic data. In order to ensure the accuracy of time stamp certification, it is necessary to strictly follow the standard time approved by the National Time Service Center. On September 3, 2018, the Supreme People’s Court passed the “Regulations on Several Issues Concerning the Internet Court Trial,” which lists the credible time stamps, hash value verification, blockchain, and other means as a fixed method of collection, and clarifies its effectiveness and value. Article 11, Paragraph 2, of this provision provides: “If the electronic data submitted by the parties can prove their authenticity through electronic signature, trusted time stamp, hash value verification, blockchain and other evidence collection, fixed and tamper-proof technical means, or through electronic forensics and certificate storage platform authentication, the Internet court shall confirm it.” In China, the Shenzhen Longgang District People’s Court in Guangdong Province actively explored the judicial application of trusted time stamps and cooperated with a time stamp’s service organization to jointly construct the “TSA electronic evidence solidification system of the People’s Court.” And, “Lilonghu” is the first case of judicial application of time stamp technology in China, achieving good legal and social effects.
From the point of ensuring the authenticity of electronic data files, the time stamp certification made by the trusted time stamp authority can be regarded as an online preservation method for electronic data. Moreover, compared with the traditional methods of printing, detaining, and sealing storage media, trusted time stamps can effectively cope with the demand for more data and timely preservation in the era of big data. A major advantage of using the hash comparisons is that an electronic data may be composed of thousands of files, and if you compare the files themselves, it will generate a huge amount of work. However, if the hash comparisons be adopted, the process will not only be more scientific, the workload required will be significantly smaller, and the efficiency will be much higher.[10] At present, some trusted time stamps in China have combined time stamps, digital authentication techniques, hash operation, and other means, playing an effective and reliable role in preserving electronic data evidence.

From this point of view, the preservation method that combines time stamp, digital authentication technology, hash operation, and other means seems to solve the existing problems of electronic data security. But is this method really perfect? It should be noticed that a common feature of these practices is “centralized online preservation and centralized storage.” Correspondingly, what follows is “decentralized online preservation and distributed storage,” that is, preservation by blockchain. At present, there are still some imperfections in “centralized online preservation and centralized storage.” For example, “decentralized online preservation and distributed storage” is safer than “centralized online preservation and centralized storage.” As the former stores data distributed on all nodes in the chain, these nodes may be distributed in different regions or countries, so that the risk of data loss caused by “centralized online preservation and centralized storage” can be avoided.

Decentralized Online Preservation of Electronic Data

The meaning and operation principle of preservation by blockchain

The so-called blockchain is in fact an open-distributed account book. It runs on a cluster of computers (P2P) that anyone can participate in and is open to the public. By importing the Proof of Work (PoW) mechanism, blockchain can protect data from arbitrary tampering.[11] The PoW mechanism cannot be separated from hash algorithm. A hash function is a function that converts a group of data into a number. Input the original data into the hash function will get the “hash value,” which has the following two characteristics. First, if you change the original data, you will get completely different hash values. Second, even if the hash value is known, the original data of the hash value cannot be deduced by the arithmetic rule(based on the operation of certain rules).[12]

Preservation by blockchain works as follows: first, you can show your file (any type) to the website that provides the service; the website will convert the file content into an encrypted digest or hash value. The algorithm can create a digest or an encrypted string to represent the data. No two abstracts will be exactly the same unless they are calculated from the same document. Therefore, the hash value can accurately represent the content of the document. After inserting the encrypted hash value of the document into a transaction and recording the transaction into a block, the time stamp of the blockchain becomes the time stamp of the document, so that the content of the document is successfully coded into the blockchain. When the same file is submitted again, the hash value can be created in the same way to verify whether the two files are completely consistent. Therefore, if any changes are made to the file, the newly obtained hash value will not match the value embedded in the blockchain at that time. This is how the system completes the document verification process.[13]

Encrypted hashing algorithm is used to prove the integrity of a file, but the problem is that it is not known when the file was created until the blockchain provides a mechanism for adding security time stamps. The method provides time stamp data in an immutable manner and at the same time ensures that the content of the data is not leaked, which is almost a perfect method for judicial officers, citizens, and government officials.[13] Blockchains are inherently traceable, de-centralized, and difficult to tamper with, which can be enough served as the basic technology of electronic data certification. From the practice of preservation, preservation by blockchain mainly includes the following links: platform registration and identity authentication, generation and transmission of electronic data, storage of electronic data, and so on.[14]

Practical exploration of preservation by blockchain in China

Positive attitudes of courts and arbitration institutions to preservation by blockchain

On June 28, 2018, the Hangzhou Internet Court publicly adjudicated a case of infringement on the right to disseminate works information on the Internet. This is the first time that the Court confirmed the legal effect of electronic evidence from the preservation platform with blockchain technology. In this case, the plaintiff automatically crawled the infringement webpage and identified the source code of the infringement page through the third-party preservation platform, and calculated these two contents and the compressed package of the call log into hash values and uploaded them to Factom blockchain and Bitcoin blockchain. The court held that such electronic data could be used as the basis for the determination of tort in this case.[15] In fact, blockchains have been used in arbitration before. Guangzhou Arbitration Commission, Weizhong Bank, and Hangzhou Yibi Technology have launched the “arbitration chain,” and Guangzhou Arbitration Commission has made awards according to the “arbitration chain.”

On October 30, 2018, the Beijing Internet Court officially opened its first case to hear a dispute over ownership and
In the field of arbitration, starting from the field of Internet finance, the China Maritime Arbitration Commission will make full use of the completed online arbitration platform and blockchain electronic preservation technology to cooperate with Huawei Yun on data security, providing a convenient, efficient, and high-quality dispute resolution service model for industries with high standardization and electronic data storage of transaction evidence (e.g., logistics, aviation, and e-commerce).\(^{[17]}\)

**Current situation of blockchain preservation institutions**

At present, China positively lays out the blockchain, and the number of related blockchain enterprises is second only to that of the United States. In the field of judicial preservation, there are dozens of blockchain preservation platforms with different sizes. For example, the representative platforms are “Ancun.com,” “Baoquan.com,” “e-signature,” “Fantai Alliance,” “China Cloud Sign,” “Chain Pass,” “Baby Certificate,” and so on. These platforms emphasize the security of electronic data preservation with the concept of “blockchain,” but there are some differences in qualification and technology level. Some platforms have good preservation technology level, but some platforms mainly use digital authentication technology and hash operation technology to construct an essentially decentralized mode in a central way of thinking.

On December 22, 2018, Baidu Company and Beijing Internet Court jointly released the news of “the balance chain,” which is an electronic evidence platform co-constructed by the Beijing Internet Court and the leading domestic industrial enterprises of blockchain, such as Baidu Company and Trustdo Technology Company. A total of 17 blockchain nodes have been constructed, and the application data docking between 24 data platforms and preservation platform has been completed.\(^{[18]}\) Further observation and research is needed on the operational effect of the blockchain preservation platform led by the centralized court. It should be noted that whether the court-led and participated in the construction of blockchain preservation platform will affect the neutrality of the court. Because in the so-called “blockchain first case” heard by the Hangzhou Internet Court, the court adhered to the principle of individual review of each case, maintained the role of a neutral referee, comprehensively reviewed from various aspects such as platform qualification, and judged with the opinions of Qianmai Appraisal Institute. The blockchain technology has the characteristics of traceability, but it is not absolutely safe. Blockchain preservation platform also has risks.

**Significance of preservation by blockchain**

First, the authenticity of electronic data is effectively guaranteed. Because of the introduction of the PoW mechanism, preservation by blockchain can protect data from arbitrary tampering by hash algorithm. The White Paper on China’s Blockchain Industry 2018 issued by the Ministry of Industry and Information Technology also points out that the use of blockchain technology to electronic evidence preservation can effectively solve the security problems faced by traditional preservation. The time stamp is given when the electronic evidence is generated, and the data integrity is verified by comparing hash values when the electronic evidence is stored. During the transmission, asymmetric encryption technology is used to encrypt the electronic evidence to ensure the transmission security, which fully guarantees the authenticity of the evidence.\(^{[19]}\)

Second, the security of the preservation system is effectively guaranteed.\(^{[20]}\) Blockchain-distributed storage determines that every node in the chain can store the data synchronously, and a single node to modify the account data is invalid. It is also very difficult for network hackers to attack all the nodes in the blockchain at the same time. The damage of any node will not affect the storage of data in the blockchain, so the data stored in the blockchain is relatively safe. In addition, the hash operation and blockchain can effectively reduce the data storage capacity, and can more effectively meet the requirements of the era of large data.

Third, effectively protect data content from disclosure. Recording a hash value through a blockchain can be evidence that the file existed at a certain point in time. Moreover, as the hash value is recorded, the content of the file will not be exposed, which can be considered a method of “zero-knowledge proof.” Hence, zero-knowledge proof is a way for a certifier to prove that he/she has the information without providing it to the other party.\(^{[21]}\)

**Potential risk of preservation by blockchain**

Blockchain technology can effectively protect the authenticity and security of electronic data. However, this technology is not absolutely reliable. It may have the following problems:

First, blockchain technology is not absolutely safe. Usually, the threat to hash values is actually reverse hashing (trying to figure out the hash value at the time by reverse calculation) and collision (make two different files generate the same hash value). The impact of these occurrences on the hash-calculating methods currently used in blockchain is very limited.\(^{[22]}\) Although the impact is limited, it is not nonexistent. In theory, these cryptographic operations can be deciphered, but it is only a matter of time and cost. If quantum computers are widely used in future, it will possibly pose a challenge to the security of blockchain technology.

Second, the design of blockchain and the selection of chains will relate to the security of data. It is possible that all nodes collude with each other and tamper with data. It is generally believed that “only trusted computers can be preselected as system nodes, so they will not do bad things,” but there is no guarantee that such a situation will never happen.
The most important feature of “independent of manager, almost impossible to be tampered” has been lost in the private blockchain.[21] In practice, consensus mechanism is very important for the operation of the blockchain, and the possibility of “collective evil” in the alliance chain cannot be ruled out.

Third, preservation by blockchain mainly solves the problem of electronic data storage, but it cannot completely solve the security of the whole process of electronic data generation, transmission, storage, and collection. For the generation and transmission of electronic data, other technical means such as forensics and identification of electronic data are also needed to verify. In a sense, blockchain preservation is a method of authenticity verification or auxiliary preservation. At present, preservation by blockchain is more an indirect authenticity verification method. The preservation by blockchain cannot completely replace other forensics and identification methods.

**Review of Blockchain-Stored Evidence**

**Content of blockchain-stored evidence review**

Blockchain is only a preservation technology, the purpose of which is to ensure the authenticity and reliability of electronic data. However, as mentioned above, the blockchain-stored evidence is not absolutely reliable, and we need to adhere to the principle of individual review of each case. The most important thing is to identify the authenticity of electronic data.

According to the current law and judicial interpretation, the authenticity of electronic evidence can be reviewed from the aspect of generation, transmission, storage, collection, and the integrity of electronic evidence.[24] Article 22 of “Provisions of the Supreme People’s Court, the Supreme People’s Procuratorate, and the Ministry of Public Security on Extracting and Reviewing Electronic Data in Criminal Case” further stipulates that whether electronic data is authentic, the following contents should be examined: (1) whether the original storage medium is transferred; if the original storage medium is unable to be sealed or moved inconveniently, whether there is an explanation for the reasons, and indicate the collection and extraction process, the location of the original storage medium or the source of the electronic data; (2) whether the electronic data have special marks such as digital signatures and digital certificates; (3) whether the process of collecting and extracting electronic data can be reproduced; (4) whether there is a description if the electronic data is added, deleted, modified, etc.; and (5) whether the integrity of electronic data can be guaranteed. It is generally believed that the links affecting the authenticity of electronic evidence mainly include: (1) the generation of electronic evidence; (2) the transmission and reception of electronic evidence; (3) the storage of electronic evidence; and (4) the collection of electronic evidence.[25]

According to graphical analysis of evidence inference chain[26] [Figure 1], this article specifically analyzes the content of blockchain-stored evidence review, combined with the content of “the first judgment of blockchain preservation” of Hangzhou Internet Court.[27]

First, review the generation and source of electronic data. Blockchain preservation technology can not alone guarantee the authenticity of electronic data in the process of generation and collection. If the source of electronic data is not reliable, it will inevitably weaken the authenticity of electronic data from blockchain preservation platform. In “the first judgment of blockchain preservation,” the Hangzhou Internet Court examined the reliability of infringement web forensics technology. “Baoquan website” automatically calls Google’s open-source program “Puppeteer” to grab pictures of the target page and, at the same time, gets the source code of the target page by calling “curl.” This system is open to all people equally and can be used by anyone. Moreover, its operation process is automatically completed by the machine according to the preset procedure of the forensic system. In the whole process of forensic and evidence-fixing, the possibility of tampering with the relevant links artificially is small, so the source of electronic data is more reliable.

Second, review the transmission and reception of electronic data. The process of electronic data transmission is indispensable from generation to storage. If the transmission process is unsafe, the authenticity of electronic data is likely to be suspected. In “the first judgment of blockchain preservation,” the Hangzhou Internet Court examined whether the electronic data was actually uploaded. For this purpose, the judge conducted a search in the FACTOM blockchain according to the transaction hash value provided by the plaintiff to see the content of the transaction hash stored and the generation time. After checking, the generation time of the block submitted by the plaintiff conforms to the time logic between the call log generation time and the FACTOM packing rule. According to the transaction hash value of the block height anchored to the bitcoin blockchain, the content contained in the block node can be queried in the bitcoin blockchain, which is consistent with the hash value of the content stored in FACTOM. Therefore, the court confirms that the “Baoquan website” has uploaded electronic data to the FACTOM blockchain and the bitcoin blockchain.

Third, review the institutional qualification of the preservation platform.[28] In general, the evidence preservation agency should be an enterprise of full-time employment in evidence preservation business with legal qualifications, equipped with professional technicians and specialized electronic equipment.[29] In practice, the court should review the institutional qualification of the blockchain preservation platform and the technical level of the operators. In “the first judgment of blockchain preservation,” the Hangzhou Internet Court first reviewed the qualification of the preservation platform. Because the shareholders and business scope of the platform company are relatively independent of Huatai One Media Company and Metropolitan Express, the platform is neutral. Moreover, the platform has passed the integrity
identification test of the National Network and Information Security Product Quality Supervision and Inspection Center, so its operational “Baoquan website” has the qualification as a third-party electronic preservation platform.

Fourth, review the storage of electronic data. As mentioned above, preservation by blockchain is based on hash operation and distributed storage, with high security and authenticity. However, it is not absolutely safe. It also needs to review the design of preservation by blockchain system, the selection of chain, and other technical issues. The review of technical reliability mainly includes the acceptability of technology itself, the matching degree of technology and application scenarios, etc. In “the first judgment of blockchain preservation,” the Hangzhou Internet Court calculated the hash value of packaging compressed file for screenshots, source code, and call information downloaded from the “Baoquan website.” By comparison, the value is consistent with the hash value of the electronic data submitted by Huatai Material Company from blockchain preservation platform. Therefore, it can be confirmed that the electronic data in question has been uploaded to the FACTOM blockchain and Bitcoin blockchain. And from transmission on the chain to the present, it is completely preserved and not modified.

Fifth, review the output and collection of electronic data. In this link, we should not only consider the safety and reliability of electronic data, but also pay attention to the requirements of the best evidence rules. Because of the particularity of electronic data evidence, most countries have moderately modified the original requirements. For example, Article 4 of Canada’s Uniform Electronic Evidence Act stipulates that an electronic record in the form of a printout that has been manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the printout, is the record for the purposes of the best evidence rule. Based on the particularity of electronic data evidence, some countries do not completely stay in the traditional requirements for authenticity, but pay more attention to the integrity of electronic data. In our country, Article 23 of “Provisions of the Supreme People’s Court, the Supreme People’s Procuratorate, and the Ministry of Public Security on Extracting and Reviewing Electronic Data in Criminal Case” specifies the method of verifying the integrity of electronic data. “Comparing the integrity checking value of electronic data” is clearly listed as one of the methods. And, hash value is a common integrity check value in practice, which provides a larger application space for hash operation and preservation by blockchain.

---

**Figure 1: Electronic data evidence review**

The diagram illustrates the review process of electronic data evidence with a flowchart, showing the relationship between evidentiary facts, inferred facts, and essential elements. It outlines the steps involved in verifying the authenticity and preservation of electronic data evidence.
Way of blockchain-stored evidence review

In order to ensure the authenticity and integrity of blockchain-stored evidence, it is necessary to implement specific review methods and procedures. Some scholars regard comprehensive comparative analysis, recognition, authentication, confrontation, and cross-examination as the specific methods of reviewing evidence. According to the characteristics of electronic data, this article briefly introduces the following ways:

First, authentication. If there is any objection to the authenticity of electronic data, it should be authenticated. Article 93 of the Provisions of the Supreme People’s Court stipulates that if there is any doubt about electronic data, it shall be appraised or tested. Article 11, Paragraph 3, of the Provisions of the Supreme People’s Court on Certain Issues in Internet Court Trial Cases stipulates that: “The parties may apply for the opinions of persons with expertise on the technical issues of electronic data. Internet courts may, on the application of the parties or according to the its jurisdiction, entrust the identification of the authenticity of electronic data or investigate other relevant evidence for verification.” In the first judgment of blockchain preservation, the Hangzhou Internet Court has made judicial appraisal on relevant professional issues in order to ensure the reliability of technology. Qianmai Authentication Institute confirmed the technicality of using puppeteer and curl programs for web page screenshots and source code calls. Therefore, in the absence of evidence to the reverse, the court held that the “Baoquan website” was reliable in generating and storing data messages by using the public version of Google’s open-source crawler to perform domain name resolution on the target page.

Second, cross-examination. Factual finding is indispensable from cross-examination, just as Wigmore said, “Cross-examination is undoubtedly the greatest legal engine ever invented for the discovery of truth.” It plays an important role in factual finding. “In theory, the adversarial system gives the fact finder the advantage of utter impartiality arising from his or her ignorance of the case. Although it is not the responsibility of a party to present the tribunal with the truth, only with his or her case, it is argued that the vigorous pursuit of evidence to serve the same interests, when added to that of the opponent, is an effective means of discovering the truth, particularly as the tribunal witnesses the attack by each side upon the evidence of the other.”

Third, comparative analysis and verification methods. The fact finding needs to be based on a complete evidence chain. The evidence in the entire evidence chain should be mutually verified to exclude contradictions. Article 104, Paragraph 3, of the Interpretation of the Supreme People’s Court on the Application of the Criminal Procedure Law of the People’s Republic of China stipulates that only when there is an intrinsic link between the evidences, pointing to the same facts to be proved, and there are no unavoidable contradictions and unexplained doubts, can they serve as the basis for the fact finding. Article 66 of the Provisions on Evidence in Civil Procedures of the Supreme People’s Court stipulates that: “The judges shall make a comprehensive examination and judgment of all evidences from the degree of connection of each evidence with the fact of the case and the relations between the evidences.” In “the first judgment of blockchain preservation,” the Hangzhou Internet Court insisted that “a case study should be conducted to examine the correlation between the evidences.”

Conclusion

The traditional methods of nononline preservation such as printing, detaining, and sealing the original storage media are greatly influenced by the operators. Moreover, the traditional methods are lagging and are less efficient, which cannot effectively meet the requirements of evidence preservation in the era of big data. Online preservation methods such as cyber notary authority, time stamp certification, and preservation by blockchain can effectively guarantee the authenticity and security of electronic data and will be more and more widely used in future. Online preservation can be divided into centralized online preservation and noncentralized online preservation. The former mainly refers to network notarization, time stamp certification, and so on, whereas the latter refers to preservation by blockchain. Based on the characteristics of distributed storage, decentralized online preservation has higher security than centralized online preservation. However, it should be acknowledged that the current blockchain technology itself is not mature and the preservation by blockchain is not without risk. The court should adhere to the principle of individual review of each case and review the electronic data from its generation, transmission, reception, storage, and collection. Looking to the future, preservation by blockchain will gradually be applied in a wider range, but it cannot completely replace other methods of evidence collection and preservation. In a long period of time, centralized online preservation and noncentralized online preservation will complement each other and jointly build an effective online preservation system for electronic data.

Financial support and sponsorship

This thesis is supported by the “NCUT Beijing Urban Governance Research Base,” “Beijing University Innovation Training Project.”

Conflicts of interest

There are no conflicts of interest.

References

1. Article 28 of “Provisions of the Supreme People’s Court, the Supreme People’s Procuratorate, and the Ministry of Public Security on Extracting and Reviewing Electronic Data in Criminal Case. Available from: http://newspaper.jcrb.com/2016/20160921/20160921_003/20160921_003_2.htm. [Last accessed on 2018 Dec 27].
2. Baosheng Z. Evidence Law. 3rd ed. Beijing: China University of Political Science and Law Press; 2018. p. 186-7.
3. Jiahong H. Evidence Law. 5th ed. Beijing: Law Press; 2013. p. 223.
4. Muzerak HJ. The Basic Course of German Civil Procedure Law. Translated by Zhou Cui. Beijing: China University of Political Science and Law Press; 2005. p. 279.
5. Article 81 of The Civil Procedure Law of the People’s Republic of China. Available from: https://www.66law.cn/tiaoli/12.aspx?from=groupmessage&isappinstalled=0. [Last accessed on 2018 Dec 27].
6. Article 46 of Arbitration Law of the People’s Republic of China. Available from: https://www.sohu.com/a/169066427_627120. [Last accessed on 2018 Dec 27].
7. Jifu W. Research on Civil Science and Technology Evidence. Beijing: Intellectual Property Publishing House; 2012 p. 236.
8. Jiahong H. Research on Electronic Evidence Law. Beijing: Law Press; 2002. p. 97.
9. Available from: https://baike.baidu.com/item/时间戳/6439235?fr=aladdin [Last accessed on 2018 Dec 27].
10. Zhenlin W. Electronic Evidence. Beijing: China University of Political Science and Law Press; 2016. p. 147.
11. Noguchi Y. Blockchain Revolution: The Emergence of Distributed Self-Disciplined Society. Translated by Han Pigeon. Beijing: Oriental Publishing Press; 2018. p. 13.
12. Noguchi Y. Blockchain Revolution: The Emergence of Distributed Self-Disciplined Society. Translated by Han Pigeon. Beijing: Oriental Publishing Press; 2018. p. 58-9.
13. Swan M. Blockchain: New Economic Blueprint and Guide. Beijing: New Star Press; 2018. p. 105.
14. Zhenshan L. Research on the block-chain based method of electronic certificate deposit with integrity. Vol. 12. Hangzhou: Computer Era; 2019. p. 2.
15. Min G. Hangzhou Internet Court first recognized the legal effect of blockchain electronic certification. 1st ed. Hangzhou: Published in Zhejiang Legal Newspaper; 29 June, 2018.
16. Available from: http://dy.163.com/v2/article/detail/DVK30JSL0519U315.html. [Last accessed on 2018 Dec 27].
17. Available from: http://www.sohu.com/a/280760699_115060. [Last accessed on 2018 Dec 27].
18. Wei Z. The Court has Built a Blockchain and Deposited 180,000 Certificates in Three Months. 5th ed. Beijing: The Legal Evening News; 23 December, 2018.
19. Available from: https://tech.sina.com.cn/roll/2018-10-20/doc-ihmrasq8603944.shtml. [Last accessed on 2018 Dec 27].
20. Jie L. Research on the present situation of internet court and block chain evidence collection. J Sichuan Vocat Tech Coll 2019;3:17.
21. Noguchi Y. Blockchain Revolution: The Emergence of Distributed Self-Disciplined Society. Translated by Han Pigeon. Beijing: Oriental Publishing Press; 2018. p. 120.
22. Swan M. Block Chain: New Economic Blueprint and Guide. Beijing: New Star Press; 2018. p. 105.
23. Noguchi Y. Blockchain Revolution: The Emergence of Distributed Self-Disciplined Society. Translated by Han Pigeon. Beijing: Oriental Publishing Press; 2018. p. 58-9.
24. Beijing High People's Court Answers to Several Questions Concerning the Application of Evidence in Civil Litigation of Intellectual Property Rights(2007)[No.101] Available from: http://www.010-lawyer.com/falv_show.asp?news_id=1508. [Last accessed on 2018 Dec 27].
25. Lixia L. Review and judgment of the authenticity of electronic evidence. J Yunnan Univ 2003;2:113.
26. Allen RJ, Kuhns RB, Swift E. Evidence Law: Texts, Questions and Cases, Zhang Baosheng, Wang Jinxi, Zhao Wei Translation. Beijing: Higher Education Press; 2006. p. 265.
27. See Details of the Judgment in this Case. Available from: https://www.jinse.com/bitcoin/207282.html. [Last accessed on 2018 Dec 27].
28. Qiannan C. Judicial Application of Blockchain Certificates of Electronic Data. Vol. 4. Beijing: People's Justice; 2009. p. 85.
29. Zhihai X. Research on the Legal System of Network Evidence and Preservation. Beijing: Law Press; 2013. p. 135.
30. Bo H. On the Legislative Value of Canada’s Unified Electronic Evidence Law. Shanghai: Political Science and Law; 2001
31. Jinyou L. Evidence Law. 1st ed. Beijing: China University of Political Science and Law Press; 2001. p. 481-502.
32. See the Judgment in this Case. Available from: https://www.jinse.com/bitcoin/207282.html. [Last accessed on 2018 Dec 27].
33. Wigmore JH. Evidence in Trials at Common Law, 1 Tillers Review Boston; 1983. p. 608.
34. Mcewan J. Evidence and the Adversarial Process. Oxford: Blackwell Publishers; 1992. p. 6.