https://doi.org/10.37420/j.mlr.2024.019

Analysis on Challenges and Improvements of Electronic Evidence Preservation on Blockchain in China

Tianying Lin*

Institute of Evidence Law and Forensic Science, China University of Political Science and Law, Beijing, China.

***Corresponding author,E-mail:2202260326@cupl.edu.cn**

Abstract

Technological innovation has always been a key factor in national development. Since moving into the Internet era, all walks of life have begun to explore ways to integrate with the Internet in order to achieve innovation and transformation, and the judicial field is no exception. In terms of the preservation of digital data, the judicial industry of China has combined with blockchain technology to make certain explorations and innovations. Blockchain technology was first widely used in the financial industry, but it can also play a unique role in the field of digital data's storage and authentication, due to its decentralisation and tamper-proofing and other technical features. However, there are still some specific challenges in the practical application of blockchain technology in the judicial field of China. On the one hand, some traditional concepts are still deeply rooted, such as the reliance on the original rule and the notary system. On the other hand, there are some shortcomings of blockchain technology itself, when applying it to preserve electronic evidence. In order to solve these difficulties faced in practice, traditional concepts of electronic evidence should be transformed, and a decentralised proof model should be developed to eliminate the reliance on traditional identification procedures. At the same time, with a view to guaranteeing the integrity and diversity of the electronic evidence preserved in blockchain, there is a need to explore ways to optimise relevant complementing system and to broaden the forms of data that can be stored on blockchain.

Keywords

Blockchain Technology, Electronic Evidence Preservation, Digital Data

1 Introduction

In the first few years after digital data was formally regulated in the major procedure law in China, the courts were very conservative in their treatment of electronic evidence, and the use of it was very restricted. This is due to the fact that its inherent vulnerability makes it easy to challenge its authenticity in judicial practice. In the face of this problem, regular methods of electronic evidence preservation have many shortcomings and heavily relies on identification procedures such as notarisation. Blockchain, characterised by decentralisation, tamper-proofness and traceability, is another important emerging technology for the current society with highly developed Internet technology. It is well suited for application in digital data storage and provides a new opportunity to solve the problem of electronic evidence authentication.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

In the context mentioned above, China's judiciary has responded to the development of the information age with the establishment of the Internet Court, and in 2018 the Supreme People's Court (SPC) issued the Provisions on Several Issues Concerning the Trial of Cases by Internet Courts, which points out the direction for the judicial application of blockchain technology. The legislation stipulates that: The Internet court shall confirm the electronic data submitted by the party concerned, provided that the authenticity of the electronic data can be proved through electronic signature, trusted time stamp, hash value check, blockchain or any other evidence collection, fixation or tamper-proofing technological means, or through the certification on an electronic evidence collection and preservation platform.This provision indicates that, in addition to existing technologies such as electronic signatures, trusted time stamps and hash value check, blockchain technology can also be used to prove the authenticity of digital data. These technologies can be used either individually or in combination. The Internet court shall confirm the digital data that has been collected and preserved using such technical means and is capable of proving its authenticity. According to the above legislation, the determination of the authenticity of digital data breaks through the limitations of traditional authentication procedures and expands the path of application of electronic evidence.

Rules of Online Litigation of People's Courts, which were issued and implemented in 2021, further made more detailed provisions on the review of electronic data's validity and authenticity based on blockchain. It affirms the authenticity of electronic data after it has been collected and preserved on blockchain and has been technical verified. In addition, in the event of any objection to the authenticity of the data, the rule also stipulates the basis of review from the perspective of the evidence preservation platform, the evidence preservation technology and so on. In terms of reviewing the authenticity of specific data, the rule make a binary division between data before and after it is stored by blockchain technology, but the authenticity review provisions for before it is preserved on blockchain are too sketchy and prone to bias in practice.

The research related to blockchain evidence preservation is not yet sufficient, but some representative results can still be summarised. There is a view that blockchain evidence can be classified according to the external pattern, which can be divided into blockchain-generated evidence, blockchain-stored evidence and blockchain-verified evidence. It's important to note that when applied to electronic data preservation as a technology-based means of authentication, blockchain technology can only guarantee the formal authenticity of electronic data after uploading, but not the substantive authenticity of electronic evidence.From the perspective of the stage of electronic data preservation, a binary review model should be constructed by combining the different characteristics of electronic data before and after storing on blockchain.However, in terms of the review of the authenticity, reliability and other elements of electronic evidence stored on blockchain, there is a lack of uniformity in the application of the law, and the industry standards, review rules and other norms need to be refined in the future.

Overall, it is still in its infancy when it comes to the application and regulation of blockchain technology in evidence preservation in China. From the practical side, the existing legal system has not been able to respond in a timely manner to the problems that have arisen in judicial practice; from the theoretical side, research is at a preliminary stage of exploration, and the academic community has not reached a consensus on many theoretical issues. In this context, this article intends to sort out the principle of the use of block-

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

chain in evidence preservation, reflect on the limitations of the use of blockchain technology in China, and then put forward the corresponding optimisation path for the judicial dilemma currently faced.

2 Principles of Applying Blockchain to Evidence Preservation

Based on the tamper proof nature of blockchain technology, the use of blockchain depository platforms to store electronic evidence can provide a strong guarantee for the authenticity of digital data. In other words, the inherent vulnerability of electronic data, when uploaded to the blockchain, will be replaced by the reliability conferred by the technology. In order to effectively overcome the difficulties in collecting, preserving and authenticating evidence, the SPC launched the Unified Judicial Blockchain Platform in 2019. Furthermore, an unprecedented opinion on the judicial application of blockchain was issued by the SPC in May 2022, filling the institutional gap of blockchain application in the digital field of judiciary.

2.1 Type of Blockchain Evidence

Blockchain evidence and evidence preserved on blockchain are two similar expressions often used in theory and practice, but their meanings are different. Blockchain evidence can be understood as digital data recorded on the blockchain, including data generated on the blockchain itself, such as transaction data of cryptocurrency, but also including data stored by blockchain technology. As to evidence preserved on blockchain, it uses a new technical means of evidence preservation, and the evidence involved is usually generated off chain and then transmitted up-chained data, and the off-chained data includes electronic data and electronic materials. No matter which kind of evidence, it should be encrypted by hash into a block, and the new block would be sequentially added to the chain according to different timestamps. The new block can store digital pieces of information and is saved in all nodes of the chain almost without delay. The hash function is characterised by the fact that any slight change in the input value produces a different result, so the judge can verify whether the evidence submitted by the parties has been tampered with by comparing the hash code.

2.2 Verification of Blockchain-related Evidence

According to Rules of Online Litigation of People's Courts, electronic data and electronic materials need to be verified for authenticity, legality and relevance, and can only be used as the basis for finding out the facts of the case after verification.Electronic data and electronic materials, even after evidence preservation by blockchain technology, still essentially belong to the category of digital data, and their verification still follows the examination requirements of authenticity, legality and relevance.

In the first place, the examination of authenticity has always been the difficulty of traditional digital data authentication, and the examination of authenticity of digital data preserved on blockchain mainly focuses on the three aspects of carrier authenticity, data authenticity and content authenticity.First, in the traditional mode, the authenticity of the carrier is mainly verified by examining the originality, homogeneity and integrity of the storage medium of digital data.In practice, priority is given to the seizure and sealing of the original storage medium, and when the original storage medium is inconvenient to seized and sealed, the data

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

will be fixed by extraction, freezing and other ways. This traditional approach requires the participation of multiple links and subjects, which inevitably leads to security loopholes, thus consuming more resources. Preservation by blockchain has broadened the form of the carrier of digital data, so that it is no longer limited to the original carrier to determine the authenticity of digital data. Although the originality of the carrier is the first choice to verify the authenticity of the carrier, the special design of blockchain technology can ensure the security of data stored on the chain, and preservation by blockchain can effectively determine the authenticity of the carrier of the digital data, and it can be used in a more low-cost and high-efficiency way compared with the traditional mode. Second, the authenticity of the data can be judged intuitively through blockchain technology. As mentioned earlier, any slight change in the original data will lead to different output hash code, and the block information on the chain is stored in all the nodes almost simultaneously, making it difficult to replace the preserved data by tampering with the block information. Therefore, in practice, the authenticity of the data can be judged by simply comparing the hash codes. Third, the authenticity of the content of the electronic evidence means that the content reflected in the digital data can be corroborated with other evidence, thus playing a role in proving the facts of the case. Whether the content of the data at the time of generation is objectively true does not involve the process of data storage and transmission, and blockchain technology can only provide formal protection for the storage of digital data on a technical level, but it cannot guarantee the authenticity of the content. If the content of the data is true before uploading, the blockchain technology can guarantee the authenticity of the content after storing; and if the data does not have the authenticity of the content before uploading, the preservation is just fixing a piece of fake data. Therefore, in judicial practice, priority shall be given to the examination of whether the content of electronic evidence is authentic before it is stored on blockchain.

In the second place, the legitimacy of blockchain technology as a means of preserving evidence was clarified in Provisions of the Supreme People's Court on Several Issues Concerning the Trial of Cases by Internet Court in 2018, which states that in terms of the examination of the legitimacy of digital data, its evidentiary status shall not be negated due to the fact that it is stored on blockchain rather than on the original carrier.In practice, it is the examination of the legitimacy of the evidence preservation platform that is the focus of the legitimacy review of evidence stored on blockchain. The application of blockchain technology to evidence preservation in China originated from preservation platforms developed by third-party companies whose neutrality and credibility are clearly insufficient, and thus the companies' qualification capabilities, technical level, neutrality and other comprehensive circumstances may have an impact on the legitimacy of the preservation platforms. After the national and regional courts actively constructed the official evidence preservation platform, the legitimacy of the relevant preservation companies was resolved accordingly, as they needed to pass certain qualification examinations before they could access the evidence preservation platform. For example, in order to safeguard judicial authority, access to the Hangzhou Internet Court electronic evidence platform needs to pass a number of examinations, such as capacity certification, market verification, and operating environment.Therefore, through the effective management of the official evidence preservation platform, the legitimacy of the preservation by blockchain technology is guaranteed.

Last but not least, digital data preserved by blockchain do not materially affect the verification of the relevance of it. The relevance of traditional evidence mainly refers to the degree of correlation between the

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

evidence and the facts to be proved. Although the digital data is stored in a virtual space of blockchain, its content has not changed due to the tamper-proof nature of blockchain technology. Therefore, compared to traditional preservation methods of electronic evidence, the use of blockchain technology does not enhance or weaken the degree of relevance between the stored digital data and the facts to be proved.

3 Difficulties of Evidence Preservation on Blockchain

Preserving electronic evidence with the help of blockchain technology is also known as one of the highlights of judicial reform, but in practice the advantages of blockchain technology have not been fully brought into play, and it is only the traditional electronic data that is covered with the outer skin of blockchain technology. As Tianping blockchain real time publicity showed, the number of digital data collection was 297594248, while the number of electronic evidence verification was 32738. (The above data is available as of 12 August 2024.) Meanwhile, searching with the keyword of blockchain in the PKU Law platform, only 346 of the 134800 judgement documents of Beijing Internet Court were obtained. Since blockchain is technically complementary to the weaknesses of the authenticity of digital data, why is there so little data on the use of the trial? Even if some of the data is pre-litigation preservation, blockchain-related cases are still far from the overall number of cases. This problem arises mainly because evidence preservation by blockchain has both practical and functional limitations.

3.1 Practical Challenges of Evidence Preservation on Blockchain

3.1.1 Controversies over Standards for the Original of Digital Data

Due to the theoretical controversy related to the original rule of digital data, judges would be suspicious of the authenticity of digital data, and would unilaterally believe that digital data are very easy to be tampered. The examination of digital data will also focus on whether the original storage medium has been transferred, and the state of impoundment and storage under seal of the original storage medium. The application of blockchain technology to electronic evidence preservation would also be caught in these theoretical disputes. In the field of electronic evidence, is it meaningful to distinguish between copies of originals? Some countries have amended their laws to fit the attributes of digital data. In Canada, digital data are considered to be originals as long as they functionally have the same effect as the originals. As for the electronic evidence preservation by blockchain, what is the difference between the validity of an original digital data and the copy of it?

According to those who advocate that the digital data preserved by blockchain belong to the original, based on the technical characteristics of computers, digital data can be reproduced in its entirety as a copy with the same function as the original data. In the case of normal operation of the system and non-interference in the reproduction process, if the digital data is reproduced in its entirety, it can be considered that the reproduction of the data has the same evidentiary effect as the original, regardless of whether the data is carried on the original storage medium. Thus, as long as the digital data is reproduced in its entirety and has the same function, the data preserved by blockchain can be regarded as the original electronic evidence. However, those who advocate that the digital data preserved by the blockchain belongs to the replica be-

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

lieve that the generation, storage and transmission of digital data are carried out under the binary system of computer, which is a process that cannot be directly perceived by human beings, and that therefore the digital data used after transformation, such as screenshots and photographs, are already replicas in its nature, not originals.

3.1.2 Recognition of the Original of Digital Data in Practice

In judicial practice, the collection of the original electronic evidence is not an easy thing, therefore, the evidentiary validity of digital data copies is recognized by the judiciary in practice, but would still be strict examined and judged. In the two views mentioned above, neither the original supporter nor the replica supporter has noticed the new development of the original rule in the context of blockchain technology. The decentralised ledger technology of blockchain is a reversal of the original rule. On the blockchain, the data in a new block is stored by all nodes with almost no delay. If the data of the node that packages and uploads the block information is taken as the original, the data saved by other nodes with synchronised updates is the replica, but when a new block is generated and uploaded by other nodes, the replica stored by the new node becomes the original, while the original of the previous node becomes the replica. This would create the paradox that when there is a need to collect block data that was once uploaded by a node, the existing blockchain is necessarily a replica. Therefore, the original rule in traditional evidence jurisprudence cannot be applied to the field of electronic evidence preserved by blockchain.

Not all electronic evidence can be found in the original storage medium in practice, so the relevant judicial interpretations in China provide for the rule of recognition under specific conditions or premises with respect to the probative value of digital data copies.The principle behind this rule is that the legislature has sacrificed the actual probative value of some electronic evidence in order to solve the problem of evidence collection in practice. This is a compromise solution to the current problem of the difficulty of collecting original electronic evidence, but it is also the best solution that can be practicable in practice. Regardless of other factors, the original digital data is indeed more conducive to the examination of its authenticity than the copy, thus helping the judge to make a comprehensive judgement on the case. However, the lack of probative value of copies is only relative to the possibility of tampering or distortion of the original. In the field of blockchain, all nodes of the block data are synchronously updated to maintain consistency. From the perspective of the probative value of evidence, it is no longer worth distinguishing between originals and copies, and the original storage medium is no longer necessary for the integrity and authenticity of the digital data. If this theoretical breakthrough cannot be recognised, the application of blockchain technology to electronic evidence preservation would still be in the shackles of traditional mode.

Unfortunately, the above advantages of blockchain technology have been neglected in the practice of electronic evidence preservation. When judges examine and judge digital data, the authenticity, integrity, and legality of it need to be verified one by one, and in practice, the questioning about digital data preserved on blockchain still focuses on the aspect of authenticity. Parties and judges prefer to convert digital data into traditional forms, and electronic evidence used as the basis for cases are often notarised or corroborated by other evidence. Even with regard to digital data preserved by blockchain technology, judges are cautious and do not take full advantage of the tamper-proof feature of blockchain to give full play to the advantages

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

offered by the new technology. This has led to the technical advantages of blockchain in the practice of evidence preservation in name only.

3.2 Functional Limitations of Evidence Preservation on Blockchain

3.2.1 Dichotomy in the Evidence Preservation Phase

The problems faced in practice are partly due to the functional limitations of blockchain technology when introduced into electronic evidence preservation. As mentioned previously, blockchain cannot guarantee the authenticity of digital data before it is preserved on blockchain. The distributed storage, hash function and other underlying technologies used in blockchain can guarantee the tamper-proof and traceability of the data on the chain, but it cannot guarantee the authenticity of the content of the data, which is a problem that cannot be avoided due to the dichotomy between the generation and storage stages of digital data. If the data has been deleted or altered before collecting and storing on blockchain, even if blockchain technology ensures that the data has not been tampered with on the chain, the result of the evidence preservation is nothing more than the fixing of a piece of evidence whose content is false. Therefore, electronic evidence preserved on blockchain still needs to be examined for authenticity in stages, which is undoubtedly a weakening of the functional advantages of blockchain technology.The most typical feature of blockchain technology is decentralisation, as the information packed into the block is consensually formed by the nodes on the chain, which ensures the authenticity of the content of the information. However, when the blockchain technology is applied to the electronic evidence preservation, its consensus mechanism has changed. The decentralisation of blockchain appeared dichotomous pattern, that is, only can achieve the tamper-proofing on the chain, but does not guarantee the authenticity of the data when it is to be uploaded.

3.2.2 Risks of Consortium Blockchain

The blockchain technology applied in electronic evidence preservation at this stage is not truly decentralised. After the 2008 financial crisis and the collapse of government credit, one person or organisation under the pseudonymous name Satoshi Nakamoto designed Bitcoin, which is introduced as “a peer-to-peer electronic cash system” without the participation of a trusted third party.It relies on blockchain distributed bookkeeping, asymmetric encryption, trusted timestamps, hash function, and other technologies to build a decentralised trust architecture. Bitcoin was the occasion for blockchain technology to attract widespread attention around the world. When it comes to blockchain technology, it generally refers to this completely decentralised architecture, i.e. the public blockchain, which is open to everyone, and every user with an account is a core node on the chain. With the development of blockchain technology, it has been integrated into all aspects of social life. In addition to public blockchain, there are also consortium blockchain and private blockchain, which are not decentralised like the public blockchain. The consensus mechanism of the consortium blockchain only sets some of the users on the chain as the core nodes, and only the core nodes have the ability to write blocks, weakening the decentralised structural design of the public blockchain. The private blockchain completely loses the decentralised function of the blockchain technology, and it is only for the internal use of individuals or a certain company.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

The electronic evidence preservation platform built by China's Internet Court belongs to the consortium blockchain on the principle of blockchain technology, and its security is not as reliable as that of the public blockchain. If more than half of the nodes on the consortium blockchain are attacked, the block data on the consortium blockchain would face the risk of being tampered with. All in all, caution should be emphasised with regard to the system security of consortium blockchains. The design of the consensus mechanism of the public blockchain makes it almost non-existent to attack more than half of the nodes and be able to continuously write new blocks, while the limited number of nodes of the consortium blockchain makes the risk of such an attack increase substantially, so its technical security is much lower than that of the public blockchain.

4 Institutional Optimisation of Evidence Preservation on Blockchain

Based on its decentralisation and other underlying technologies, blockchain has the characteristics of high trustworthiness, strong anti-tampering and traceability. The biggest role of blockchain technology in evidence preservation is to enrich the way of traditional electronic evidence collection, preservation and authentication in judiciary, and at the same time, simplify the rules of judge's review of electronic evidence, so as to change the reliance on people and things to the trust based on technology.In order to maximise the role of blockchain, it is necessary to change the concept of the use of electronic evidence and improve the supporting system of evidence preservation upon blockchain.

4.1 Shifting the Mode of Electronic Data Application

4.1.1 Reducing the Reliance on Third Parties

When the authenticity of electronic evidence is disputed by any of the parties, the data certified by the notarial institution have a significant advantage in trials due to their endorsement by the State's credibility. The rate of admissibility of electronic evidence has increased significantly after the use of the notary procedure, which shows that notarisation plays an important role for the credibility of electronic evidence. A notarial office is a lawfully established non-profit-making certification institution, and notarisation is one of the most common ways of proving authenticity in Chinese litigation. As long as the matter is within the scope of notarisation under any law or administrative regulation, the notarial office shall carry out the notarisation upon application by the party concerned. In practice, in addition to providing the original digital data, the party providing the data would also generally provide other evidence which can play a supporting role in order to strengthen the authenticity of the electronic evidence, and thus strengthen the proof of the facts to be certified. In addition to notarisation, the common way of proving authenticity is to apply for forensic identification and request for expert clarification. These are all centralised proof model that relies on a neutral third party, and are all aimed at affirming that the relevant evidence is the original state without tampering, so as to maximise the possibility of proving the credibility of the evidence.

In the first case where blockchain technology was used for evidence preservation, in addition to submitting the digital data stored on blockchain, the plaintiff also applied for forensic identification, which indicates the importance of notarisation, forensic identification and other procedures in verifying the au-

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

thenticity of electronic evidence. Although there is no mandatory requirements for supplementary proof of digital data, but the lack of notarisation and other supplementary proof would often make the authenticity of digital data in an unfavourable position. Due to the tamper-proof feature of blockchain technology itself, its self-authentication is a new feasible and credible way of examining the authenticity of digital data that has been recorded by the evidence preservation of blockchain technology. In the early stage of the development of new technology, there is a slow acceptance process for those who are used to traditional technology. However, notarisation and other traditional procedures are long and costly, and it is difficult to meet the massive and immediate demand for electronic evidence preservation in the context of the big data era. The blockchain-supported evidence preservation, with strong technical reliability and lower cost, could play a better role, which is precisely a task being promoted by the judicial reform at this stage.

4.1.2 Developing the Decentralised Proof Model

The absolute preference for traditional means of proof, such as notarisation, is in fact a strong illustration of trust in centralised demonstration. Notarisation is a very common and traditional mode of centralised demonstration, whereby the notarial institution uses the authority of the national credibility as a guarantee upon verification of the credibility of the evidence. The traditional centralised mode like notarisation has two dimensions of trust basis. From the perspective of legitimacy, the notarisation institution is legally authorised with the right to judge the credibility of the evidence. From the perspective of competence, there are a group of notaries with professional ability, which could gain the general recognition and trust of the society. However, the authority is not entirely reliable, and the loss of government credibility during the financial crisis is well known around the world. Moreover, the scope of admissibility of notarisation is limited, and when emerging issues arise, due to the lag in the knowledge base of notaries, notarisation is unable to give play to its advantages.

It was to get rid of the aforementioned centralised trust dilemma that Satoshi Nakamoto came up with the idea of Bitcoin. When a technology meets the conditions for self-authentication, there is no longer a need for additional official guarantees of authenticity from a centralised authority. With blockchain technology blooming, faced with an increasing amount of blockchain-related evidence, the authenticity should be judged in the light of the characteristics of blockchain technology. The decentralised underlying design of the blockchain itself is sufficient to ensure that the information recorded on the block is reliable in the absence of central authority. The application of blockchain technology to evidence preservation can replace the traditional procedures of preservation and notarisation, thus making the time, manpower, money and other judicial resources consumed in the traditional model can be greatly saved.

Overall, the centralised and authoritative verification of digital data plays an important role in verifying authenticity in an era when there is a lack of means of verification. However, when the use of blockchain technology has become a common global trend, the shift from national notarisation to technological self-authentication, and from centralised to decentralised modes, is both a new trend in the popularisation of technology and a new direction for judicial reform. Applying blockchain technology to evidence preservation can save judicial resources and also improve judicial efficiency. The application of blockchain technology in evidence preservation should be encouraged in practice to bring into play the advantages of blockchain technology and promote the diversified development of evidence preservation methods.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

4.2 Improving the Supporting System for Evidence Preservation on Blockchain

From the perspective of the national development of vigorously promoting blockchain plus, the in-depth integration of blockchain technology and justice is the future direction of judicial science and technology innovation.In the future, the number of litigation cases using evidence preservation by blockchain would gradually increase, and courts at all levels would also join the construction of blockchain platforms of evidence preservation one after another, therefore, the improvement of the relevant supporting system becomes particularly important.

On the one hand, it is necessary to regulate the integrity of digital data before uploading to blockchain. As mentioned earlier, the inability to guarantee the authenticity of digital data before being stored on blockchain is one of the functional limitations of evidence preservation by blockchain. Therefore, the first issue to be considered in evidence preservation on blockchain is how to determine the authenticity of the digital data before accessing to the chain. In practice, if no party objects to the authenticity of the digital data before being recorded and stored on blockchain, the judge would presume that it is true. However, in order to substantially improve the authenticity of electronic evidence before being stored on blockchain, it is still necessary to build a relevant supporting system of evidence preservation on blockchain. The premise of improving the authenticity of digital data before being recorded and stored on blockchain is to guarantee the integrity of the data. When digital data are generated in original storage medium, in addition to the data itself, they are accompanied by computer affiliated information and associated traces, which can assist in the confirmation of the authenticity of electronic evidence. Therefore, when digital data are collected and stored on blockchain platform of evidence preservation, it could be required to package and store its affiliated information and associated traces together, which is conducive to assisting in confirming the integrity of the digital data through the affiliated information and associated traces, so as to provide a comprehensive judgment of the process of generating the digital data before being recorded and stored on blockchain.

On the other hand, the forms of evidence for blockchain platform of evidence preservation can be expanded. It should be recognised that not all electronic evidence used in litigation is generated from computer systems. There is a phenomenon in practice where traditional forms of evidence, such as documentary evidence, are converted into the form of electronic data by means of photographs, scans, etc., and then used in litigation. There is a dispute as to whether this type of evidence is electronic data under the category of evidence law, and therefore it is generally referred to as digitalised evidence. There is a dispute in the academic community as to whether this type of evidence is electronic data under the category of evidence, which is generally referred to as electronic evidence. It should be noted that the Hangzhou Internet Court has included it in the scope of electronic evidence. It is stipulated in the Norm that electronic evidence, including digital data and other digitalised evidence, can also be applied to blockchain platform of evidence preservation. With the advancement of the construction of the Internet Court and online litigation, in case the loss of original evidence, there is such a demand for traditional evidence to be electronically stored on the blockchain platform for evidence preservation. Therefore, by expanding the scope of evidence preserved on blockchain and including digitalised evidence in the blockchain platform of evidence preservation, the application of blockchain technology on evidence preservation can be uniformly regulated and the evidence preservation based on blockchain can be specifically optimised.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

5 Conclusion

There is a divergence between technocracy and rule of law regarding the values behind evidence preservation via blockchain technology. There is a view that technical truth was different from the truth of the case pursued in litigation, and that over-reliance on technology would ignore the standard of proof in the evidence theory, fearing that technocracy, with its emphasis on efficiency, could not guarantee the authority of the law. There are also views that since the trend of technological development is unstoppable, it is better to actively make good use of technology to improve judicial efficiency. When legal issues and technical issues collide, they are not in an antagonistic relationship, but can cooperate with each other in order to achieve a win-win situation.The value of the application of blockchain in electronic evidence preservation not only lies in the technical leap, but more importantly in the technology-driven changes in the evidence theory and the innovation of the traditional system. Much practical experience has been accumulated in the initial exploration of the application of blockchain in electronic evidence preservation in China, and this should be used as the basis for the next step, to accelerate the innovations from technological field to institutional field, and to create a higher level of judicial civilisation in the new technology era.

References

[1]Provisions of the Supreme People's Court on Several Issues Concerning the Trial of Cases by Internet Court, Article 11.

[2]Rules of Online Litigation of People's Courts, Article 16.

[3]Rules of Online Litigation of People's Courts, Article17.

[4]Rules of Online Litigation of People's Courts, Article 18.

[5]Liu Pinxin. (2021). On Blockchain Evidence. Chinese Journal of Law, 43(06), 130-148.

[6]Xie Dengke. (2021). The Legal Nature and Applicable Boundaries of Electronic Data Preserved by Blockchain. Lanzhou Academic Journal, (12), 5-15.

[7]Wang Yin & Liu Shaojun. (2022). A Research on the Construction of the Binary Review Model of Blockchain Evidence. Journal of Anhui University (Philosophy and Social Sciences Edition), 46(04), 109-117.

[8]Hu Meng. (2021). Analysis of the effectiveness of blockchain-based electronic evidence and its path to normalization. Evidence Science, 29(01), 31-40.

[9]Xie Dengke. (2021). The Legal Nature and Applicable Boundaries of Electronic Data Preserved by Blockchain. Lanzhou Academic Journal, (12), 5-15.

[10]Rules of Online Litigation of People's Courts, Article 15.

[11]Chu Fumin. (2018). Three Dimensions of Authenticity of Electronic Evidence. Chinese Journal of Law, 40(04), 121-138.

[12]Huang Peng. (2021). Blockchain Guarantees the Authenticity of Evidence: the Fit of Technology and Demand. Journal of Dalian University of Technology (Social Sciences), 42(04), 96-104.

[13]Hu Meng. (2021). Analysis of the effectiveness of blockchain-based electronic evidence and its path to normalization. Evidence Science, 29(01), 31-40.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

[14]Norms for Electronic Evidence Platform of Hangzhou Internet Court (For Trial Implementation), Chapter 2.
[15]Liu Pinxin. (2020). On the Institutional Value of Electronic Data's Storage and Authentication Based on Blockchain. Archives Science Bulletin, (01), 21-30.
[16]Interpretation by the Supreme People's Court Regarding the Application of the Criminal Procedure Law of the People's Republic of China (2021), Article 110-111.
[17]Liu Pinxin. (2009). On the Original Rule of Electronic Evidence. Science of Law (Journal of Northwest University of Political Science and Law), 27(05), 119-127.
[18]Liu Zhewei. (2015). On the independence of electronic evidence in civil procedure: from text to substance. Evidence Science, 23(06), 678-685.
[19]Provisions by the Supreme People's Court on Evidence in Civil Procedures (2019), Article 23.
[20]Li Haixin. (2024). The Chinese Path of Authenticating Electronic Data with Blockchain Technology. Academic Exchange, (02), 80-92.
[21]Satoshi Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
[22]Gong Shanyao. (2023). Function Clarification and Practice Development of Electronic Evidence Blockchain Storage. Journal of Dalian University of Technology (Social Sciences), 44(05), 111-119.
[23]Wang Yin & Liu Shaojun. (2022). A Research on the Construction of the Binary Review Model of Blockchain Evidence. Journal of Anhui University (Philosophy and Social Sciences Edition), 46(04): 109-117.
[24]Tong Feng. (2017). Study on the Electronic Signature Notarisation System: From the Perspective of the Evidentiary Effectiveness of Digital Data. China Notary Journal, (06), 35-39.
[25]See Case of Infringement on the Right to Communicate Works to Public over Information Networks (Hangzhou Huatai Yimei Culture Media Co., Ltd. v. Shenzhen Daotong Technology Development Co., Ltd.).
[26]Huang Zhen & Zhan Qing. (2020). The Court Practice and Rational Reflection of Technology Innovation of Justice: Empirical Research on the Innovation of Judicial Blockchain in China. Journal of Nanchang University (Humanities and Social Sciences), (03), 91-99.
[27]Subject Group of Jiangsu High People's Court. (2023). Judicial Application of Blockchain Technology with Background of Digital Economy. People's Judicature, (07), 91-95.
[28]Rules of Online Litigation of People's Courts, Article 18.
[29]Zhu Jianming, Zhang Qinnan & Gao Sheng. (2020). Research Progress of Blockchain Key Technologies and Their Application. Journal of Taiyuan University of Technology, (03), 321-330.
[30]Norms for Electronic Evidence Platform of Hangzhou Internet Court (For Trial Implementation), Article 4.
[31]Liu Pinxin. (2020). On the Institutional Value of Electronic Data's Storage and Authentication Based on Blockchain. Archives Science Bulletin, (01), 21-30.
[32]Luo Tianxuan & Tan Yufei. (2022). Analysis on the Application of Block Chain Deposit in China's Civil Online Litigation. Academic Exchanges, (05), 49-60.
[33]Chen Liyang. (2018). The Legal Reflection of Block Chain Research: Based on the Perspective of Knowledge Engineering. Oriental Law, (03), 100-108.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)