Authenticity Judgment of Electronic Data Stored in Blockchain

Qingxing Li
School of Taiyuan University of Science and Technology, Taiyuan 030000, China

Abstract

As the "preeminent form of evidence" in the age of networked information, the reliability and authenticity of case information contained within electronic data is paramount in ensuring the accuracy of facts and fairness of judgment outcomes. However, due to the inherent ease with which electronic data can be edited, tampered with, forged and verified without corresponding technical means to confirm its authenticity, its evidentiary value is greatly diminished. In instances where authenticity cannot be fully guaranteed, the evidentiary value of electronic data is called into question, leading to difficulties in verification and low acceptance by courts. The uncertainty brought about by both the digital era and global economic instability due to the pandemic has necessitated a transformation from industrial-era evidence law to digital-era evidence law. Blockchain-based electronic data certification has emerged as a solution to address these shortcomings. In June 2018, Hangzhou Internet Court announced China's first blockchain judicial deposit case. In June 2021, China's Supreme People's Court issued its Online Litigation Rules which clarified review standards for legal effect, validity scope and authenticity for blockchain-based electronic data storage. When evaluating the three characteristics of electronic data (authenticity, relevance and legality), court examination primarily focuses on authenticity. The use of blockchain-based evidence storage reduces disputes over the authenticity of electronic data during court proceedings and shifts the focus towards the relevance and legality of such data. This is clearly advantageous in improving court efficiency. In other words, the primary objective of blockchain-based certification storage is to address issues related to the authenticity of electronic data. Therefore, this paper will concentrate on analyzing existing problems and obstacles associated with assessing the authenticity of blockchain-based electronic data certification storage and will seek to identify improvements and countermeasures at various levels.

Keywords

Blockchain technology, Electronic data stored in blockchain, Authenticity judgment.

1. An Overview of Electronic Data Storage within a Blockchain Framework

1.1. The Implications of Blockchain Technology

Since its introduction in 2008 with the advent of Bitcoin, blockchain has become synonymous with emerging internet technology. From its inception, blockchain has been viewed as a potential replacement for traditional trust centers due to its inherent 'trustless' nature. Blockchain technology enables the separation of trust relationships from trust centers, resulting in the creation of a 'trustless' trust system.

Blockchain is a technical solution that is collaboratively maintained by multiple parties and utilizes cryptographic techniques to ensure its integrity. This solution enables multiple nodes within the system to record data generated within a specific time period in a data block using homomorphic encryption algorithms and timestamps. The data block key can then be used to verify the authenticity of subsequent data blocks generated in the same manner. In this way, all nodes within the system can collectively determine the veracity of data records across the entire blockchain.

Blockchain technology can be classified into three categories based on user scope: public chains, consortium chains and private chains. Public chains refer to consensus-based blockchains that are open to anyone. Private chains are non-public 'chains' that typically require authorization for node participation. Consortium chains refer to blockchains that are jointly managed by multiple institutions.

From a technical perspective, blockchain encompasses a range of scientific and technological disciplines including mathematics, cryptography, internet technology and computer programming. It represents a novel application of computer technology. At the application level, blockchain functions as a distributed shared database with data and information stored within it exhibiting characteristics such as decentralization, tamper-resistance, end-to-end tracking and traceability, collective maintenance and openness and transparency. Currently, countries around the world are actively developing blockchain technology and applying it to various aspects of social management. China's blockchain industry is also experiencing rapid growth.

1.2. The utilization of traditional electronic data in judicial proceedings presents significant challenges

The definition of electronic evidence within the judicial system can be categorized into two distinct interpretations: a narrow definition and a broad definition. The narrow interpretation primarily emphasizes the relationship between electronic evidence and telecommunication network service providers. In contrast, the broad interpretation encompasses all electronic storage information relevant to the case.

As a form of legal evidence, electronic evidence has become increasingly prevalent in court proceedings due to the rapid advancement of internet information technology. However, from a judicial practice perspective, there are significant challenges associated with the application of electronic evidence. These challenges primarily revolve around the authenticity of electronic evidence and can be divided into two main aspects. Firstly, the acceptance rate of electronic evidence is exceedingly low. Case analysis reveals that courts often reject electronic evidence due to their inability to comprehensively and accurately verify its authenticity. This may manifest as an inability to prove the objective authenticity or integrity of electronic evidence or to verify its upload time. Secondly, even when electronic evidence is accepted as evidence, it is often converted into material evidence, documentary evidence or verbal evidence for adoption by judicial organs. This effectively renders electronic evidence as a form of legal evidence non-existent.

1.3. The Implications of Electronic data stored in blockchain

Electronic data stored on a blockchain utilizes blockchain technology to address the challenges associated with the judicial application of traditional electronic data. The information storage and verification capabilities of blockchain technology are widely recognized within the industry as one of its most valuable derivative applications. In response to these challenges, several internet courts in China, including those in Hangzhou, Beijing and Guangzhou have implemented judicial blockchains to facilitate the storage of electronic evidence.

Electronic data stored on a blockchain possesses several distinct characteristics, including confirmability, repeatability, objectivity, stability and trace reinforcement within its carrier. Depending on the timing and method of blockchain technology intervention, it can be classified into three categories: generated blockchain electronic data, stored blockchain electronic data and network data verified using blockchain encryption verification technology. In recent years, several measures have been implemented to guide the innovative practice of internet courts and standardize the use of electronic data.

In September 2018, the Supreme People's Court issued provisions concerning the trial of cases by internet courts. In May 2020, the Ministry of Justice released technical specifications for electronic data storage. In June 2021, the Supreme People's Court published online litigation rules clarifying the review criteria for legal effect, validity scope and authenticity of electronic data stored on a blockchain. Finally, in May 2022, the Supreme People's Court issued opinions on strengthening the judicial application of blockchain technology indicating its widespread adoption within the national court system.

In June 2018, the Hangzhou Internet Court announced China's first blockchain judicial storage case. The court accepted evidence stored on a blockchain by the plaintiff and determined the fact of infringement accordingly. This marked the first judicial recognition of blockchain storage methods. In July 2019, China's first criminal case involving blockchain storage was adjudicated in the People's Court of Shangyu District in Shaoxing City, Zhejiang Province. This case applied blockchain storage to criminal justice in a fraud case. Blockchain storage technology has been widely adopted within China's three internet courts located in Hangzhou, Beijing and Guangzhou. These courts have each established electronic evidence platforms known as 'judicial blockchain', 'balance chain' and 'Netcom legal chain' respectively. These platforms have accumulated vast amounts of electronic evidence using blockchain technology, significantly improving case handling efficiency. In addition to internet courts, other ordinary courts are also gradually implementing blockchain storage technology.

As an emerging internet technology, blockchain holds significant legal value due to its introduction of a 'technology self-certification' mode that differs from traditional electronic data review and verification methods. In the near future, all processes involving fidelity, verification, recording and authentication - including evidence preservation, submission and verification during judicial adjudication - can be facilitated using blockchain technology. Unlike traditional evidence, electronic data stored on a blockchain does not require the formation of a complete evidence chain. Instead, it can complete the authenticity test of electronic data based on the effect of blockchain 'technology self-certification'. This 'self-certification' test exists throughout the entire cycle of electronic data from its upload to a judicial alliance chain until the conclusion of litigation activities. During this cycle, electronic data cannot be tampered with or forged.

2. Overview of Authenticity Judgment of Electronic Data Stored on a Blockchain

From a judicial practice perspective in China, the review and judgment of electronic data by courts is based on the authenticity of information within virtual space. When reviewing the three characteristics of electronic data - authenticity, relevance and legitimacy - courts primarily focus on cross-examining its authenticity. The relevance and legitimacy reviews serve mainly to ensure authenticity. Blockchain storage reduces disputes over the authenticity of electronic data during court trials and shifts the focus towards examining the relevance and legitimacy of electronic data. This can significantly improve court efficiency. In other words, the primary objective of blockchain storage is to address the authenticity of electronic data.

2.1. The Connotation of Authenticity Judgment

Authenticity review is a critical aspect of evaluating electronic data stored on a blockchain. It focuses on ensuring the integrity and identity of electronic data during litigation to prevent modification or deletion during circulation. Given the technical characteristics of blockchain technology, when examining the authenticity of blockchain evidence it is necessary to consider its potential for technical self-certification.

Technical self-certification distinguishes stored electronic data from traditional electronic data and must be considered when reviewing the authenticity of stored electronic data. Generally speaking, technical self-certification can be achieved in two environments: first, through complete synchronous storage where electronic data is fully and synchronously stored on a judicial blockchain platform from the time it is generated. The entire process of its generation, operation and completion achieves on-chain storage. In this case, the authenticity of electronic data can be effectively guaranteed allowing for technical self-certification. Second, through complete upload and storage where all electronic data associated with contracts signed under a network environment are synchronously stored on the service provider's server. If the server synchronizes or later uploads and stores complete and unedited electronic data on a blockchain storage platform then technical self-certification can also be established.

2.2. Classification of Authenticity Judgment

There are disputes within academic circles regarding the authenticity of electronic data stored on a blockchain. Some scholars argue that the authenticity of electronic evidence includes 'the authenticity of electronic data, the authenticity of electronic data content and the authenticity of electronic data carrier'. The authenticity of electronic data refers to whether it can be technically guaranteed to remain consistent with the original data. Other scholars further subdivide the authenticity of an electronic evidence carrier into the authenticity of its source and circulation.

This paper proposes that the authenticity of electronic data can be equated with formal authenticity for reforming the separation between complicated and simple civil procedures. Blockchain technology storage - a specialized method for securing electronic evidence - ensures that the data authenticity of electronic evidence is fully guaranteed by technology. The authenticity of electronic data content primarily refers to the accuracy of information contained within it and can be used interchangeably with substantive authenticity. The authenticity of an electronic data carrier mainly concerns its integrity, originality and identity as a storage medium for electronic data.

3. Challenges and Constraints in Assessing the Authenticity of Electronic Data Stored on the Blockchain

3.1. Blockchain storage does not fully ensure the substantive authenticity of electronic data.

While blockchain storage can guarantee the formal authenticity of electronic data, it cannot completely ensure its substantive authenticity. Formal authenticity provides a solid foundation for ensuring substantive authenticity; however, it is not sufficient on its own. Evidence must possess both evidentiary capacity and probative force to serve as the basis for a final decision. The authenticity of physical evidence is just one factor that affects its evidentiary capacity. This means that even if physical evidence meets authentication requirements, it may still be rejected by a judge. Authentication primarily addresses issues related to the formal authenticity of physical evidence and serves as a preliminary confirmation of its identity. It acts as an initial screening mechanism for evidence information carriers.

As a technical authentication method for electronic data, blockchain storage's primary function is to ensure that online electronic data remains unaltered and tamper-proof. It can only guarantee the formal authenticity and identity of online electronic data. For electronic data stored on the blockchain, courts must still consider other forms of evidence and apply life experience and logical rules when evaluating its authenticity.

3.2. Blockchain storage cannot ensure the authenticity of electronic data prior to its entry onto the chain

In judicial practice, there are two primary methods for entering electronic data onto a blockchain: first, electronic data can be uploaded synchronously to a blockchain storage platform via smart contract technology at the time of its generation; second, after electronic data has been generated, forensic subjects may collect it using relevant technologies and equipment as dictated by case needs before uploading it to a blockchain storage platform. Blockchain technology employs distributed ledgers, digital signatures, hash verification and smart contracts to establish a system of trust. However, while it can enhance trust through technical means, it cannot eliminate risks associated with unreliable information. Blockchain technology can only ensure that electronic data remains unaltered and undeleted after being entered onto the chain; it cannot guarantee the authenticity of electronic data prior to its entry.

4. Enhancing and Implementing Measures for Assessing the Authenticity of Electronic Data Stored on the Blockchain

4.1. Improvements and Measures at its own level

Firstly, attention should be paid to the elements and steps involved in assessing authenticity. The elements of authenticity assessment include: 1) the generation of authentic electronic data - verifying and tracing the technology and pathways used in its generation, transmission and fixation; 2) reliable electronic data storage - ensuring reliable off-chain electronic data storage systems to support on-chain storage; and 3) complete electronic data content - leveraging blockchain’s resistance to deletion and alteration to ensure data integrity. Courts should follow specific steps when assessing authenticity: 1) inputting a hash value onto a blockchain storage platform to query data storage time and block height, confirming that electronic data has been uploaded onto the blockchain; 2) preserving and authenticating generated data through CA authentication to ensure its objectivity and truthfulness; 3) comparing trusted timestamps recorded by national time service center nodes on blockchain platforms to ensure reliable electronic data storage times; and 4) verifying hash values of storage certificates submitted by parties to confirm that electronic data has not been tampered with and is relevant to the dispute at hand.

Secondly, the authenticity of electronic evidence prior to its entry onto the blockchain can be ensured through institutional development. Under a blockchain storage architecture, technical solutions alone are insufficient for addressing pre-chain authenticity. To overcome practical challenges to blockchain storage authenticity, it may be necessary to introduce supporting legal systems. Some scholars suggest that front-end control concepts could be used to facilitate automatic and synchronous storage of electronic data at the time of its generation rather than after infringement has occurred. This approach can also effectively prevent retention of multiple versions of electronic evidence and arbitrary selection of version content that benefits one party over another, thereby reducing the authenticity and probative force of electronic evidence. Additionally, some in the academic community advocate for addressing pre-upload authenticity issues through judicial presumptions. This typically involves presuming that certain evidence is true if it meets specific conditions unless effective counter-evidence is presented by another party. Theories such as adverse self-proof and reinforcement may also be employed to address the authenticity of electronic evidence stored on a blockchain.

Thirdly, the legitimacy of procedures should be reviewed. Procedural legitimacy review is a critical component of authenticity assessment and, together with technology, provides dual assurance for the authenticity of electronic data stored on a blockchain. In terms of procedural and technological dimensions, comprehensive self-inspection of network link authenticity must be conducted prior to forensic and storage activities to ensure that these processes are legitimate. This can be accomplished in three steps: 1) checking browser LAN settings and proxy status to ensure that no virtual proxy websites are present; 2) verifying complete IP, DNS and other information for all network adapters to exclude virtual websites; and 3) ensuring the authenticity of the path to a target website's web server via its domain name in order to guarantee the authenticity of links used to access it.

Fourthly, an independent storage mode should be adopted. During blockchain storage pilot programs, while theorists have yet to reach consensus on storage modes, courts have explored two different approaches: 1) a "third-party storage mode" commonly used by internet courts in which litigants cannot directly upload evidence onto a blockchain and must instead purchase services from data service providers designated by the court; and 2) an "independent storage mode" preferred by traditional courts in which litigants can directly use electronic evidence platforms for storage without relying on third-party data service providers. Of these two modes, independent storage is preferred as it reduces the number of handlers involved in evidence storage and decreases the risk of information disclosure. Third-party storage platforms are intermediaries engaged in information services and their internal staff may disclose data for personal gain or due to negligence. In contrast, independent storage allows parties to directly upload evidence onto a storage platform without involving third-party service providers. This reduces intermediate links and effectively decreases the risk of data leakage while increasing data security and authenticity.

4.2. Enhancing and Implementing Measures in Judicial Practice

Firstly, judges' subjective attitudes towards evidence assessment should be changed. The application of blockchain technology in judicial storage has enriched traditional methods for fixing and storing electronic data while simplifying rules for assessing electronic data. However, many judges remain conservative and cautious when it comes to using and authenticating blockchain evidence. Subjectively, while judges may have confidence in their professional abilities, their lack of expertise in blockchain technology may lead them to adopt a cautious approach towards blockchain storage.Objectively, there are still risks associated with blockchain storage and gaps or deficiencies exist in rulemaking. Influenced by both subjective and objective factors, judges must carefully determine the probative force of electronic data stored on a blockchain. Even with self-certification through blockchain technology, it can be difficult to quickly alleviate judges' internal concerns. As such, assessments are often conducted according to electronic data assessment rules or technical assessment steps are avoided altogether in favor of alternative evidence materials such as documentary or audio-visual materials.Judges must directly confront the challenges posed by blockchain technology as this forms the basis for assessing the authenticity of electronic evidence stored on a blockchain. As blockchain technology becomes more widely adopted, judges' cognitive states should gradually shift from stubborn caution to active engagement.

Secondly, technical investigators should be introduced. As it will likely be difficult for technical self-certification to completely supplant the independent role of national credit certification issuance in the near future, technical investigators can be introduced as trial assistants to enhance judges' confidence and credibility while strengthening the effectiveness of technical authenticity assessments.

The introduction of technical investigators is necessary for several reasons. Firstly, blockchain technology is highly specialized and requires advanced computer knowledge to accurately assess electronic data evidence. However, judges' expertise primarily lies in their understanding and application of legal theory and practice. Their knowledge structure may not necessarily include expertise related to blockchain technology which could lead to errors when deciding whether or not to use electronic data.Secondly, technical investigators are more neutral and authoritative than expert assistants. In terms of introducing technical investigators, reference can be made to systems used in intellectual property litigation or “expert witnesses” from a comparative law perspective which can produce similar effects in litigation. When introducing technical investigators, the procedures and effectiveness of their participation in litigation activities should be clearly defined.

However, it should be noted that the role of a technical investigator is primarily to reinforce evidence. If a party can demonstrate that a technical investigator’s opinion is insufficient for proving the authenticity of a record or if other evidence exists that contradicts such authenticity, then a technical investigator’s opinion cannot remedy inherent defects in the evidence itself.

Thirdly, a dual judicial trust mechanism combining “technology self-certification” and “national credit certification” should be adopted. Traditional electronic data judicial trust mechanisms are established jointly by several departments with public power attributes such as notary offices and judicial authentication agencies. These mechanisms are characterized by centralization and a focus on external certification effectiveness through national credit letters issued by notary offices and judicial authentication centers. In contrast to traditional judicial trust mechanisms, new trust mechanisms built using blockchain storage achieve decentralization. Even storage with judicial intervention can be considered “virtual centralization.”

The technical self-certification provided by blockchain electronic data storage has led to conflicts with national credit authentication. This raises the question of whether judicial authentication and notarization nodes should be retained in blockchain storage. Article 111, Paragraph 2 of the Several Provisions of the Internet Court states that courts should confirm the authenticity of stored electronic data if it can be proven. However, understanding what constitutes “being able to prove its authenticity” requires interpretation in conjunction with cross-examination by parties.

In cases where technical self-certification cannot be fully applied, judicial authentication and notarization are approved methods for authentication by courts. As such, it remains necessary to retain these two national credit nodes in blockchain storage. The new “trust+supervision” judicial trust mechanism built using blockchain storage represents an essential difference from traditional single judicial trust mechanisms for electronic data. This mechanism not only achieves openness and decentralization in storage but also verifies the relative rationality of technical self-certification to a certain extent. This provides guidance on how to use blockchain technology to build a fairer, more reliable and convenient new judicial trust mechanism that can effectively reduce court burdens and enhance judicial credibility.

5. Conclusion

The primary objective of blockchain storage is to ensure the authenticity of electronic data. This paper examines the challenges and limitations associated with verifying the authenticity of electronic data stored on a blockchain. These include the inability to fully guarantee the substantive authenticity of electronic data and to verify the authenticity of data prior to its entry onto the chain. To address these issues, this paper proposes improvements and countermeasures at both the technical and judicial levels.

The technical nature of electronic evidence stored on a blockchain presents both opportunities and challenges for the judiciary in the age of artificial intelligence. While blockchain evidence can help overcome low recognition rates for electronic evidence, it also increases pressure on judges, lawyers, and other legal practitioners to adapt to new technologies. Law is not a static set of rules but rather a living entity that must actively respond to new challenges. The application of blockchain storage represents just one aspect of these ongoing changes. In light of technological innovation, there is a need for procedural and evidentiary rules to be updated in order to effectively address these challenges in judicial practice.

References

[1] Chen Aifei. Legal regulation of electronic data blockchain certificate storage - analysis based on 66 judgments [J] Journal of Suzhou University (Philosophy and Social Sciences Edition), 2022,43 (05): 85-97.

[2] Hu Ming. Application and Regulation of Blockchain Judicial Depository [J]. Modern Law, 2022,44 (04): 158-170.

[3] Xi Zhehan. Judgment of the "three characteristics" of evidence in electronic data of blockchain evidence [J]. Social Scientist, 2022 (07): 126-132.

[4] Yiran. The status quo and rule improvement of electronic evidence authentication in blockchain storage [J]. Law Application, 2022 (02): 106-117.

[5] Sheldenko. The legal nature and application boundary of electronic data blockchain certificate storage [J]. Lanzhou Academic Journal, 2021 (12): 5-15.

[6] Han Kang. On the mode of blockchain certificate deposit - comparison between "third-party certificate deposit" and "independent certificate deposit" [J]. Academic Exploration, 2021 (10): 47-54.

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

[8] Liu Pinxin On the institutional value of blockchain certificate storage [J] Archives Communication, 2020, (01): 21-30.

[9] Li Kun. Technical advantages and review rules of blockchain evidence [J]. Journal of the People's Public Security University of China (Social Science Edition), 2022,38 (04): 87-95.

[10] Xu Zhaohui. Research on the construction and application of blockchain technology in criminal litigation supervision and prosecution [A] Shanghai Law Society Shanghai Legal Research, Volume 4, 2021, Volume 52 [C] Shanghai Law Society, 2021:195-207.

[11] Lv You. On the impact of blockchain technology on procuratorial work in the context of big data [A] Shanghai Law Society Collection of Shanghai Legal Research (Volume 20 of 2019) - Collected works of Shanghai Qingpu District Procuratorate [C] Shanghai Law Society, 2019: 111-115.

[12] Wang Yin, Liu Shaojun. Research on the construction of dualistic review model of blockchain evidence [J] Journal of Anhui University (Philosophy and Social Sciences Edition), 2022,46 (04): 109-117.

[13] Chu Fumin. Three levels of the authenticity of electronic evidence: an analysis of criminal proceedings [J] Legal Research, 2018,40 (04): 121-138.

[14] Fuyong Z, Yaduo W. On the Construction of Technology-Embedded View of Authenticity of Blockchain Evidence[J]. East Asian Law, 2022 (97): 159-184.