Technical Solutions for Ensuring the Evidentiary Validity of Trusted Electronic Records (Postprint)

Authors: Xu Xiaotong, Hou Jingrui

Date: 2023-04-01T16:02:50+00:00

Abstract

[Purpose/Significance] From an interdisciplinary perspective of electronic records management and electronic evidence application, this paper proposes technical solutions for safeguarding the evidentiary effect of trusted electronic records.

[Method/Process] We systematically analyze the principles, advantages, and outstanding issues of various judicially recognized authenticity assurance technologies, summarize and propose three categories of technical solutions for safeguarding the evidentiary effect of trusted electronic records: "electronic signature + timestamp," "blockchain-assisted authenticity verification," and "full blockchain management of electronic records and electronic evidence," analyze their applicability, and plan corresponding management processes.

[Results/Conclusion] The three categories of technical solutions can support different organizations in comprehensively deploying relevant management work according to factors such as litigation requirements, format, and classification level of electronic records, thereby significantly enhancing the effectiveness of evidentiary effect safeguarding.

Full Text

Study on Technical Schemes for Guaranteeing the Evidence Effectiveness of Trusted Electronic Records

Xu Xiaotong[1,2] **Hou Jingrui**[3]

[1] School of History and Culture, Shandong University, Jinan 250100, China
[2] Electronic Records Management Research Center, Renmin University of China, Beijing 100872, China
[3] School of Information Management, Wuhan University, Wuhan 430072, China

Abstract: [Purpose/Significance] Based on an interdisciplinary perspective of electronic records management and electronic evidence application, this paper proposes technical schemes for maintaining the evidence effectiveness of trusted electronic records. [Method/Process] This paper systematically analyzes the principles, advantages, and unresolved issues of various authenticity protection technologies recognized by the judiciary, summarizes and proposes three types of technical schemes for guaranteeing the evidence effectiveness of trusted electronic records: "Electronic Signature + Time-stamp," "Blockchain-assisted Authenticity Verification," and "Full Blockchain Management of Electronic Records-Electronic Evidence," and analyzes their applicability while planning corresponding management processes. [Result/Conclusion] The three technical schemes can support different organizations in comprehensively deploying relevant management work according to factors such as litigation requirements, formats, and confidentiality levels of electronic records, significantly improving the effectiveness of evidence effectiveness guarantee for electronic records.

Keywords: trusted electronic records; evidence effectiveness; technical schemes; electronic records management

Classification: G275
DOI: 10.13266/j.issn.0252-3116.2021.09.004

With the rapid development of new infrastructure, smart society, and Industry 4.0, technologies such as cloud computing, Internet of Things, blockchain, and artificial intelligence have rapidly penetrated various industries, and production and life have comprehensively tended toward networking, informatization, and datafication. Trusted information, records, and data, as the basic units for building digital trust mechanisms, have become critical for maintaining and promoting the development of digital social ecosystems. Theoretically, the "International Research on Permanent Authentic Records in Electronic Systems (InterPARES)" defines the criteria for determining the trustworthiness of a record as authenticity, reliability, and accuracy [1]; in practice, the trustworthiness of electronic records is reflected in whether they can serve as evidence of business activities, achieving recognition from internal institutional processes to final judicial acceptance. Electronic records management constitutes the "front-end control" link of electronic evidence, while electronic evidence represents one of the "back-end applications" of electronic records management [2]. In the management of electronic records with strong circulation and high litigation probability, selectively and systematically configuring technical solutions aligned with judicial requirements helps maintain the evidence effectiveness of electronic records, providing them with probative advantages when addressing disputes and litigation risks, and enhancing trust efficiency among institutions and at the societal level.

1. Domestic and International Research Status

Due to differences in legal systems and legislative processes, domestic and international research focuses on guaranteeing the evidence effectiveness of electronic records vary. In 1982, the Secretary General of the European Council proposed in the report "Electronic Processing of Fund Transfers" that computer records could be equivalent to written documents as evidence [3]. Common law countries successively clarified the admissibility of electronic evidence by adapting evidence rules such as the hearsay rule, best evidence rule, and authentication rule to electronic evidence. Specifically, on one hand, they focus on whether documents were "made in the usual and ordinary course of business" [4-5]; on the other hand, they emphasize the integrity of electronic records and systems, such as Canada's Uniform Electronic Evidence Act, which presumes integrity and admissibility by examining whether electronic records and their storage systems were in proper operating condition at critical moments [6].

In common law systems, concerns about the evidence effectiveness of electronic records are often considered comprehensively from the perspective of information systems, such as the U.S. national standard ANSI/AIM TR31 "Legal Acceptance of Records Produced by Information Technology Systems," which specifies basic requirements and self-assessment for records produced by information systems; the Canadian national standard CAN/CGSB-72.34 "Electronic Records as Documentary Evidence" stipulates requirements for electronic records as legal evidence and overall records management solutions, explaining the coordinated use of electronic and physical signatures [7]. Additionally, foreign scholars have applied digital forensics technology to electronic records management to assist in reliable capture and transmission of electronic records and detect forgery or unauthorized behavior [8]. For example, J.L. John positioned some technical means of digital forensics within the business processes of electronic records management [9]; the "Digital Records Forensics (DRF)" project constructed a digital forensics functional model that can interface with electronic records management [10]; C. Lee developed the digital forensics technology tool BitCurator for use in digital curation practices in libraries and archives, assisting in the formation, extraction, and presentation of digital resources that meet legal specifications [11].

China promulgated the "Electronic Signature Law" in 2004, which clarified the legal evidence effectiveness of data messages. At a time when paper records were mainstream, scholars such as Xue Sixin et al. [12] and Wang Yanming [13] actively explored application paths for electronic signature technology in electronic records management systems, viewing it as a powerful means to maintain the legal effectiveness of electronic records, and the field of records and archives management began to focus intensively on electronic signature technology. Until 2012, when electronic evidence was formally established as the eighth type of evidence in the three major procedural laws, relevant laws and regulations grew rapidly. According to the author's search and review in the Peking University Law Database and Peking University Law Intent Database, as of February

4, 2021, there were already 14 legal documents providing detailed regulations on electronic evidence collection, preservation, and review. Influenced by the overall legislative process of electronic evidence, previous research on electronic records management technology had limited integration with judicial admissibility, but scholars examined the following types of electronic records authenticity protection technologies from the perspective of records and archives management: Electronic signature technology. As mentioned above, the promulgation of the "Electronic Signature Law" sparked research enthusiasm for electronic signature technology in the records and archives management field; with the widespread application of electronic signature technology in practical work, issues regarding the archival disposition of electronic signatures have attracted attention [14-15]. Digital watermarking technology. Research has examined the types and characteristics of digital watermarking technology [16] and analyzed its protective effect on archival originality and application prospects [17].

Time-stamp technology. Discussion has focused on the application of trusted time-stamps in electronic archives transfer, backup, and long-term preservation [18], and specific schemes for electronic archives forensics and verification based on trusted time-stamps have been designed [19]. Blockchain technology. In the past three years, blockchain technology has become a hotspot, with its application prospects in document management scenarios [20-21], blockchain-based electronic records storage solutions [22], system models [23], and trusted ecosystems for document management [24] receiving attention. Additionally, Zhao Yi conducted specialized research on the tamper-proof principles of technologies such as record fixation, hash verification, digital signatures, trusted time-stamps, and blockchain, focusing on analyzing their impact and implications for records management work [25].

Summarizing the above achievements, from a research perspective, foreign research on electronic records management technology frequently interacts and integrates with judicial evidence; whereas China's relevant legal provisions have been formulated mostly in recent years, and previous research often started from the needs of the records and archives management field itself, with less integration with judicial evidence purposes. Regarding research content, current domestic research on electronic records authenticity protection technologies in China mostly focuses on explaining technical principles and analyzing application significance, or conducts research on specific management scenarios, with relatively limited comprehensive research on multiple technologies. Based on this, this paper adopts an interdisciplinary perspective of electronic records management and electronic evidence application, aims to maintain evidence effectiveness, systematically analyzes the principles and characteristics of authenticity protection technologies such as electronic signatures, electronic authentication, trusted time-stamps, hash verification, and blockchain that are recognized by the judiciary, explores technical solutions adapted to different types of institutions for guaranteeing electronic records evidence effectiveness, provides references for the trusted generation, circulation, sharing, and storage of electronic records at the institutional, inter-institutional, and societal levels,

and lays a foundation for the standardized application of industry technologies and the construction of digital trust ecosystems.

2. Judicially Recognized Authenticity Protection Technologies for Electronic Records

To more targetedly deploy technical schemes for guaranteeing the evidence effectiveness of trusted electronic records, it is necessary to clarify the principles of various judicially recognized authenticity protection technologies and explain their advantages, characteristics, and unresolved issues when applied to electronic records management.

2.1 Technical Principles of Judicially Recognized Authenticity Protection Technologies for Electronic Records

According to the provisions of various legal documents, judicially recognized authenticity protection technologies include hash verification, electronic signatures, electronic authentication, trusted time-stamps, and blockchain. Their technical principles are briefly analyzed below.

2.1.1 Hash Verification Technology Hash verification is an authenticity protection technology based on hash function operations. Its principle is to convert variable-length strings or other types of data into fixed-length digital strings through a hash function or hash table mapping [26]. When any change occurs to an electronic record, its hash value also changes, and it is impossible to reverse-engineer the changes to the electronic record from the hash value. This irreversible characteristic is the key to using hash algorithms for tamper-proofing and identity authentication. Generally, the longer the output length, the more secure the hash algorithm. Currently, commonly used hash algorithms internationally include SHA-1 (160bit), MD5 (128bit), etc. The SHA-1 variant SHA-256 can also output a 256bit hash value [27], and China's national cryptographic SM3, which is benchmarked against SHA-256, is also a mainstream algorithm with relatively high security.

2.1.2 Electronic Signature and Electronic Authentication Technology According to the definition in the "Electronic Signature Law," electronic signature refers to data in electronic form contained in or attached to a data message to identify the signer's identity and indicate the signer's approval of its content. Its most common implementation is digital signature, which uses asymmetric key encryption technology [28] and requires the application of public key algorithms and the aforementioned hash algorithm. Unless otherwise specified, electronic signatures mentioned in this paper refer to digital signatures. The sender uses their private key to sign information (usually the hash value of an electronic record), and the receiver uses the sender's public key to verify the signature, ensuring that the information comes from the sender themselves and achieving non-repudiation. Electronic authentication, in the legal sense,

refers to the legal service provided by specialized, qualified Certificate Authorities (CA) that verify the authenticity of electronic signatures and their holders' identities [29], forming third-party guarantees of the sender's identity; at the technical implementation level, it refers to encryption technology centered on electronic authentication certificates (also called digital certificates), which uses PKI (Public Key Infrastructure) to encrypt, decrypt, sign, and verify information transmitted over networks [30]. Although legal documents list electronic signatures and electronic authentication as two separate electronic evidence authenticity protection technologies, they should be complementary: electronic signatures mainly solve the problem of verifying whether information has been altered, while electronic authentication further confirms whether the communication partner is the genuine party; electronic signatures can be directly applied in closed, interactive systems, while open networks require third-party guarantees from electronic authentication; electronic signatures are technical-level protections, while electronic authentication is a complex system or process encompassing organizations, technology, and infrastructure.

2.1.3 Time-stamp Technology As mentioned above, electronic signatures can effectively solve problems of forgery, tampering, and identity impersonation of electronic records. However, in confirming creation time, time-stamp technology has greater advantages, which is significant for authenticity review of electronic evidence and the formation of evidence chains. In China, legally recognized time-stamps specifically refer to the "trusted time-stamp" service provided by the National Time Service Center of the Chinese Academy of Sciences and the United Trust Time Stamp Authority (NTSC UniTrust Time Stamp Authority, TSA). A time-stamp file includes three parts: the hash value of the electronic record, the date and time when the time-stamp service institution received the hash value, and the signature of the time-stamp service institution. Its working principle is basically consistent with electronic signatures and electronic authentication, capable of proving that an electronic record has not been tampered with from a specific time point until verification. It can be regarded as an electronic signature containing time information.

2.1.4 Blockchain Technology Blockchain is a bookkeeping technology maintained by multiple parties, applying cryptography to ensure transmission and access security, achieving consistent data storage that is difficult to tamper with and repudiate, also known as distributed ledger technology [31]. It is not a "new" technology or single technology, but rather an innovative application model in the Internet era combining distributed storage, consensus mechanisms, peer-to-peer transmission, encryption algorithms, etc. [20,32]. As the name suggests, the characteristic of "blockchain" lies in organizing and storing data blocks in a chain structure, which is the key to achieving tamper-proofing. On a blockchain, each block consists of a block header and block body. The block header contains a timestamp recording when the block was encapsulated and a Merkle root hash value, while the block body records data information such as

hash values of electronic records as needed. The Merkle root hash value is the total hash value generated by pairwise hash operations of data stored as Merkle tree leaf nodes in the block body. Any data change in the block body will cause a change in the Merkle root hash value. Blocks are connected through hash pointers and distributed in a chain structure along the timeline. Any change to data in a block will cause changes to hash values in all subsequent block headers. Once data is written, it cannot be tampered with. Blockchain technology firmly binds the content and creation time and sequence of electronic records together, maintaining the overall authenticity, integrity, and traceability of data.

2.2 Comprehensive Comparison and Analysis of Various Technologies

Through the specific analysis above, it can be seen that the working principles and functions of various authenticity protection technologies are not independent of each other but are interrelated and continuously developing. Hash verification is the core for achieving tamper-proof verification. Based on this, electronic signature and electronic authentication technology and time-stamp technology have been developed. The former can identify the validity of the digital identity of record creators on the basis of tamper-proofing, while the latter achieves confirmation of authoritative time information. Currently, many digital signature or time-stamp products have integrated the common advantages of these two technologies, achieving simultaneous confirmation of ownership and creation time. Blockchain technology can achieve trust without authoritative third parties based on the aforementioned three technologies plus smart contracts and consensus mechanisms.

When the above technologies are promoted and applied to electronic records management practice, they also have different advantages and unresolved issues:

Hash verification technology's tamper-proof mechanism makes it the foundation of a series of authenticity protection technologies, providing a simple and efficient proof method for the authenticity of electronic records. Moreover, hash function algorithms are public and transparent, and the generation and verification of hash values can be achieved at almost "zero cost" with low barriers to use. However, the effect of hash verification is relatively singular. When conducting business between departments or institutions, it is also necessary to confirm the ownership and creation time of electronic records, which requires implementation through electronic signatures and electronic authentication and time-stamp technologies.

Electronic signature and electronic authentication technology have certain advantages in guaranteeing the evidence effectiveness of electronic records: on the one hand, they facilitate tamper-proofing of content by comparing the consistency between real-time hash values and original signed hash values, helping to confirm whether electronic record content remains intact; on the other hand, they help ensure non-repudiation of actions. CA institutions endorse the unique correspondence between the public and private keys of electronic record senders.

As long as private keys have not been leaked, the signers of electronic records can be determined, eliminating the possibility of identity impersonation and assisting in the determination of the "person-event" correlation in electronic evidence identification. However, the limitations of electronic signatures and electronic authentication are also obvious: in terms of efficiency and cost, the addition of processes such as digest generation, encryption/decryption, and signature verification affects the operational efficiency of existing electronic records management processes to a certain extent, and the service costs of CA institutions also create objective obstacles. In terms of subsequent disposition, whether and how to archive electronic signatures remains undetermined. Currently, there are more than 30 CA institutions in China, and trust conflicts may arise when using services from different CA institutions [33]. Practical work also faces issues such as inability to verify due to CA institution shutdowns, departure from original hardware and software environments, algorithm failures, or digital certificate revocation, or inability to successfully migrate electronic signature information during electronic records migration [14], further affecting the stability and timeliness of electronic signatures.

Time-stamp technology's core advantage in guaranteeing the evidence effectiveness of electronic records is also based on the one-way irreversibility of hash algorithms, ensuring that electronic records have not been tampered with. Compared with general electronic signatures, trusted time-stamp technology adds authoritative, credible, and secure time information to electronic records. Moreover, currently there is only one authoritative time service institution in China, avoiding disputes and helping to determine the formation and creation time of electronic records to assist in forming credible evidence chains. Additionally, trusted time-stamps have price advantages; for example, the price for electronic data authentication is 10 yuan per record, with even more economical rates for bulk use [34]. However, in accurately identifying the identities of electronic records and signers, since general organizations rely on administrators to manually allocate time-stamp usage permissions internally after purchasing time-stamp service interfaces and administrator rights, and the specific allocation may not have a one-to-one correspondence, requiring investigation of operation traces, this reduces the efficiency of determining electronic records ownership to a certain extent.

Blockchain technology has unique advantages in guaranteeing the evidence effectiveness of electronic records: on the one hand, it implements a new trust mechanism. Its model of operation without central institutions, central systems, or third-party endorsements, relying on consensus mechanisms, makes information on the blockchain "self-verifying," achieving a transformation from trust mechanisms centered on people and authoritative institutions to trust mechanisms based on logic and code [35]; on the other hand, the mechanism of smart contracts that automatically trigger when conditions are met helps reduce uncertain factors from human intervention and maintain the integrity of evidence custody chains. Although blockchain technology has obvious advantages in tamper-proofing, as it is still an emerging technology with relatively insufficient

industry norms and standards, its application to trusted electronic records management still faces a series of issues: first, the immutability of blockchain, while giving it technical advantages in maintaining authenticity, also poses challenges to electronic records management processes, i.e., record changes must regenerate blocks and are difficult to delete; second, because blockchain systems cover functions such as fixation, long-term preservation, and authenticity protection [20], they weaken the necessity of archiving, appraisal, and other links, making it difficult to interface and adjust with electronic records management systems, potentially affecting institutional business processes; third, blockchain technology can only guarantee "on-chain authenticity." If electronic records cannot be placed on the chain at the time of creation, other means are still needed to prove their off-chain reliability; finally, to maintain data security, blockchain must perform a large number of meaningless calculations, thus facing objective difficulties in operational efficiency and cost investment. The UK's blockchain electronic records trust management project ARCHANGEL only stores hash values of electronic records and related metadata on the chain to improve efficiency [36]. However, if full automatic management based on smart contracts is to be achieved, higher requirements are placed on the infrastructure and economic investment of each blockchain node, requiring organizations themselves to have strong willingness and determination for "chain reform."

In summary, various technologies each have their advantages in terms of tamper-proof mechanisms, functions, costs, and efficiency, and also have certain problems when applied to electronic records management (see Table 1). Accordingly, starting from the requirements of electronic records management scenarios, relevant technologies can be combined to form "complementary" technical solutions to maximize their advantages and avoid potential problems and risks.

3. Design and Applicability Analysis of Technical Schemes for Guaranteeing Electronic Records Evidence Effectiveness

From the perspective of maintaining electronic records trustworthiness and guaranteeing electronic records evidence effectiveness, the technologies described above all have the ability to guarantee the authenticity of electronic records in the absence of rebuttal evidence. Therefore, organizations can select applicable technologies or technology combinations based on analysis of the characteristics of each technology, combined with their own business needs and actual conditions of records management, avoiding unnecessary cost investment and resource waste caused by excessive technology use, and preventing coordination and operational efficiency risks. The design and selection of evidence effectiveness guarantee technical schemes should fully consider front-end business development needs, i.e., pay attention to the "antecedent" [37] attributes in electronic records management, and solve trust issues among organizations or between different CA institutions. Based on the analysis of the advantages and characteristics of various judicially recognized authenticity protection technologies

above, this paper summarizes three types of technical schemes for guaranteeing electronic records evidence effectiveness: "Electronic Signature + Time-stamp," "Blockchain-assisted Authenticity Verification," and "Full Blockchain Management of Electronic Records-Electronic Evidence," which intervene in the electronic records lifecycle at different time points and in different forms, applicable to different types of electronic records management scenarios.

3.1 Scheme 1: "Electronic Signature + Time-stamp"

Generally, electronic records are created by various business systems, manually archived or automatically captured into records and archives management systems for long-term preservation, while the system automatically generates metadata describing the above management processes. On this basis, electronic signature technology and time-stamp technology cooperate to form a very stable authenticity protection technology combination capable of confirming the ownership and creation time of electronic records. This scheme has been widely applied and verified in practical work. For example, Xue Sixin's [38] concept of an "electronic records identity card" semantically calculates core metadata, electronic record entities, and electronic record hash values to fuse a unique identity identifier belonging to the electronic record, which is encapsulated together with the digital signature and time-stamp added by the electronic record generation unit. The key points of the "Electronic Signature + Time-stamp" technical scheme are: The earlier the application of electronic signature technology and time-stamp technology, the better, ideally advanced to the business processing stage to fix content and creation time; Electronic records and their metadata, electronic signatures, and time-stamps should be encapsulated together as an archival information package to serve as proof of authenticity protection technology use, ready for audit or litigation needs to form a timeline evidence chain.

This technical scheme is relatively common in application with clear cost investment and high compatibility with the processes and logic of general electronic records management work. It can be used to manage electronic records with litigation needs and risks, and can be promoted to institutions with complete electronic records management systems, standardized management processes and systems, and average management capabilities.

3.2 Scheme 2: "Blockchain-assisted Authenticity Verification"

With the widespread application of blockchain technology, some institutions such as China Petroleum & Chemical Corporation (Sinopec) and Hefei Branch of the Chinese Academy of Sciences have introduced blockchain technology into document management scenarios for the long-term trusted preservation of electronic records. "Blockchain-assisted Authenticity Verification" is an "on-chain + off-chain" technical scheme. Its formation and circulation stages are consistent with Scheme 1, but after the archival information package is formed, its hash value must be calculated immediately and stored in the blockchain system, while the archival information package composed of electronic records and other

information is still saved off-chain. When litigation occurs, the hash value of the archival information package stored in the system can be recalculated and compared with the hash value stored on the blockchain. Consistency proves that the electronic records have not been tampered with. The core of this scheme lies in using blockchain technology's tamper-proof "self-verification" method to solve trust issues among organizations or between different CA institutions. However, it should be noted that this scheme only begins to apply blockchain technology to assist hash value storage during the archiving stage, and can only prove that records have not been tampered with after being placed on the chain. In January 2021, the Supreme People's Court's newly issued "Provisions on Several Issues Concerning Online Case Handling by People's Courts (Draft for Comments)" also clearly states that if a party claims that data was not authentic when placed on the chain for storage, the party providing evidence should also provide supplementary explanations regarding the specific source of the data placed on the chain, generation mechanisms, storage processes, third-party notarization and witnessing, and corroborating data. Therefore, the prerequisite for implementing Scheme 2 lies in the compliance of management before electronic records are placed on the chain. Overall, using blockchain to assist authenticity verification is a reliable technical solution that is conducive to enhancing the probative force of electronic records.

For general organizations, Scheme 2 of "Blockchain-assisted Authenticity Verification" adds icing on the cake for evidence effectiveness guarantee based on existing electronic records management work order and is easy to promote and implement. Moreover, because blockchain has fixed requirements for on-chain formats, with fixed and limited scalability of block sizes [39], this scheme can assist in the on-chain management of hash values for unstructured or large-capacity electronic records. Additionally, only storing hash values on the chain is beneficial for maintaining the confidentiality of electronic record content information and preventing leakage risks. For electronic records with legal effect that need to perform corresponding functions during business processing, placing them on the chain only from the archiving stage still carries risks. It is recommended that organizations with distributed storage conditions or blockchain application needs use this scheme for transition and piloting, gradually exploring more comprehensive blockchain applications.

3.3 Scheme 3: Full Blockchain Management of Electronic Records-Electronic Evidence

As mentioned above, the characteristic that data cannot be tampered with once registered gives blockchain technology the function of "self-verification" of authenticity. The key to Scheme 3 is to place the entire process of electronic records formation, management, and long-term preservation on the chain and connect to judicial blockchains, using judicial organs' witness to achieve tamper-proofing and traceability throughout the entire chain of electronic records-electronic evidence. Additionally, another core function of blockchain

technology is smart contracts, and the mechanism of "automatically triggering once conditions are met" also aligns with the judgment standard in electronic evidence review and determination regarding "whether electronic evidence is automatically sent by the system." Currently, for electronic record types with high litigation rates such as emails, electronic contracts, and design documents, companies such as NetEase, Baidu, Evidence Cloud, and United Trust Time Stamp have launched electronic evidence storage service products covering various fields like "Justice Mail," "Electronic Signature," and "Micro Copyright." Some of these products directly cooperate with notarization and identification institutions, enabling "one-click certification" when litigation needs arise. These services achieve "formation equals fixation" and "formation equals on-chain" for business through the Internet, ensuring content reliability through formal authenticity and proving that electronic records have not been tampered with from formation through collection and submission to the court.

The prerequisite for full blockchain management of electronic records-electronic evidence is placing business processes on the chain. First, organizations need to select underlying blockchain technology solutions according to their own needs, build business environments and records management environments, and convert electronic records into "virtual asset" tokens (Token) that can circulate in the blockchain system during business processing, achieving electronic records management through Token management. Second, it is necessary to write electronic records management rules for archiving, appraisal, disposition, etc., into smart contracts and pre-install them in the blockchain system to achieve automated operations, such as setting time limits for executing regular off-chain storage. Additionally, to meet the high litigation needs of some electronic records, qualified institutions can apply to join alliance chains constructed by judicial organs to achieve direct verification and real-time invocation of electronic records and data in litigation, making the transformation from electronic records to electronic evidence more convenient. For example, the Beijing Internet Court has successively promulgated the "Tianping Chain Application Access Management Specifications" and "Tianping Chain Application Access Technical Specifications," providing detailed guidance for external systems to access Tianping Chain, helping to comprehensively construct a blockchain-based trusted electronic records management ecosystem.

Compared with the first two technical schemes, full blockchain management of electronic records-electronic evidence can maximize the advantages of blockchain technology, but it has greater impact on existing business order and higher upfront investment and later maintenance costs, making it difficult to promote to all types of electronic records management work in a short time. However, for fields such as finance, taxation, and intellectual property that are sensitive to electronic records authenticity protection and have high litigation needs, pilot programs can be first conducted on structured electronic record types such as electronic contracts and electronic invoices that already have certain legal effect. Once this management model is applied in various industries, the resulting production efficiency and economic benefits, as well as time and cost savings

from avoiding unnecessary litigation and disputes, will be considerable.

3.4 Comprehensive Comparison and Analysis of Technical Schemes

In judicial evidence determination, reviewing the integrity of the chain of custody is a necessary component. It requires complete records of evidence circulation and placement processes and the evolution of relevant custodians, with corresponding responsibilities [40], which is similar to the full lifecycle management emphasized in electronic records management. From this perspective, the electronic signatures and time-stamps used in Scheme 1 confirm the ownership and time of electronic records at the time of formation. Combined with reference to Article 94 of the 2019 "Provisions of the Supreme People's Court on Several Issues Concerning Evidence in Civil Litigation," which states that "electronic data kept in the manner of records management can be deemed authentic in the absence of rebuttal evidence," archived electronic records have probative advantages. Therefore, Scheme 1 can achieve authenticity certification throughout the entire lifecycle of electronic records, but the prerequisite is using management systems developed by qualified developers that meet national and industry standards to ensure the cleanliness of electronic records management and storage environments, facilitating confirmation that electronic records and metadata meet records management requirements. The timing of blockchain technology use in Scheme 2 is at the time of archiving, so it can generally be combined with Scheme 1 to supplement authenticity proof during the electronic records formation stage. Scheme 3 achieves full lifecycle on-chain management of electronic records and connects with judicial blockchains, enabling full-process authenticity witnessing of electronic records-electronic evidence. The three schemes each have their advantages and characteristics and can be applied to different types of electronic records and different types of organizations, as specifically shown in Table 2 .

4. Implementation Process for Guaranteeing Trusted Electronic Records Evidence Effectiveness Based on Multiple Technical Schemes

The three evidence effectiveness guarantee technical schemes discussed above intervene in the electronic records lifecycle at different times and in different forms, but their authenticity guarantee mechanisms also have similarities; their management processes have both differences and intersections. In practice, electronic records management work may interface with multiple businesses and face diverse evidence effectiveness guarantee needs, requiring simultaneous adoption of multiple technical schemes or step-by-step, batch implementation of different schemes. To more intuitively demonstrate the differences and connections between the management processes corresponding to multiple technical schemes, this paper provides a comprehensive explanation, as detailed in Figure 1 [Figure 1: see original paper].

As shown in Figure 1, assume an organization is equipped with various business systems such as office automation systems, core business systems, and financial systems (Business System, hereinafter referred to as BS). Three types of business systems, BS-1, BS-2, and BS-3, respectively generate electronic record types applicable to Schemes 1, 2, and 3 mentioned above. The blockchain system deployed in this example scheme is an alliance chain.

Electronic records generated by BS-1 are captured by the Electronic Records Management System (ERMS) after adding electronic signature and time-stamp information, and together with relevant metadata, are encapsulated to form Archival Information Package 1. Four-character testing is performed on it and it is preserved long-term in Trusted Digital Repositories (TDR). When electronic records face certification needs, the effectiveness of their electronic signatures and time-stamps and the reliability of system qualifications can be verified. Electronic records that pass verification can then be used for certification. The above management process is entirely implemented in local systems. In practice, the core idea of the archival data preservation by the Suda Suhang Data Preservation Center is similar to this scheme: after receiving archival data packages, the preservation center performs four-character testing, calculates their hash values, and adds trusted time-stamps; simultaneously, three backup copies of the data package are made and stored on different servers for long-term preservation. When users need to access data, the hash value of the archived data package is recalculated and compared with the hash value at the time of receipt. Consistency proves that the preservation process has not been tampered with. Since the business scope of the data preservation center does not involve record formation and circulation, there is no need to add electronic signatures to confirm data ownership. Using only trusted time-stamps as proof that electronic records have not been tampered with since receipt is sufficient.

The management process of electronic records generated by BS-2 before archiving is consistent with BS-1, but before archiving, the archival information package must also be hashed, and the hash value stored in the hash value database on the blockchain, while the archival information package composed of electronic records and other information is still saved off-chain in TDR-1. When electronic records face certification needs, the archival information package stored in TDR-1 can be hashed and compared with the hash value stored on the blockchain. Consistency allows the records to be used for certification. The formation and storage stages of the above management process rely on local systems, while the archival preservation of hash values is implemented in the blockchain system. This scheme is one of the most commonly adopted schemes for applying blockchain technology in the electronic records management field. For example, to solve inter-institutional trust issues, Sinopec Archives Blockchain stores hash values of characteristic information and metadata of electronic records formed or accessed across institutions on the blockchain platform, while original electronic records are preserved according to original requirements [41]; an institution in Dazhu County, Sichuan Province, simultaneously stores electronic record hash values in the local comprehensive archives' blockchain system when archiving

from the office automation platform, achieving full lifecycle tracking. Both institutions have stated that they plan to achieve full lifecycle on-chain management of electronic records in the future and explore strategies for managing files on other business blockchains, which is also consistent with the core idea of Scheme 3 in this paper.

Electronic records in BS-3 circulate in the form of Tokens, such as an electronic contract or an electronic insurance policy. Users can add attributes to Tokens and decide whether to use electronic signatures to endorse data ownership based on circumstances. General business information that can be shared among alliance chain node institutions can be added in plaintext, while sensitive and confidential information such as ID numbers and phone numbers can be desensitized and encrypted. Electronic record registration numbers can also be added. Meanwhile, smart contracts are pre-installed in the blockchain system to achieve automated management of Tokens, enabling them to automatically execute activities such as registration, archiving, and destruction, and store newly formed blocks in the alliance chain distributed ledger database. Additionally, to address data redundancy caused by directly storing Token attribute information, periodic off-chain storage of on-chain electronic records can be implemented. Specifically, off-chain storage cycles can be set in smart contracts according to relevant regulations. When electronic records go off-chain into local storage, hash values are simultaneously generated and stored long-term in corresponding databases. For example, according to the "Vaccine Administration Law of the People's Republic of China," records related to vaccine receipt, purchase, storage, distribution, and supply must be preserved for no less than five years beyond the vaccine's expiration date for future reference [42]. Therefore, the off-chain storage cycle can be set at five years or more. When facing certification and utilization needs, the process for BS-3 is consistent with BS-2. Currently, Scheme 3 remains a theoretical concept, but with the in-depth development of blockchain technology, business platforms based on blockchain such as Bank of Communications' "Chain Finance" securities system and Alibaba Health Blockchain will gradually increase. It is foreseeable that the full blockchain management model of electronic records-electronic evidence will be more widely applied in the future.

In summary, organizations can comprehensively sort out the nature, structural types, litigation needs, and confidentiality requirements of electronic records generated by various business systems, fully evaluate their electronic records management capabilities, infrastructure conditions, and funding investment levels, and select one or more applicable technical schemes under the guidance of their electronic records management work plans, integrating their implementation processes into existing business processes and management order to achieve optimal effectiveness in guaranteeing trusted electronic records evidence effectiveness.

5. Conclusion and Outlook

Through the research on the mechanisms of judicially recognized electronic records authenticity protection technologies and the discussion of technical schemes in the preceding sections, it can be seen that the three technical schemes each have their own characteristics in guaranteeing the evidence effectiveness of electronic records and assisting in judicial evidence determination. Although blockchain technology's characteristic of "self-verification" of authenticity has inherent advantages, enabling "self-endorsement" without relying on other authoritative institutions and avoiding third-party risks, using qualified electronic records management systems and legal electronic authentication and time-stamp services can also complete authenticity certification. From this perspective, institutional electronic records management work does not need to excessively or repeatedly adopt relevant authenticity protection technologies or blindly pursue emerging technologies. Whether adding electronic signatures and time-stamps on the basis of existing management order or deploying blockchain systems covering business ends, all can be reasonably self-consistent within their respective probative value certification systems. Moreover, technical schemes only serve as protective means to maintain the trustworthiness of electronic records content and management traces. Which records to manage, when to manage them, and how to manage them are the keys to guaranteeing electronic records evidence effectiveness. Therefore, when selecting technical schemes, organizations should aim for optimal effectiveness in guaranteeing electronic records evidence effectiveness, fully consider multiple factors such as their records management foundation, business work needs, staffing, and funding allocation, and focus on key issues such as whether records themselves have legal attributes, the magnitude of litigation needs, confidentiality requirements, and whether they are urgently needed in digital transformation, making comprehensive decisions based on these considerations. With technological development and changes in business environments, the integration of electronic records management with emerging technologies such as blockchain will be an irreversible trend. Subsequent research on practical issues such as coordination and integration among business systems, electronic records management systems, and blockchain systems, and strategies for electronic records "on-chain" and "off-chain" management will require in-depth research and joint exploration from academia and industry.

References

[1] DURANTI L, PRESTON R. International research on permanent authentic records in electronic systems 2: experiential, interactive and dynamic records[M/OL]. [2020-10-23]. http://www.interpares.org/ip2/display_{file}.cfm?doc=ip2_{{{book}}}_{{comp

[2] Xu Xiaotong, Xiao Qiuhui. Comparison and evolutionary analysis of related concepts in electronic records and evidence law[J]. Archives Science Bulletin, 2019(2): 23-28.

[3] Liu Pinxin. On the positioning of electronic evidence—speculation based on China's current evidence law[J]. Studies in Law and Business, 2002(4): 37-44.

[4] Shen Daming. Anglo-American evidence law[M]. Beijing: University of International Business and Economics Press, 2015.

[5] Canada evidence act[EB/OL]. [2021-02-01]. https://laws-lois.justice.gc.ca/PDF/C-5.pdf.

[6] He Jiahong, Liu Pinxin. Research on electronic evidence law[M]. Beijing: Law Press, 2002.

[7] Electronic records as documentary evidence[EB/OL]. [2021-02-01]. https://www.scc.ca/en/standardsdb/standards/28933.

[8] Digital Preservation Coalition. Digital preservation handbook[EB/OL]. [2021-02-01]. https://www.dpconline.org/handbook/technical-solutions-and-tools/digital-forensics.

[9] JOHN J L. Digital forensics and preservation[M]. Salisbury: Charles Beagrie Ltd., 2012.

[10] Digital records forensics project. Digital forensics function model[R/OL]. [2021-02-01]. http://www.digitalrecordsforensics.org/display_{file}.cfm?doc=drf_{{{conduct}}}*{{digital}}*{{

[11] LEE C. Archival application of digital forensics methods for authenticity, description and access provision[J]. Comma, 2012(2): 133-140.

[12] Xue Sixin, Wang Jianming, Wang Yu. Interpreting the "Electronic Signature Law" and contemplating electronic records archiving[J]. Archives Science Study, 2005(3): 54-57.

[13] Wang Yanming. Several impacts of the "Electronic Signature Law" on electronic records management[J]. Archives Science Study, 2006(1): 43-46.

[14] Cai Yingfang. Research on processing of electronic signatures in electronic records archiving[J]. Archives Science Study, 2019(4): 103-108.

[15] Liu Yuenan, Yang Jianliang, Zhang Yangyang. Research on archival preservation schemes for electronic signatures under the single-track system[J]. Archives Science Bulletin, 2019(3): 26-35.

[16] Xi Yalan. Digital watermarking technology for digital archives security maintenance[J]. Archives, 2006(5): 44-45.

[17] Zhang Jianming. Application prospects of digital watermarking in digital archives[J]. Zhejiang Archives, 2005(1): 19-20.

[18] Yang Xiya, Zhao Yonggang. Trusted time-stamp builds a security fortress for electronic archives[J]. Archives and Construction, 2013(7): 19-22.

[19] Yu Yarong, Zhang Zhaoyu. Design of electronic archives evidence collection and verification scheme based on trusted time-stamp services[J]. Archives Management, 2020(1): 66-68.

[20] Liu Yuenan. Preliminary exploration of blockchain technology application in records and archives management[J]. Zhejiang Archives, 2018(5): 7-11.

[21] Zhang Shan. Applicability and application prospects of blockchain technology in electronic archives management[J]. Archives Management, 2017(3): 18-19.

[22] Shi Jin, Xue Sixin, Zhao Xiaoke. Research on electronic records authenticity guarantee system model based on blockchain technology[J]. Library and Information Knowledge, 2019(6): 111-119.

[23] Cai Yingfang. Analysis of blockchain storage methods applied to electronic archives management[J]. Archives Science Study, 2020(4): 104-109.

[24] Wang Ping, Li Muyan, Liu Xiaochun. Construction of a trusted ecosystem for records and archives management from a blockchain perspective[J]. Archives Science Study, 2020(4): 115-121.

[25] Zhao Yi. Impact and implications of electronic records authenticity protection technology development on archives management[J]. Archives Science Study, 2019(6): 77-85.

[26] Han Hongqi. Semantic fingerprint author name disambiguation theory and application[M]. Beijing: Science and Technology Literature Press, 2018.

[27] Liang Xingqi. E-commerce security technology and applications[M]. Hefei: Hefei University of Technology Press, 2006.

[28] Zhao Zhenzhou. Information security management and application[M]. Beijing: China Fortune Press, 2015.

[29] Li Shouliang. Introduction to e-commerce[M]. Zhengzhou: Henan Science and Technology Press, 2016.

[30] Han Yingmei, Wang Shuang. E-commerce regulations[M]. Beijing: China Railway Publishing House, 2008.

[31] China Academy of Information and Communications Technology. Blockchain white paper (2019)[EB/OL]. [2020-11-18]. http://www.caict.ac.cn/kxyj/qwfb/bps/202001/P020200

[32] Ministry of Industry and Information Technology. 2016 China blockchain technology and application development white book[EB/OL]. [2020-11-18]. http://www.199it.com/archives/526865.html.

[33] The 10th "China Electronic Records Management Forum" grand opening! Opening ceremony, 10th anniversary celebration, main report! Quickly presented[EB/OL]. [2021-04-01]. https://www.sohu.com/a/360417972_{734807}.

[34] Trusted time-stamp service[EB/OL]. [2020-11-14]. http://www.tsa.cn/html/kxsjcfw/.

[35] How does blockchain solve trust mechanisms?[EB/OL]. [2020-11-18]. https://blog.csdn.net/QianZhaoVic/article/details/88771934.

[36] Yang Xixi. Analysis of electronic archives trust management model based on blockchain technology: enlightenment from the UK ARCHANGEL project[J]. Archives Science Study, 2019(3): 135-140.

[37] Feng Huiling, Liu Yuenan, Ma Linqing. Digital transformation of records management: identification of key elements and analysis of promotion strategies[J]. Archives Science Bulletin, 2017(3): 4-11.

[38] Xue Sixin. Implementation mechanism of electronic records management in cloud computing environments[M]. Shanghai: World Book Publishing Company, 2013.

[39] China Blockchain Technology and Industry Development Forum. Blockchain data format specification[EB/OL]. [2020-11-26]. https://blog.csdn.net/wxb880114/article/details/7

[40] GARNER B A. Black's law dictionary[M]. Minnesota: Thomson West, 2014.

[41] Li Chunyan, Qiao Chao. Application of blockchain technology in electronic records management of large enterprise groups: taking Sinopec as an example[J]. Archives Science Bulletin, 2020(1): 13-20.

[42] Vaccine Administration Law of the People's Republic of China[EB/OL]. [2020-12-18]. http://www.npc.gov.cn/npc/c30834/201907/11447c85e05840b9b12c62b5b645fe9d.shtml.

Author Contributions: Xu Xiaotong: Topic selection, writing, and revision; Hou Jingrui: Participated in revision.

Study on Technical Schemes for Guaranteeing the Evidence Effectiveness of Trusted Electronic Records

Xu Xiaotong[1],[2] **Hou Jingrui**[3]

[1] School of History and Culture, Shandong University, Jinan 250100, China
[2] Electronic Records Management Research Center, Renmin University of China, Beijing 100872, China
[3] School of Information Management, Wuhan University, Wuhan 430072, China

Abstract: [Purpose/Significance] Based on an interdisciplinary perspective of electronic records management and electronic evidence application, this paper proposes technical schemes which aim to maintain the evidence effectiveness of trusted electronic records. [Method/Process] This paper demonstrated the authenticity protection mechanism, advantages and unresolved problems of tamper-proof technologies recognized by the judiciary. And three technical schemes for ensuring the evidence effectiveness of trusted electronic records were proposed: "Electronic Signature and Time-stamp," "Blockchain Assisted Authenticity Verification" and "Electronic Records-Electronic Evidence Full Blockchain Management," their applicable scenarios and management processes were discussed respectively. [Result/Conclusion] The technical schemes support various organizations to deploy the work of electronic records management

according to the legal requirements, formats, and confidentiality level, which improve the efficiency of evidence effectiveness guaranteeing of the electronic records.

Keywords: trusted electronic records; evidence effectiveness; technical schemes; electronic records management

Note: Figure translations are in progress. See original paper for figures.