Siqi, Chen, Ramalinggam Rajamanickam, Nazura Abdul Manap. "Legal Framework for Authenticity of Blockchain Electronic Evidence in China: Under a Comparative Law Perspective" *Hasanuddin Law Review* 10 no. 3 (2024): 272-291. DOI: 10.20956/halrev.v10i3.5638

HasanuddinLawReview

Volume 10 Issue 3, December 2024
P-ISSN: 2442-9880, E-ISSN: 2442-9899

Legal Framework for Authenticity of Blockchain Electronic Evidence in China: Under a Comparative Law Perspective

Chen Siqi[1], Ramalinggam Rajamanickam[2], Nazura Abdul Manap[3]

[1] *Faculty of Law, National University of Malaysia, Malaysia. E-mail: adam47chen@gmail.com*
[2] *Faculty of Law, National University of Malaysia, Malaysia. E-mail: rama@ukm.edu.my*
[3] *Faculty of Law, National University of Malaysia, Malaysia. E-mail: nazura@ukm.edu.my*

Abstract: This article analyses the attitudes of various courts towards blockchain electronic evidence and the inconsistent conclusions on its authenticity in China's judicial practice. The purpose of this article is to explore the rules for determining the authenticity of blockchain electronic evidence that are suitable for China's reality. This article adopts a qualitative approach to analyse the rules for determining the authenticity of blockchain electronic evidence in China, and identifies the problems faced when reviewing the authenticity of blockchain electronic evidence in Chinese judicial practice. Finally, by comparing and learning from the U.S. rules for determining the authenticity of blockchain electronic evidence, this article puts forward proposals for establishing the best evidence rule and the hearsay rule for blockchain electronic evidence, refining the rules for judicial presumptions as well as explicitly reviewing the authenticity of the electronic evidence prior to uploading it to the blockchain.

Keywords: Authenticity; Blockchain; Electronic Data; Blockchain Evidence; Hash Value Test

1. Introduction

The meaning of blockchain electronic evidence referred to in this article can be defined from the following two levels.[1] At the technical aspect, blockchain electronic evidence is the use of blockchain technology to transform the original electronic data information into hash values, synchronized with each node to achieve the deposit. The use of signature verification, data plus decoding and other technologies, combined with the decentralized characteristics of blockchain technology, to achieve subsequent security, data tampering and audit traces.[2]

At the legislative aspect, blockchain deposit is an evidence preservation method that uses its technological advantages to complete the online verification of the authenticity of evidence and the traceability query of evidence relevance. On the one hand, the underlying technology on which blockchain electronic evidence relies essentially belongs to computer technology. On the other hand, the output of the evidence is in the form of

[1] Hong Wu and Guan Zheng, "Electronic Evidence in the Blockchain Era: New Rules on Authenticity and Integrity," *Computer Law & Security Review* 36 (April 2020): 105401, https://doi.org/10.1016/j.clsr.2020.105401.

[2] Roman Beck et al., "Blockchain Technology in Business and Information Systems Research," *Business & Information Systems Engineering* 59, no. 6 (December 15, 2017): 381–84, https://doi.org/10.1007/s12599-017-0505-1.

a hash value, which is a fixed value calculated using the hash function algorithm, and is actually electronic data.[3]

Blockchain electronic evidence is not a new type of evidence.[4] Blockchain electronic evidence can be divided into two categories based on whether it is automatically generated by a computer system. One category is direct forensic evidence, which is generated synchronously by the system when the event occurs, and the process of generating and preserving the evidence is completed automatically by the system. The second category is the converted depository evidence, which means that after the evidence is generated, the relevant data is transformed into hash values and uploaded to the blockchain for preservation.[5]

At present, China's practical and theoretical circles characterize data stored through blockchain technology as electronic data. Although different countries may differ in the division of the types of evidence, the characterization of blockchain electronic evidence is currently accepted by most countries.[6] Specifically, blockchain electronic evidence is electronic data generated or stored on the blockchain, and after the electronic data is uploaded to the blockchain, it is packaged into a 'block' marked with a hash value. The hash value is its unique ID, and the authenticity of the evidence can be tested by comparing the hash value of the blockchain electronic evidence in the court.

In recent years, the increase in the number of Internet users has significantly increased the chances of electronic data being used as key evidence in cases. With the rise of blockchain depository technology, electronic data generated or stored by it is even more frequent in the judicial field. Since 2018, China's three major Internet courts have developed review rules that distinguish them from traditional electronic data in the process of exploring the technology from scratch.[7]

Since blockchain electronic evidence has entered the judicial field, relevant legislation has been introduced to clarify its legal status. Such as Provisions of the Supreme People's Court on Several Issues Concerning the Trial of Cases by Internet Courts (hereinafter

[3] Xavier Burri et al., "Chronological Independently Verifiable Electronic Chain of Custody Ledger Using Blockchain Technology," *Forensic Science International: Digital Investigation* 33 (June 2020): 300976, https://doi.org/10.1016/j.fsidi.2020.300976.

[4] Elijah Asante Boakye, Hongjiang Zhao, and Bright Nana Kwame Ahia, "Emerging Research on Blockchain Technology in Finance; a Conveyed Evidence of Bibliometric-Based Evaluations," *The Journal of High Technology Management Research* 33, no. 2 (November 2022): 100437, https://doi.org/10.1016/j.hitech.2022.100437.

[5] Shiqun Cui, "Research on the Authenticity Examination of Blockchain Evidence," *Business and Economic Law Review*, no. 3 (2021): 142–58.

[6] Aifei Chen, "Research on Admissibility of Blockchain Evidence: Establishing Blockchain Evidence Rules in China," *Journal of Comparative Law*, no. 2 (2022): 29–43.

[7] Meirong Guo, "Internet Court's Challenges and Future in China," *Computer Law & Security Review* 40 (2021): 105522, https://doi.org/https://doi.org/10.1016/j.clsr.2020.105522.

'SICTCIC'), article 11,[8] Rules of Online Litigation of People's Courts (hereinafter 'ROLPC'), articles 16-17, [9] The newly amended Provisions by the Supreme People's Court on Evidence in Civil Procedures (hereinafter 'ECP'), articles 93-94,[10] etc., are clarifying the legal status of blockchain electronic evidence. While clarifying the legal status of blockchain electronic evidence, they have formulated different rules of review according to its characteristics. However, in judicial practice, as the blockchain technology is not mature enough, Chinese legislation is not complete and systematic, which makes it difficult for judges to judge the evidential capacity of blockchain electronic evidence based on the existing legislation.

In addition, the current theoretical research on blockchain electronic evidence mainly focuses on evidence preservation, aiming to illustrate the advantages of blockchain technology applied in the judicial field, but there is little theoretical research on the evidential capacity of blockchain electronic evidence, especially the authenticity determination. It is worth noting that although blockchain electronic evidence can guarantee the authenticity of the evidence that has been uploaded to the blockchain, it cannot guarantee that the evidence before uploading has not been tampered with. Based on this, this article takes the rules and methods of authenticity determination of blockchain electronic evidence as an entry point to further improve the existing rules of authenticity determination of blockchain electronic evidence.

Thera are some of research on authenticity determination of blockchain electronic evidence. Yang Dong and Xu Xinyu believe that blockchain electronic evidence can naturally guarantee the authenticity of the chain electronic data involved in the case, and there is no possibility of distortion.[11] However, Li Yan believes that the authenticity of blockchain electronic evidence before and after uploading is doubtful, and there is no guarantee that the data has been tampered with before uploading to the blockchain, and there is also the possibility of tampering after uploading to the blockchain.[12] In addition, the China Blockchain Judicial Deposit Application White Paper states, 'Blockchain technology can guarantee the authenticity of the carrier of the electronic data and the

[8] Provisions of the Supreme People's Court on Several Issues Concerning the Trial of Cases by Internet Courts (promulgated by Supreme People's Court, Sep. 6, 2018, effective Sep. 7, 2018) translated in LawInfoChina (last visited May 23, 2024) (P. R. C).

[9] Rules of Online Litigation of People's Courts (promulgated by Supreme People's Court, Jun. 16, 2021, effective Aug. 1, 2021) translated in LawInfoChina (last visited May 23, 2024) (P. R. C).

[10] Provisions by the Supreme People's Court on Evidence in Civil Procedures (promulgated by Supreme People's Court, Dec. 16, 2008, effective Dec. 31, 2008) translated in LawInfoChina (last visited May 23, 2024) (P. R. C).

[11] Dong Yang and Xinyu Xu, "Block Chains and the Innovation of Courts' Work: Constructing Judicial Credit System of Data Sharing," *Journal of Law Application*, no. 1 (2020): 12–22.

[12] Yan Li and Muoying Wang, "Research on Blockchain Electronic Evidence Storage Issues," *Network Security Technology & Application*, no. 4 (2022): 25–26, https://doi.org/10.3969/j.issn.1009-6833.2022.04.018.

copy of the evidence on the carrier, but this does not determine the authenticity of the electronic data itself.'[13]

Regarding the way of determining the authenticity of blockchain electronic evidence, in China's judicial practice, it is mostly a formal review, and the content of the review of the authenticity of electronic data and the relationship between the three is not yet clear.[14] Alexia Pollacco summarized three ways to deal with blockchain electronic evidence: formulating special blockchain electronic evidence laws, amending existing laws, and making a distinction between blockchain electronic evidence and traditional evidence in the form of a declaration.[15] The United States has adapted and modified its original rules of evidence through jurisprudence and legislation, and State of Vermont has developed special rules of evidence based on the characteristics of blockchain electronic evidence. State of Arizona gave blockchain records legal status by amending UETA.[16]

The electronic IDentification, Authentication and trust Services (hereinafter 'eIDAS') of EU also clarifies the legal status of blockchain electronic evidence.[17] In terms of theory, scholars in various countries are mainly concerned about how to regulate blockchain and prevent data leakage when depositing evidence. For example, Kevin Werbach believes that the main obstacle to the application of blockchain is the regulation and the law is not accurate, the law is too harsh or lax will cause the same serious consequences, will stop the development of blockchain.[18]

In summary, for the application of blockchain technology in the judicial field, all countries are in the exploratory stage, and the rules for determining the authenticity of blockchain electronic evidence are even more limited. However, it is undeniable that all are actively trying to incorporate blockchain technology into the legal framework. From the foregoing, it can be seen that the countries and regions of the common law system, especially the United States in the field of electronic data and blockchain technology in the research started earlier and made faster progress, forming a set of more perfect and developed rules for the authenticity of electronic data. Often with the help of a series of presumption rules of system integrity and reliability to prove the existence and size of

[13] China Academy of Information and Communications Technology and Trusted Blockchain Initiatives, "Blockchain Judicial Depository Application White Paper (Version 1.0)," China Academy of Information and Communications Technology and Trusted Blockchain Initiatives, June 2019, http://www.caict.ac.cn/kxyj/qwfb/bps/201906/t20190614_201169.htm.

[14] Fumin Chu, "Three Dimensions of Authenticity of Electronic Evidence," *Chinese Journal of Law* 40, no. 4 (2018): 121–38.

[15] AT Pollacco, "The Interaction between Blockchain Evidence and Courts--A Cross-Jurisdictional Analysis," Blockchain Advisory, 2020, https://blog.bcas.io/blockchain_court_evidence.

[16] Joanna Diane Caytas, "Blockchain in the U.S. Regulatory Setting: Evidentiary Use in Vermont, Delaware, and Elsewhere," *Innovation Law & Policy EJournal*, 2017, https://api.semanticscholar.org/CorpusID:157720799.

[17] Amir Sharif et al., "The EIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes," *Applied Sciences* 12, no. 24 (December 10, 2022): 12679, https://doi.org/10.3390/app122412679.

[18] Kevin Werbach, *Trust, But Verify: Why the Blockchain Needs the Law*, ed. Shaowei Lin, Translated (Shanghai: Shanghai People's Press, 2019).

the probative power of electronic data. At present, compared with the European Union, the United States and other regions, the main problems that exist in China in the research and judicial practice of blockchain electronic evidence are: the original legal attributes of the blockchain electronic evidence have not yet formed a unanimous view of the blockchain electronic evidence, blockchain electronic evidence has not yet been the legal status of a clear distinction between the difference between it and other evidence. On the other hand, guidelines such as the rules for determining authenticity are not clear enough; instead, other rules of evidence are directly applied to the process of determining the authenticity of blockchain electronic evidence without sufficient consideration of the characteristics of blockchain electronic evidence, and the operability is not strong, leading to greater disputes in judicial practice. There are legal gaps in China's blockchain governance, the application and regulation of blockchain electronic evidence and platforms are still in the early stage, and the legislation on blockchain technology is not sufficient to solve the problems arising from blockchain electronic evidence in judicial practice. In this regard, China should fully understand the characteristics of blockchain technology, and by drawing on and learning from the relevant laws and regulations of other countries or regions, such as the United States, amend or promulgate relevant legislation applicable to China in a targeted manner, so as to incorporate appropriate rules for determining the authenticity of blockchain electronic evidence.

2. Method

This article adopts a qualitative research methodology to analyse in detail the literature related to the authenticity of blockchain electronic evidence. The qualitative research methodology aims to provide an in-depth reading of the social worlds of the research participants by understanding their social and physical environments, their experiences, perspectives and histories.[19] Qualitative research methods focus on the life experiences of individuals as they are presented in the form of thoughts, ideas, feelings, attitudes and perceptions. In addition, the research methodology emphasizes human behaviour and social interaction, and it explores the quality of phenomena rather than their quantity.[20] Data sources for the qualitative research methodology include primary and secondary sources. Primary sources include legislation and cases, and secondary sources include literature related to the field.

A qualitative approach is best suited for research on blockchain electronic evidence because it allows for a deep, contextual understanding of complex issues that cannot be fully captured through quantitative methods. This topic involves intricate relationships

[19] Jo Moriarty, Qualitative Methods Overview, 1st ed. (London: NIHR School for Social Care Research, 2011), 2.
[20] Ann Öhman, "Qualitative Methodology for Rehabilitation Research1," *Journal of Rehabilitation Medicine* 37, no. 5 (September 1, 2005): 273–80, https://doi.org/10.1080/16501970510040056.

between technology, law, and judicial practice, all of which require a nuanced examination of their principles, applications, and limitations. The study of blockchain electronic evidence involves analyzing abstract legal and technological concepts, such as authenticity, evidentiary capacity, and system integrity. A qualitative approach allows the researcher to delve into the underlying principles and interpret how these concepts interact within the legal framework. In China, the *Provisions of the Supreme People's Court on Several Issues Concerning the Trial of Cases by Internet Courts* (SICTCIC) and articles 93-94 of the *Provisions on Evidence in Civil Procedures* offer conceptual guidance on blockchain evidence but lack detailed operational rules. Analyzing these provisions qualitatively provides insight into their intent and applicability. The use of blockchain electronic evidence in courts often involves a case-by-case evaluation of its admissibility, authenticity, and relevance.

A qualitative approach enables researchers to analyze specific cases to understand how courts are interpreting and applying legal principles. Hangzhou Internet Court's landmark blockchain case (2018).[21] This case accepted blockchain-stored evidence for the first time, setting a precedent for its use in Chinese judicial practice. A qualitative analysis can uncover the court's reasoning and how it balanced blockchain's technical reliability with legal standards of evidence. This article comprehends and studies the existing literature, understands the current situation of authenticity determination of blockchain electronic evidence in China, learns the rules of authenticity determination of blockchain electronic evidence in other countries, and makes suggestions for the difficulties faced by authenticity determination of blockchain electronic evidence in China.

3. Current Rules and Problems Facing the Authenticity Determination of Blockchain Electronic Evidence in China

Evidence with authenticity is not necessarily adopted by the court, but the admissibility of blockchain electronic evidence cannot be discussed without the blockchain electronic evidence authenticity determination rules. At present, there already exists a part of Chinese legislation on the determination of authenticity of blockchain evidence, which reflects the legislative spirit of some of the evidence rules.[22] Currently, the blockchain evidence authenticity determination rules are mainly as follows:

3.1. Best Evidence Rule and its shortcomings

The meaning of the best evidence rule is that copies, duplicates of evidence can be provided only when the original of the evidence is not available or has been destroyed or

[21] China Case Translation, "Case Translation: China," *Digital Evidence and Electronic Signature Law Review* 5, no. 0 (January 23, 2014), https://doi.org/10.14296/deeslr.v5i0.1831.

[22] Wanqi Liu, Pinze Zhang, and Xiaoling Zhang, Jurisprudence of Evidence (Beijing: People's Public Security University of China Press, 2020), 220.

when the nature of the evidence makes it inconvenient to provide the original of the document. The original of an evidentiary document is said to be 'best' because it has been obtained in its original state without any transformation or environmental contamination.[23] Article 70 of the Civil Procedure Law of the People's Republic of China (hereinafter 'CPL') restricts the scope of application of this rule to documentary and material evidence,[24] Article 23 of the ECP, on the other hand, extends to electronic data and audio-visual materials.[25]

In fact, there is no obstacle to the application of the best evidence rule to documentary and physical evidence, but the code is the true original of the electronic data, and the data presented is transformed, so it is obviously a paradox to try to apply this rule to adjust electronic data. In addition, Article 12 of the Supreme People's Court (hereinafter 'SPEAL') provides that, in principle, the original carrier of the electronic data should be submitted, and that copies should be provided only in case of difficulty. The original carrier here refers to the medium and equipment for storing electronic data, while the original carrier of computer data needs to be transformed in order to present information that people can understand, and the direct submission of the original requires the separation of the computer from the storage medium.[26]

From this, we can see that in practice, the electronic data produced are often copies, so it is somewhat unreasonable to stipulate that copies can only be provided when there are genuine difficulties. It can be seen from the provisions of Articles 12-13 of the ROLPC that, in principle, electronic materials can be submitted in copies, and only under certain conditions should the original be provided. Although this provision takes into account the characteristics of electronic materials, it is at odds with the best evidence rule.

The best evidence rules emphasise any evidence of the original of the strongest effect, but ignored part of the evidence of data and carrier of the inseparability. Therefore, in judicial practice, electronic data is often submitted to the court in the form of copies, but also often due to the original cannot be checked and lost as a basis for the qualification of the case.

[23] Nasir Majeed and Amjad Hilal, "The Best Evidence Principle: Meaning, Development, Consequences And Its Application In Pakistan," Pakistan Journal of Social Research 04, no. 03 (September 30, 2022): 446–55, https://doi.org/10.52567/pjsr.v4i03.734.

[24] Civil Procedure Law of the People's Republic of China (promulgated by the Standing Comm. Nat"l People"s Cong., Sep. 1, 2023, effective Jan. 1, 2024) translated in LawInfoChina (last visited May 24, 2024) (P. R. C.).

[25] Provisions by the Supreme People's Court on Evidence in Civil Procedures (promulgated by Supreme People's Court, Dec. 16, 2008, effective Dec. 31, 2008) translated in LawInfoChina (last visited May 23, 2024) (P. R. C).

[26] Several Provisions on Evidence in Administration Litigation by the Supreme People's Court (promulgated by Supreme People's Court, Jul. 24, 2002, effective Oct. 1, 2002) translated in China Law Translate (last visited May 24, 2024) (P. R. C.).

3.2. The Hearsay Rule and its shortcomings

The hearsay rule, also known as the hearsay exclusion rule, is a general term for the exclusion rule on hearsay evidence which means the hearsay evidence is inadmissible in principle except in cases prescribed by law.[27] The formation and development of the hearsay rule has been profoundly influenced by the common law system, and this rule once occupied the core position of evidence rules in the common law system. The Chinese judge on whether the evidence is admissible, is through the evidence, cross-examination and a series of operations to make a comprehensive judgement.

Due to the complexity of the rule, coupled with the differences between the two legal systems, there are two distinct voices on the establishment of the hearsay rule in China. Currently, there are some provisions in China on the hearsay rule. Article 76 of the CPL provides for the obligation of witnesses to appear in court and also provides for exceptions which means with the permission of the court, testimony may be given by means of written testimony, audio-visual transmission technology, and audio-visual materials.[28] This provision has allowed hearsay evidence to flow into the realm of civil litigation.

In addition, although Articles 85 and 88 of the ROLPC do not specify what hearsay is, they also indicate the attitude towards hearsay evidence, which means to examine and verify the evidence in a comprehensive and objective manner, and to make independent judgements on the qualifications of the evidence and the degree of probative value.[29] Hearsay evidence usually cannot be used alone as a basis for deciding a case, and can only be admitted if it forms a complete chain of evidence. Currently, there are no detailed provisions on hearsay evidence, but only guiding interpretations in principle, so the standard for the admission of hearsay evidence is an issue that needs to be resolved urgently.

The conflict between the hearsay rule and electronic data is manifested in the fact that the hearsay rule excludes electronic data with a high application rate, which not only hinders the development of electronic data, but also tends to increase the distance between the adjudicator and the truth. On the issue of whether blockchain evidence is hearsay, it is currently more controversial, and some scholars take whether there is the involvement of human factors as a criterion for judgement, but its specific content is also

[27] H. Ho, "A Theory of Hearsay," *Oxford Journal of Legal Studies* 19, no. 3 (September 1, 1999): 403–20, https://doi.org/10.1093/ojls/19.3.403.

[28] Civil Procedure Law of the People's Republic of China (promulgated by the Standing Comm. Nat"l People"s Cong., Sep. 1, 2023, effective Jan. 1, 2024) translated in LawInfoChina (last visited May 24, 2024) (P. R. C.).

[29] Provisions by the Supreme People's Court on Evidence in Civil Procedures (promulgated by Supreme People's Court, Dec. 16, 2008, effective Dec. 31, 2008) translated in LawInfoChina (last visited May 23, 2024) (P. R. C).

difficult to be directly applied to the determination of the authenticity of blockchain evidence.[30]

The amendment of Vermont Rules of Evidence clearly stipulates that blockchain evidence is hearsay, but there are exceptions under certain conditions. Although China has part of the similar hearsay rule, but because it is not fully established, its application is not ideal, because the rule also exists exceptions, so the impact of the rule on blockchain evidence is not obvious enough.[31] The adoption of similar hearsay evidence in China's judicial practice is also relatively common, and there will be no substantive defence as to whether the evidence is hearsay or not, and the same is true for blockchain evidence, so it seems that the hearsay rule is dispensable for blockchain evidence. However, since there are different types of blockchain evidence, it is of great significance to establish such a rule, and since the hearsay rule is a reasonable kernel of the partyism model borrowed from the common law system in China, the establishment of the substantive hearsay rule in China is just around the corner.[32]

3.3. The rule of treating as original and its shortcomings

Distinguishing between original and copy of blockchain evidence has certain theoretical and practical significance for determining the authenticity of electronic data.[33] In order to deal with disputes over original copies in judicial practice, Article 5 of the Electronic Signature Law of the People's Republic of China (hereinafter 'ESL') provides that a data message that meets certain conditions shall be considered an original.[34] Article 15 of the ECP provides that the parties shall submit the original electronic data as evidence. This provision expands the scope of originals by considering copies identical to the original and other identifiable and displayable output media as originals, and establishes the rule of deeming them to be originals.[35]

With regard to the conversion of the original form, the Supreme People's Court Civil 1st Trial Division has held that an electronic copy with a reliable electronic signature or other safeguards also meets the requirements of the original form.[36] From this, it can be seen

[30] Glen Wiessenberger, "Judge Wirk Confronts Mr. Hillmon: A Narrative Having Something To Do with the Law of Evidence," *SSRN Electronic Journal*, 2001, https://doi.org/10.2139/ssrn.264316.

[31] Bo Peng, "Evolution, Progress, and Review of the United States Federal Rules of Evidence.," *Evidence Science*, no. 5 (2023): 565–82, https://doi.org/10.3969/j.issn.1674-1226.2023.05.005.

[32] Jianghua Chen and Kai Zhang, "The Localization of the Electronic Evidence and Development of the Rule of Hearsay Evidence," *Science Technology and Law*, no. 2 (2006): 81–87, https://doi.org/10.3969/j.issn.1003-9945.2006.02.015.

[33] Wenwen Zhang, "Research on Authenticity Confirmation of Electronic Evidence," *Journal of Hainan Radio & TV University* 20, no. 2 (2019): 94–99, https://doi.org/10.13803/j.cnki.issn1009-9743.2019.02.017.

[34] Electronic Signature Law of the People's Republic of China (promulgated by the Standing Comm. Nat"l People"s Cong., Aug. 28, 2004, effective Apr. 1, 2005, amended Apr, 23, 2019) (P. R. C.).

[35] Provisions by the Supreme People's Court on Evidence in Civil Procedures (promulgated by Supreme People's Court, Dec. 16, 2008, effective Dec. 31, 2008) translated in LawInfoChina (last visited May 23, 2024) (P. R. C).

[36] Supreme People's Court Civil 1st Trial Division, *Understanding and Application of the Supreme People's Court's New Civil Litigation Evidence Provisions.* (Beijing: People's court press, 2020).

that although the data attributes of converted depository evidence are copies, they can be recognised as originals in accordance with the above provisions. This understanding can help judicial officers deal with the dispute between the original and the copy of electronic data, and has high reference value. In addition, since the evidence on the blockchain is instantly synchronised when the data is uploaded to the chain, it can be deemed to be the same as the original. Due to the different ways of generating blockchain evidence, there is no way to know whether the data has been changed at the time of uploading.

According to the source of the direct forensic evidence, the data on the chain can be regarded as the original. However, as there is a time gap between generation and storage, the possibility of tampering is higher, so the same approach cannot be adopted as for direct forensic evidence, and the originals and duplicates should be handled separately. Therefore, it is meaningless to distinguish between originals and copies for evidence generated directly by the system, but it is necessary to do so for data generated by human-computer interaction.

3.3. Judicial presumption rule and its shortcomings

Blockchain evidence, depending on the stage at which it is generated, can still be tampered with and cannot be verified in court. In order to solve this problem, China's current legislation establishes a judicial presumption of the authenticity of electronic data. The so-called 'presumption' refers to the court in accordance with the provisions of the law or rules of thumb, according to the known premise facts inferring the existence of unknown results, and allows the parties to adduce evidence to overturn a rule of evidence.[37]

Article 94 of the ECP stipulates the circumstances under which the authenticity of electronic data 'shall' and 'may' be confirmed, but may be rebutted whenever there is evidence to the contrary. Among them, 'shall' be presumed to be true refers to the notarisation by a notary public, because of the guarantee of public power, making it more admissible than general evidence. The circumstances in which authenticity 'may' be confirmed apply to both the rebuttable presumption of general evidence and electronic data provided or preserved by third-party platforms, formed in the course of normal business activities, and preserved by way of archive management or agreed upon by the parties.[38] Article 16 of the ROLPC stipulates that if the blockchain evidence has been technically verified as being consistent, the people's court can find that it has authenticity, unless there is evidence to the contrary sufficient to overturn it. In this rule,

[37] Jinyou Liu, Evidence Law (New Edition) (Beijing: China University of Political Science and Law Press, 2003), 263.
[38] Provisions by the Supreme People's Court on Evidence in Civil Procedures (promulgated by Supreme People's Court, Dec. 16, 2008, effective Dec. 31, 2008) translated in LawInfoChina (last visited May 23, 2024) (P. R. C).

premises and facts are linked by the ability of blockchain evidence to achieve 'technical self-evidence'.[39] Specifically, being technically tested, notarised, stored by agreement of the parties or in a fixed manner is the prerequisite, and not being tampered with and not being contradicted by evidence to the contrary is the result.

The ECP provides for circumstances in which truth can and should be presumed, but there are exceptions and evidence to the contrary. In judicial practice, the defendant is absent or present but does not defend the case is very common, for this case directly presumed to be true will be too far-fetched, in addition, for can be presumed to be true situation does not take into account the situation of the electronic data before uploading is obviously the loophole of the rules. In addition, the above judicial interpretations are of a lower legal status, the provisions are vague and have not yet formed a complete system, the relationship between the rules is not clear, the conclusions reached on the basis of different judicial interpretations are different, and there is a lack of uniformly applicable rules in the judicial field.

4. The Rules of Authenticity Determination of Blockchain Electronic Evidence in the United States

4.1. Rule of expanded scope of the original

When reviewing blockchain electronic evidence, the United States takes the rules of evidence regarding electronic data as the basis for determination. The best evidence rules of the United States stipulate that when documents other than the electronic data itself, such as copies, duplicates, etc., can have the same legal effect as signatures, they can be regarded as the original electronic data.[40]

The Federal Rules of Evidence (hereinafter 'FRE') deal with the distinction between an original and a copy of electronic data and the circumstances under which a copy can be regarded as an original. This rule solves the difficulty of identifying originals due to copying by expanding the interpretation of 'instrument' to include writings, videos, and images, and by expanding the scope of originals to include data that accurately reflects the content of the data and is legible. This provision treats the 'printout' and 'electronic copy' of an electronic document that 'accurately reflects the information in the original' as the original.[41] When examining the original electronic data, the United States focuses on whether it is complete and reliable in the entire process from generation to access, and no longer makes a simple distinction between the original and the copy, and grants blockchain evidence with completeness and reliability the legal effect of the original, and

[39] Rules of Online Litigation of People's Courts (promulgated by Supreme People's Court, Jun. 16, 2021, effective Aug. 1, 2021) translated in LawInfoChina (last visited May 23, 2024) (P. R. C).

[40] Yuqian Bi, Rules of Evidence for Electronic Data in Civil Litigation (Beijing: China University of Political Science and Law Press, 2016), 87.

[41] Jinxi Wang, The Federal Rules of Evidence (Beijing: China Legal Publishing House, 2012), 332.

takes these two characteristics as the standard for determining the authenticity of the original of the blockchain evidence.

4.2. Exceptions to the hearsay rule

Evidence introduced in a civil trial in federal court is subject to the FRE, which requires that, to be admissible, the evidence should be relevant, reliable, and correct. The most notable issue surrounding the admissibility of blockchain evidence is if the record constitutes 'admissible hearsay'. Is blockchain evidence hearsay, and if so, does it fall within the business records exception to hearsay. In the United States, the state of Vermont legally considers evidence to be hearsay, but treats it as a 'record of regularly conducted business activities', which is an exception to hearsay. The Vermont Rules of Evidence provide that unless the source of the evidentiary material or the method of collection lacks credibility, data stored using blockchain technology shall be deemed to be a 'record of regularly conducted business activities', subject to provisions for authentication.[42]

A study of the anecdotal properties of blockchain evidence will inevitably refer to United States v. Lizarraga-Tirado.[43] This case cites the 2008 decision United States v. Lamons,[44] in which the court held that inadmissible hearsay applies only to out-of-court statements made by individuals, that computer statements generally cannot be considered hearsay, and that evidence that is automatically generated without the intervention of the human element is not hearsay.[45] An analogous application of the doctrine suggests that courts may consider blockchain evidence to be entirely computer-generated rather than hearsay assertions. Although people interact with the protocol in order to make transactions, the actual record of the transaction, i.e., the information contained in the block, is computer-generated. Similar to obtaining the same data after searching for the same content on different devices, blockchain data is also replicated throughout a network of nodes that verify the correct version of the record through a consensus mechanism (as opposed to human action), which further solidifies the likelihood that a court will overturn a party's objection to blockchain evidence based on hearsay.

Records that are automatically generated by the system do not constitute hearsay, whereas for those that are stored by humans, the possibility exists that they do. Only blockchain records with a hearsay exception need to be tested under the hearsay rule, whereas direct forensic evidence does not need to be subject to the hearsay rule, and its authenticity can be determined by testing under the rule of forensics.[46] Although China

[42] Vt. R. Evid. 803 (6) Records of regularly conducted business activity.

[43] United States v. Lizarraga-Tirado, 789 F.3d 1107,1108 (9th Cir. 2015).t

[44] United States v. Lamons, 532 F.3d 1251,1263(11th Cir. 2008).

[45] Emily Knight, "Blockchain Jenga: The Challenges of Blockchain Discovery and Admissibility Under the Federal Rules," *Hofstra Law Review* 48 (May 1, 2020): 519–62.

[46] Pinxin Liu, Dianzi Zhengjufa, 1st ed. (Beijing: China Renmin University Press, 2021), 62.

does not have a specific hearsay rule, it has been applied in concrete practice. Regarding whether blockchain evidence belongs to the exception of hearsay evidence, the level of legal norms is also not clear. However, the fact that this difficulty is not encountered at present does not mean that it will not occur in the future, so it is necessary to decide whether it is necessary to clarify this rule based on a careful analysis of extraterritorial practice.

4.3. The presumption of authenticity rule

Rules 301[47] and 303[48] of the Vermont Rules of Evidence establish presumptions of authenticity, form, time, and recorder. In terms of the presumption of authenticity of blockchain evidence, it is stipulated that records and facts generated, stored and effectively verified by blockchain technology can be found to be true. In terms of the presumption of form, it is required that the use of blockchain records as evidence must be agreed upon by both parties and the method of presentation must be negotiated in order to be recognized as the form of evidence.

With respect to the presumption of time, the time when a fact or record is established through the blockchain is presumed to be the time when the electronic data is added to the chain. With respect to the presumption of recordership, the person who made the record on the chain is presumed to be the person who made the record. With respect to the presumption rule, the Vermont Rules of Evidence provide that while facts or records stored and verified using blockchain technology are presumed to be true, the presumption does not apply to the authenticity and validity of the content. Vermont has not legislatively established that blockchain evidence is tamper-evident, but only emphasizes the consistency of the data.

Vermont is much less restrictive in its legal definitions, and it does not guarantee that data stored on the blockchain is necessarily authentic, meaning that it recognizes that blockchain evidence is difficult to tamper with, but that the possibility of tampering still exists. Vermont's affirmation of blockchain evidence's ability to be self-authenticating and its presumption of authenticity greatly recognizes the value of blockchain evidence. The above rules can get rid of the reliance on notarization and solve the problem of authenticity determination of electronic evidence under certain circumstances, which provides a good reference basis for the improvement of the authenticity determination rules of blockchain evidence in China.

[47] Vt. R. Evid. 301 Presumptions in Civil Cases.
[48] Vt. R. Evid. 303 Presumptions in Criminal Cases.

5. Suggestions for improving the Rules of Authenticity Determination of Blockchain Electronic Evidence in China

5.1. Establish the best rule of evidence for blockchain electronic evidence

Blockchain evidence is quite different from traditional evidence in terms of the principle of generation and the form of dissemination. The online litigation promoted nowadays cannot be separated from various kinds of electronic data, so it has become a trend to adjust the content of the best evidence rules. According to this approach, expand the scope of the original of the best evidence rules, and even do not make a distinction between the original and the copy, as long as the blockchain evidence has the reliability and completeness, it will have the same legal effect as the original. Legal effect. The original standard, as an important element of the best evidence rules, should also be changed in line with the changes, that is, it is not necessary to strictly require the original medium when applying this rule. Of course, the above adjustment is for blockchain evidence, in principle, the original is still the main, but when the blockchain evidence as the adjustment object of the rule, it can be judged according to the original standard depending on the situation.

5.2. Establish the hearsay rule for blockchain electronic evidence

Blockchain evidence essentially belongs to electronic data, but whether blockchain evidence meets the characteristics of hearsay evidence is a different matter. For the direct forensic evidence, since it has no human factor involved, it is original evidence in itself, so it does not constitute hearsay evidence. In contrast, converted depository evidence is stored after the fact, so its authenticity and reliability are doubtful, so it can be regarded as hearsay evidence. Therefore, in the application of the hearsay rule, should be treated differently, rather than accepting or opposing all. Only blockchain evidence automatically generated by a computer system is treated as an exception to the hearsay rule and is not subject to this rule.

5.3. Improve the judicial presumption rule for blockchain electronic evidence

First, judge the electronic data according to the time interval before and after it is uploaded on the chain. For blockchain evidence, the timelier it is uploaded, the more reliable its authenticity is. Therefore, attention should be paid to its status at the time of uploading. For electronic data uploaded in a timely manner at the time of generation and controlled by the front-end before uploading, the authenticity of this part of the evidence is greater, with less possibility of being tampered with, and it can be presumed to be true in the event that the hash value is verified without error. In summary, electronic data formed after a long period of time has not yet been uploaded to the chain, this part of the evidence may have been falsified or other unreliable factors, excluded from the presumption of truth.

Secondly, whether the blockchain evidence is certified by an authoritative organisation. Blockchain depository platforms themselves cannot guarantee the authenticity of blockchain evidence, and separate appraisals or forensics are often less reliable due to the lack of public authority involved. In contrast, the authentication results of the alliance chain composed of notaries public, forensic institutions, etc., are much more reliable. In this regard, the current provisions can be continued, and blockchain evidence that has been notarised can generally be presumed to be true, unless there is other evidence that is sufficient to disprove it.

5.4. Explicitly review the authenticity of electronic evidence in the category of conversion and deposit

For blockchain evidence, although the electronic data of the transformed deposit category has not entered into the litigation procedure, its authenticity can still be determined by applying the traditional rules of authentication, i.e., examining its collection and fixation procedures to determine whether the content of the electronic data is true and complete. Transformation of the storage mode of the class of electronic data is centralised, the data generated in the terminal medium at the same time also be stored in its link to the master server. This kind of evidence needs to distinguish between originals and copies, and only the electronic data located in the master server belongs to the original, while the others are copies or backup data, so there are risks in terms of completeness and authenticity when using this kind of evidence to determine the facts of the case. Therefore, it is necessary to transform the electronic data of the class of evidence to carry out a separate authentication, in order to ensure the consistency of the content of the data.

For direct forensics class of electronic data, due to direct forensics class of electronic data is the use of decentralised distributed storage, so through the hash value checksum, trusted timestamps and other technologies to achieve self-verification. For such evidence, self-authentication is to verify whether it is consistent and complete before and after it is uploaded to the blockchain, which is actually the process of reviewing the electronic data uploaded to the blockchain, and this process can be completed through the subjective proof of the completeness of the evidence of the blockchain and the auxiliary proof of the technical reliability.

5.5. Establishing Rigorous Blockchain Rules of Evidence

While China leads the world in introducing blockchain technology into the judicial sector, the current level of application is still superficial, and rigorous blockchain evidence rules need to be established to leave room for future technological development. As the Vermont legislature, a pioneer of blockchain legislation in the United States, stated in its

report on blockchain back in 2016, recognising the legal status of blockchain technology would create a head start in attracting a convergence of economic activity around blockchain technology development. Although the legislative process for blockchain evidence rules has not yet formally begun at the U.S. federal level, judges in U.S. courts can exercise discretion in individual cases to capture the value of blockchain evidence without having to amend evidence laws at every turn.[49] In contrast, in China, as a statutory law country, the discretion of judges is strictly limited, and therefore rigorous blockchain evidence rules need to be established to deal with it.

Comparing the blockchain evidence rules of the United States and China, the United States adopts partyism, and the burden of proving whether the blockchain evidence complies with the hearsay rule or the rule of forensics is borne by the parties; while China is influenced by ex officio, especially in the application scenario of 'blockchain + notary public', the court acts as a node on the blockchain, which greatly reduces the burden of proof of the parties. The burden of proof of the parties. In the application scenario of blockchain deposit, blockchain evidence does not need to be examined for authenticity item by item like traditional electronic data, and will be analysed in detail from the aspects of generation, collection, storage and transmission of blockchain evidence:

Generation and collection of electronic data. For traditional electronic data, the generation and collection of electronic data are two distinct processes; the generation of electronic data requires that the electronic data have a unique, identified, and reliable source as well as clear, objective, and accurate content, while the collection of electronic data requires that the extraction be comprehensive, secure, and objective. Although the source of blockchain evidence may be traditional electronic data, the evidence submitted by the parties and reviewed by the court is not the original electronic data but the blockchain evidence. In this sense, blockchain technology is not only a means of evidence storage, but also time stamps electronic data and generates hash values to make it blockchain evidence that is different from traditional electronic data. As for blockchain evidence, the boundaries between electronic data generation and collection are no longer so obvious, and the generation and collection of data on the blockchain are almost synchronised.

As each blockchain evidence has a unique and verifiable hash value and timestamp, it can be judged to be unique and certain. In addition, different from traditional electronic data, blockchain evidence is uploaded to the system by the parties themselves after real-name authentication, which can avoid the influence of subjective factors of data collectors as much as possible, and the decentralised feature of blockchain can also ensure that the uploaded data is difficult to be tampered with by the persons concerned. The reliability

[49] Xukang Wang, Ying Cheng Wu, and Zhe Ma, "Blockchain in the Courtroom: Exploring Its Evidentiary Significance and Procedural Implications in U.S. Judicial Processes," *Frontiers in Blockchain* 7 (April 12, 2024), https://doi.org/10.3389/fbloc.2024.1306058.

of the original electronic data as the source of blockchain evidence is directly related to the authenticity of blockchain evidence. Vermont, on the one hand, gives blockchain records a very high degree of credibility, and on the other hand, it also makes a strict demarcation between the record and its content, i.e., the fact or record verified through the effective application of blockchain technology is true, but it cannot be presumed that the content of the fact or record is also true.

The current practice in China is to conduct a prior review of the nodes accessing the judicial blockchain. For example, the Hangzhou Internet Court Electronic Evidence Platform Regulation (Trial Implementation) proposes that the accessing party not only needs to be audited and approved by the court administrator, but must also be certified by a state-authorised third-party electronic authentication body, and the third-party data The third-party data service provider also puts forward the requirements that it should have the ability to continuously provide depository services and strict real-name authentication, and puts forward specific requirements for the system or software operating environment of all access nodes. When the data uploaded by the access nodes are examined by the Internet Court beforehand, the Court will determine that their authenticity meets the standard of high cover.[50]

Storage of electronic data. As mentioned earlier, blockchain evidence still belongs to the category of electronic data, the formation or storage of which depends on the corresponding electronic media. Traditional electronic data review focuses on the proof of the integrity of the chain of custody, requiring that the storage and custody medium of the electronic data be clear, and that the manner and means of custody be appropriate. Although the hardware and software environment of the computer system on which the blockchain evidence relies must also be safe and reliable, compared to traditional electronic data, the security of blockchain evidence storage has a higher degree of credibility. This is because the blockchain is decentralised and self-trusting, and even if there are individual nodes in the system that are damaged or missing, they will not affect the operation of the entire blockchain. Once the electronic data is uploaded to the blockchain, it will be exchanged to each node without human operation, and it can check whether there are additions, deletions, modifications, and incompleteness of the electronic data through the hash value operation.

Transmission of electronic data. For traditional electronic data, whether the hardware and software environment such as computer system and other hardware and software environment relied on for transmission is safe and reliable will directly affect the authenticity of the electronic data, therefore, the evidence sealing system is adopted in practice to reduce the instability and insecurity of the transmission process leading to the

[50] Hanying Zhu, "'Zhejiang Experience': Problems and Countermeasures in the Construction of Internet Courts," in *Proceedings of the 4th International Conference on Economy, Judicature, Administration and Humanitarian Projects (JAHP 2019)* (Paris, France: Atlantis Press, 2019), https://doi.org/10.2991/jahp-19.2019.100.

destruction, loss and tampering of the electronic data as much as possible. However, in the application scenario of blockchain deposit, such heavy work will no longer be necessary. In the judicial blockchain, courts, notaries, third-party certification bodies, appraisal agencies and relevant industry organisations are nodes on the chain, and once electronic data is uploaded to the judicial blockchain, all the above nodes can view the electronic data through public interfaces without the need for human transmission. The technical features of the blockchain, such as openness and transparency within the chain and joint maintenance by the nodes on the chain, make the electronic data free from transmission problems.

6. Conclusion

This article addresses the critical issue of authenticity determination for blockchain electronic evidence in China. By examining existing practices, legal frameworks, and international experiences, it identifies the limitations in China's judicial system, including gaps in legislation, inconsistencies in applying evidentiary rules, and insufficient adaptation of traditional standards to blockchain technology. The findings highlight the need for a robust legal framework tailored to blockchain electronic evidence, incorporating innovations such as expanded definitions of "originals," refined hearsay rules, and updated judicial presumption standards. Drawing lessons from jurisdictions like the United States, this study proposes adjustments to China's best evidence and hearsay rules, emphasizing the importance of aligning blockchain authenticity standards with the unique characteristics of this technology. Practically, these recommendations aim to ensure fair, efficient, and reliable adjudication in cases involving blockchain evidence while fostering trust and confidence in blockchain's application in the legal domain. For future legislative and judicial reforms, a key focus should be on balancing technological innovation with legal safeguards, paving the way for comprehensive and adaptive blockchain evidence rules in China.

References

Beck, Roman, Michel Avital, Matti Rossi, and Jason Bennett Thatcher. “Blockchain Technology in Business and Information Systems Research.” *Business & Information Systems Engineering* 59, no. 6 (December 15, 2017): 381–84. https://doi.org/10.1007/s12599-017-0505-1.

Bi, Yuqian. *Rules of Evidence for Electronic Data in Civil Litigation*. Beijing: China University of Political Science and Law Press, 2016.

Boakye, Elijah Asante, Hongjiang Zhao, and Bright Nana Kwame Ahia. “Emerging Research on Blockchain Technology in Finance; a Conveyed Evidence of Bibliometric-Based Evaluations.” *The Journal of High Technology Management Research* 33, no. 2 (November 2022): 100437. https://doi.org/10.1016/j.hitech.2022.100437.

Burri, Xavier, Eoghan Casey, Timothy Bollé, and David-Olivier Jaquet-Chiffelle. "Chronological Independently Verifiable Electronic Chain of Custody Ledger Using Blockchain Technology." *Forensic Science International: Digital Investigation* 33 (June 2020): 300976. https://doi.org/10.1016/j.fsidi.2020.300976.

Case Translation:, China. "Case Translation: China." *Digital Evidence and Electronic Signature Law Review* 5, no. 0 (January 23, 2014). https://doi.org/10.14296/deeslr.v5i0.1831.

Caytas, Joanna Diane. "Blockchain in the U.S. Regulatory Setting: Evidentiary Use in Vermont, Delaware, and Elsewhere." *Innovation Law & Policy EJournal*, 2017. https://api.semanticscholar.org/CorpusID:157720799.

Chen, Aifei. "Research on Admissibility of Blockchain Evidence: Establishing Blockchain Evidence Rules in China." *Journal of Comparative Law*, no. 2 (2022): 29–43.

Chen, Jianghua, and Kai Zhang. "The Localization of the Electronic Evidence and Development of the Rule of Hearsay Evidence." *Science Technology and Law*, no. 2 (2006): 81–87. https://doi.org/10.3969/j.issn.1003-9945.2006.02.015.

China Academy of Information and Communications Technology and Trusted Blockchain Initiatives. "Blockchain Judicial Depository Application White Paper (Version 1.0)." China Academy of Information and Communications Technology and Trusted Blockchain Initiatives, June 2019. http://www.caict.ac.cn/kxyj/qwfb/bps/201906/t20190614_201169.htm.

Chu, Fumin. "Three Dimensions of Authenticity of Electronic Evidence." *Chinese Journal of Law* 40, no. 4 (2018): 121–38.

Cui, Shiqun. "Research on the Authenticity Examination of Blockchain Evidence." *Business and Economic Law Review*, no. 3 (2021): 142–58.

Guo, Meirong. "Internet Court's Challenges and Future in China." *Computer Law & Security Review* 40 (2021): 105522. https://doi.org/https://doi.org/10.1016/j.clsr.2020.105522.

Ho, H. "A Theory of Hearsay." *Oxford Journal of Legal Studies* 19, no. 3 (September 1, 1999): 403–20. https://doi.org/10.1093/ojls/19.3.403.

Knight, Emily. "Blockchain Jenga: The Challenges of Blockchain Discovery and Admissibility Under the Federal Rules." *Hofstra Law Review* 48 (May 1, 2020): 519–62.

Li, Yan, and Muoying Wang. "Research on Blockchain Electronic Evidence Storage Issues." *Network Security Technology & Application*, no. 4 (2022): 25–26. https://doi.org/10.3969/j.issn.1009-6833.2022.04.018.

Liu, Jinyou. *Evidence Law (New Edition)*. Beijing: China University of Political Science and Law Press, 2003.

Liu, Pinxin. *Dianzi Zhengjufa*. 1st ed. Beijing: China Renmin University Press, 2021.

Liu, Wanqi, Pinze Zhang, and Xiaoling Zhang. *Jurisprudence of Evidence*. Beijing: People's Public Security University of China Press, 2020.

Majeed, Nasir, and Amjad Hilal. "THE BEST EVIDENCE PRINCIPLE: MEANING, DEVELOPMENT, CONSEQUENCES AND ITS APPLICATION IN PAKISTAN." *Pakistan Journal of Social Research* 04, no. 03 (September 30, 2022): 446–55. https://doi.org/10.52567/pjsr.v4i03.734.

Moriarty, Jo. *Qualitative Methods Overview*. 1st ed. London: NIHR School for Social Care Research, 2011.

Öhman, Ann. "Qualitative Methodology for Rehabilitation Research1." *Journal of Rehabilitation Medicine* 37, no. 5 (September 1, 2005): 273–80. https://doi.org/10.1080/16501970510040056.

Peng, Bo. "Evolution, Progress, and Review of the United States Federal Rules of Evidence." *Evidence Science*, no. 5 (2023): 565–82. https://doi.org/10.3969/j.issn.1674-1226.2023.05.005.

Pollacco, AT. "The Interaction between Blockchain Evidence and Courts--A Cross-Jurisdictional Analysis." Blockchain Advisory, 2020. https://blog.bcas.io/blockchain_court_evidence.

Sharif, Amir, Matteo Ranzi, Roberto Carbone, Giada Sciarretta, Francesco Antonio Marino, and Silvio Ranise. "The EIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes." *Applied Sciences* 12, no. 24 (December 10, 2022): 12679. https://doi.org/10.3390/app122412679.

Supreme People's Court Civil 1st Trial Division. *Understanding and Application of the Supreme People's Court's New Civil Litigation Evidence Provisions*. Beijing: People's court press, 2020.

Wang, Jinxi. *The Federal Rules of Evidence*. Beijing: China Legal Publishing House, 2012.

Wang, Xukang, Ying Cheng Wu, and Zhe Ma. "Blockchain in the Courtroom: Exploring Its Evidentiary Significance and Procedural Implications in U.S. Judicial Processes." *Frontiers in Blockchain* 7 (April 12, 2024). https://doi.org/10.3389/fbloc.2024.1306058.

Werbach, Kevin. *Trust, But Verify: Why the Blockchain Needs the Law*. Edited by Shaowei Lin. Translated. Shanghai: Shanghai People's Press, 2019.

Wiessenberger, Glen. "Judge Wirk Confronts Mr. Hillmon: A Narrative Having Something To Do with the Law of Evidence." *SSRN Electronic Journal*, 2001. https://doi.org/10.2139/ssrn.264316.

Wu, Hong, and Guan Zheng. "Electronic Evidence in the Blockchain Era: New Rules on Authenticity and Integrity." *Computer Law & Security Review* 36 (April 2020): 105401. https://doi.org/10.1016/j.clsr.2020.105401.

Yang, Dong, and Xinyu Xu. "Block Chains and the Innovation of Courts' Work: Constructing Judicial Credit System of Data Sharing." *Journal of Law Application*, no. 1 (2020): 12–22.

Zhang, Wenwen. "Research on Authenticity Confirmation of Electronic Evidence." *Journal of Hainan Radio & TV University* 20, no. 2 (2019): 94–99. https://doi.org/10.13803/j.cnki.issn1009-9743.2019.02.017.

Zhu, Hanying. "'Zhejiang Experience': Problems and Countermeasures in the Construction of Internet Courts." In *Proceedings of the 4th International Conference on Economy, Judicature, Administration and Humanitarian Projects (JAHP 2019)*. Paris, France: Atlantis Press, 2019. https://doi.org/10.2991/jahp-19.2019.100.

Conflict of Interest Statement: The author(s) declares that the research was conducted in the absence of any commercial or financial relationship that could be construed as a potential conflict of interest.

Hasanuddin Law Review (Hasanuddin Law Rev. – HALREV) is an open access and peer-reviewed journal published by Faculty of Law, Hasanuddin University, Indonesia.

Open Access