

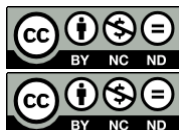


Authentication of Electronic Evidence Derived from Digital Transactions and Communications

Nguyen Thanh Minh Chanh ¹

¹ PhD in Law Candidate at Ho Chi Minh City University of Economics and Finance.
Lecturer at Industrial University of Ho Chi Minh City, Vietnam

✉ **Corresponding author:**
nguyenthanhminhchanh@iuh.edu.vn.



This work is licensed under CC BY-NC-ND 4.0.
To view a copy of this license, visit
<https://creativecommons.org/licenses/by-nc-nd/4.0>

ABSTRACT: The rapid advancement of digital technologies, artificial intelligence, and blockchain has profoundly transformed how information is generated, exchanged, and utilised in commercial transactions. This evolution raises urgent legal and technical challenges regarding the authentication of electronic evidence, which is crucial to ensuring the integrity, reliability, and probative value of digital data in judicial and arbitral proceedings. This paper examines the theoretical foundations and practical challenges of authenticating electronic evidence derived from digital transactions and communications in Vietnam. Through comparative analysis of legal frameworks in Singapore, the United States, and the European Union, the study identifies Vietnam's lack of integration between legal provisions and technical standards as the main obstacle to effective authentication. The research proposes a series of reforms, including establishing authentication mechanisms for specific digital transactions, creating a trusted third-party verification system, regulating the chain of custody, institutionalising a national digital forensic centre, and promoting capacity building through public-private partnerships. The findings highlight that improving Vietnam's legal and technical framework for the authentication of electronic evidence is essential not only for procedural fairness and legal certainty but also for fostering a transparent and trustworthy digital economy.

KEYWORDS: Electronic evidence; Authentication; Blockchain; Digital data; Vietnam.

How to cite: Minh Chanh, N. T. (2025). Authentication of Electronic Evidence Derived from Digital Transactions and Communications. *International Conference on Economic Sciences and Management in the Changing World 2025*, (pp. 302-309). Futurity Research Publishing. <https://doi.org/10.5281/zenodo.17926441>

Introduction

In the digital era, commercial, financial, and administrative activities are increasingly conducted through online platforms, resulting in the proliferation of electronic data in the form of contracts, emails, messages and social media content. These digital records have become vital sources of evidence in civil and commercial dispute resolution. However, the inherent characteristics of electronic data, such as its ease of duplication, modification, and deletion, pose significant challenges for determining authenticity, reliability, and evidentiary value in legal proceedings (Nguyen Thanh Minh Chanh, 2021; Tran, 2022). The key issue in contemporary litigation and arbitration is therefore not whether to accept electronic evidence but how to authenticate it in a manner that ensures legal validity and probative force.

The authentication of electronic evidence is a dual challenge that lies at the intersection of law and technology. It requires both legal mechanisms to establish the evidentiary status of digital data and technical tools to verify its integrity and origin. Many jurisdictions, such as Singapore, the United States and the European Union, have developed sophisticated frameworks that combine legal rules with technical standards such as digital signatures, hash functions, timestamps and blockchain to maintain a secure chain of custody (Wu & Zheng, 2020),(Al-E'mari et al., 2024), (Xiao et al., 2024). By contrast, Vietnam's legal framework remains at a foundational stage. However, the *Civil Procedure Code* 2015 and the *Law on Electronic Transactions* 2023 recognise the legal validity of data messages and electronic documents; they lack detailed guidance on technical authentication, digital forensics and procedural verification (Civil Procedure Code, 2015; Law on Electronic Transactions, 2023).

Research Aim

This study aims to examine the theoretical foundations, international practices, and practical challenges related to the authentication of electronic evidence derived from digital transactions and communications in Vietnam. By comparing Vietnam's legal framework with those of advanced jurisdictions such as Singapore, the United States, and the European Union, the research seeks to propose legal and technical reforms to ensure that electronic evidence is of consistent integrity, authenticity, and probative value, in line with international standards. The goal is to contribute to the modernisation of Vietnam's judicial system and enhance the transparency and reliability of dispute resolution in the digital era.

To achieve this objective, the study addresses the following three research questions:

1. How is the authentication of electronic evidence understood in the context of rapidly developing digital data and technology?
2. What technical and legal mechanisms are employed in advanced countries for the authentication of electronic evidence?
3. What provisions does Vietnam need to add or improve to ensure the legal value and feasibility of authenticating electronic evidence?

Results and Discussion

In the context of global digital transformation, digital transactions and information exchanges are increasingly becoming the foundational platform for business and commercial relations in Vietnam. As a result, electronic evidence formed from digital data and interactions in online environments has become central in modern dispute resolution. However, the most complex legal issue today is not whether to “accept” electronic evidence but how to “authenticate” it, verifying the integrity, origin, and authenticity of the data. This challenge is not merely technical but requires coordination between law and technology to ensure the probative value of electronic information (Nguyen Thanh Minh Chanh, 2021; Tran, 2022).

From a theoretical perspective

Electronic evidence has legal value only if it is secured through both legal and technical measures, particularly by demonstrating the integrity and origin of the data (Mason & Seng, 2017). This view is supported by Ferreira & Gromova, who emphasise that, in arbitration proceedings, authentication of electronic evidence must be supported by technologies such as encryption, digital signatures, or blockchain to protect the original data and guard against fraud (Ferreira & Gromova, 2023). From a broader perspective, blockchain, hash functions, and metadata may become core tools in maintaining a chain of custody – a factor that ensures data is not altered during collection and use (Rahul et al., 2024; Wu & Zheng, 2020). Additionally, because electronic evidence is easily copied and altered, it cannot be authenticated by the senses as traditional physical evidence can; instead, it must be verified through “digital traces” such as access logs, access-control systems, and digital forensic evidence. This view opens a new approach: authentication of electronic evidence is not simply a technological procedure but an essential component of a modern procedural mechanism, requiring that law keep pace with technical advances (Xiao et al., 2024; Al-E’mari et al., 2024).

In Vietnam, the law has so far only recognised the legal value of electronic data, without establishing technical norms for authentication. Although Article 94 of the Civil Procedure Code 2015 (Civil Procedure Code, 2015), which included electronic data as admissible evidence, also addresses data messages and electronic records, the Law on Electronic Transactions 2023 addresses them. Article 11 provides that: “*A data message shall not be denied legal effect, validity or enforceability solely because it is in electronic form. Its evidentiary value is determined based on its reliability, methods of generation, storage, transmission and the ability to maintain its integrity and identify its origin*” (Law on Electronic Transactions, 2023). The law recognises the legal value of electronic data and digital signatures; their provisions remain at a principled level, lacking specific technical guidance on authentication. However, this insufficiency leads to many difficulties when the lack of digital forensic tools forces the bench to rely on witness testimony rather than technical evidence. These instances clearly reflect that Vietnam’s judiciary still lacks a chain of custody and an independent data verification process (Nguyen Thanh Minh Chanh, 2021; Tran, 2022).

From international experience, many advanced jurisdictions have established close coordination between legal rules and technical standards to ensure the authenticity of electronic data. In the United States, courts are increasingly recognising the probative value of social media data and digital platform content, while warning of risks of manipulation or deletion. Proposals include using timestamping and blockchain to enhance the reliability of evidence (Wang et al., 2024). Similarly, in Europe, cases involving social networks show that although jurisprudence is evolving, challenges regarding the authenticity of digital data persist (Psychogiopoulou, 2021). In Asia, Singapore is seen as a leading example of combining legal regulation with technical authentication, allowing courts to verify messages, emails, or OTT data through service provider confirmation. This mechanism ensures data integrity and authenticity and significantly shortens litigation time (Seng, 2024). These instances clearly show that Vietnam can draw on such experience to improve its legal framework.

From Practical Context

In Vietnam's commercial dispute resolution practice, the authentication of electronic evidence remains a significant challenge for both courts and arbitral tribunals. Despite the Civil Procedure Code 2015 and the Law on Electronic Transactions 2023 acknowledging the legal effect of data messages, electronic signatures, and digital documents (Civil Procedure Code, 2015), (Law on Electronic Transactions, 2023), these provisions remain largely principled and lack specific procedural guidance on authentication, collection, preservation and digital forensic examination (Nguyen Thanh Minh Chanh, 2021), (Tran, 2022).

Judicial practice reveals that many cases are delayed or dismissed due to insufficient verification of the origin or integrity of digital data. In a "loan contract dispute", for example, the People's Court of Binh Xuyen District (TAND huyện Bình Xuyên, 2024). refused to admit printed Zalo messages as evidence because of the absence of digital forensic tools, compelling the court to rely on oral testimony instead of technical proof. This highlights the absence of a clearly defined chain of custody to ensure authenticity during data collection, storage, and presentation. Vietnam also lacks an independent digital forensic authority with a mandate to assist courts and arbitration tribunals in analysing, recovering, or authenticating electronic evidence (Nguyen Thanh Minh Chanh, 2021; Tran, 2022).

Compared to advanced jurisdictions, Vietnam's legal framework still lacks effective integration between legal provisions and technical standards governing the authentication of electronic evidence. In contrast, Singapore has established a detailed and coherent regime under its Evidence Act (1983) (Singapore Parliament, 1983) and Electronic Transactions Act (2010) (Singapore Parliament, 2010). *Section 9 of the Evidence Act mandates proof of "the integrity of the data storage system" as a condition for establishing authenticity.* Furthermore, Singapore's legal practice permits network service providers and digital platforms to verify essential metadata, such as the sender's identity, transmission time, and IP address, in civil and commercial disputes, ensuring the technical traceability of digital evidence (Seng, 2024).

In the United States, the Federal Rules of Evidence (Rules 901 and 902) (13), (14) explicitly address the authentication of electronic evidence (Federal Rules of Evidence, 2024). Under these provisions, electronic evidence may be deemed self-authenticating if accompanied by a valid technical certification, such as verified copies with a hash value, metadata or confirmation by a system administrator. U.S. courts also accept digital forensic reports as independent proof of authenticity and origin (Wang et al., 2024).

In the European Union (EU), the eIDAS Regulation (European Union, 2014) establishes a unified framework for electronic identification and trust services. Under this regime, digital signatures, timestamps, and electronic seals (e-seals) carry the same legal effect as handwritten signatures and are mutually recognised across all Member States, thereby ensuring both the legal validity and technical verifiability of electronic data (Psychogiopoulou, 2021; Stoykova, 2021).

In contrast, Vietnam's system remains fragmented and essentially principle-based. Unlike Singapore, the United States, and the EU—where mandatory technical standards such as hash verification, timestamping, and chain-of-custody procedures are clearly defined—Vietnam has yet to codify comparable procedures. As a result, the assessment of electronic evidence in Vietnam often depends on judicial discretion rather than objective technical criteria, which undermines consistency, predictability and transparency in adjudication (Nguyen Thanh Minh Chanh, 2021; Tran, 2022).

Recommendations for Improving the Vietnamese Law on the Authentication of Electronic Evidence Derived from Digital Transactions and Communications

In the context of a rapidly developing digital economy, online transactions and communications (such as emails, OTT applications, e-commerce platforms, electronic contracts, and blockchain-based exchanges) have increasingly become the primary sources of evidence in the resolution of commercial disputes. However, Vietnamese law currently stops at recognising the legal validity of data messages, without establishing a coherent, scientific, and internationally standardised mechanism for authenticating electronic evidence originating from digital transactions and communications. Therefore, it is necessary to improve the law in the following directions.

Establishing Authentication Mechanisms for Specific Types of Digital Transactions

Vietnam should develop specific authentication mechanisms suited to various types of digital transactions and communication platforms—such as email, OTT messaging applications (e.g., Zalo, Viber), e-commerce exchanges, and electronic contracts. These mechanisms must clearly define the source and method of data collection, identify both the sender and recipient, and record essential metadata such as IP addresses, timestamps, and hash values. Such technical specifications are crucial for ensuring data integrity, authenticity and traceability throughout the transaction process.

Vietnam may refer to the Singaporean model [Evidence Act (Cap. 97, Revised Edition)] (Singapore Parliament, 1983), which requires proof of “the integrity of the data storage system” as a condition for authenticating electronic information generated from digital transactions.

Legal Framework for Trusted Third-Party Authentication

A comprehensive legal framework should be established to enable the authentication of electronic evidence through trusted third parties. These entities may include electronic certification authorities, telecommunications service providers, or licensed online transaction platforms that are authorised to verify the identity of parties, the transmission time, and the integrity of content.

The European Union's Regulation (EU) No. 910/2014 (eIDAS) provides a valuable reference, as it ensures the cross-border legal recognition of electronic signatures, timestamps and seals, thereby reinforcing transparency and technical verifiability. This framework grants digital evidence the same legal status as traditional paper-based documents, promoting trust and legal certainty in digital environments (European Union, 2014).

Regulation of the Chain of Custody for Electronic Evidence

Vietnam should promulgate detailed regulations governing the chain of custody for electronic evidence derived from digital transactions and communications. These regulations should encompass all procedural stages from recording, storage and transfer to verification and presentation—under the supervision of judicial authorities or independent digital forensic institutions. To ensure consistency with international best practices, Vietnam should adopt ISO/IEC 27037:2012, which provides standardised guidelines for the collection, preservation, and handling of digital evidence. This approach guarantees that the integrity and reliability of data are maintained throughout the entire evidentiary process (ISO, 2012).

Establishment of a Digital Forensic Centre for Civil and Commercial Matters

Vietnam should consider creating a Digital Forensic Centre for Civil and Commercial Matters to assist courts and arbitral tribunals in authenticating electronic evidence arising from digital transactions and communications. This specialised centre should be empowered to collaborate with network service providers, e-commerce platforms, and technology enterprises to verify data origins, retrieve deleted files, and analyse metadata.

The United States model, in which digital forensic reports are treated as self-authenticating evidence under Federal Rules of Evidence 901 and 902(13), (14) (2024), demonstrates the effectiveness of institutionalising forensic expertise within the evidentiary system (Federal Rules of Evidence, 2024).

Capacity Building and Public-Private Partnerships

To ensure effective implementation, Vietnam should invest in capacity building by organising specialised training programs on the authentication of electronic evidence for judges, arbitrators, prosecutors, and legal practitioners.

Simultaneously, public-private partnerships (PPPs) should be encouraged between judicial authorities and major technology companies (e.g., Meta, Google, Zalo, Shopee, Tiki) to develop

standardised procedures for data provision, sender-recipient verification, and timestamp confirmation. These partnerships must also prioritise privacy protection and data security, ensuring that evidentiary authentication aligns with both technological realities and legal safeguards.

Conclusion

The authentication of electronic evidence derived from digital transactions and communications has become a pivotal aspect of Vietnam's legal modernisation. Despite the Civil Procedure Code (2015) and the Law on Electronic Transactions (2023) establishing foundational principles recognising the legal validity of data messages, electronic signatures, and digital documents, the absence of detailed procedural and technical standards continues to hinder their effective implementation. In contrast, jurisdictions such as Singapore, the United States, and the European Union have developed comprehensive legal-technical frameworks that integrate mechanisms such as hash verification, timestamping, and chain-of-custody procedures with legal presumptions of authenticity, thereby ensuring the reliability and admissibility of digital evidence in judicial and arbitral proceedings. Vietnam, however, remains at an early stage of this development due to the lack of an independent digital forensic authority, inconsistent judicial assessment of electronic evidence and limited cooperation between judicial institutions and digital service providers. To overcome these challenges, Vietnam should urgently standardise the authentication process in line with international best practices by adopting clear regulations on the chain of custody, incorporating ISO/IEC standards for digital evidence collection and preservation, and recognising trusted third parties as legitimate authenticators. Additionally, reestablishing a national digital forensic centre and enhancing digital literacy among judges, arbitrators, and legal practitioners are essential to ensuring objective, scientific, and globally aligned evaluations of electronic evidence. Ultimately, the authentication of electronic evidence from digital transactions and communications is not merely a technical issue but a crucial step toward establishing a transparent, reliable, and innovation-driven legal foundation for Vietnam's digital economy.

References

- Al-E'mari, S., Sanjalawe, Y., Makhadmeh, S., & Alqudah, H. (2024). Digital Forensics Meets Blockchain: Enhancing the Authenticity and Traceability of Evidence. *2024 2nd International Conference on Cyber Resilience (ICCR)*, 01-06. <https://doi.org/10.1109/ICCR61006.2024.10532961>
- Civil Procedure Code (2015).
- European Union. (2014). *REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.*
- Federal Rules of Evidence (2024).
- Ferreira, D. B., & Gromova, E. A. (2023). Electronic evidence in arbitration proceedings. *Digital Evidence and Electronic Signature Law Review*, 30-39.

- <https://doi.org/10.14296/deeslr.v20i.5608>
- ISO. (2012). *Information technology-Security techniques-Guidelines for identification, collection, acquisition, and preservation of digital evidence*.
- Law on Electronic Transactions, Pub. L. No. No. 20/2023/QH15, National Assembly (2023).
- Mason, S., & Seng, D. (2017). *Electronic Evidence*.
- Nguyen Thanh Minh Chanh. (2021). *Pháp luật về chứng cứ điện tử trong tố tụng dân sự Việt Nam*. <http://lapphap.vn>
- Psychogiopoulou, E. (2021). Judicial dialogue in social media cases in europe: Exploring the role of peers in judicial adjudication. In *German Law Journal* (Vol. 22, Issue 6, pp. 915-935). Cambridge University Press. <https://doi.org/10.1017/glj.2021.57>
- Rahul, M., Bharati, K., Khodke, P. G., Khadilkar, C. P., & Bawiskar, S. K. (2024). Forensic Bytes: Admissibility and Challenges of Digital Evidence in Legal Proceedings. *International Journal of Scientific Research in Science and Technology (Www.Ijsrst.Com)* |, 11(16), 24-35. <https://doi.org/10.32628/IJSRST>
- Seng, D. K. B. (2024). *Electronic Evidence*. <https://doi.org/10.2139/ssrn.4964150>
- Singapore Parliament. (1983). *Evidence Act 1893 and 2020 revised edition*.
- Singapore Parliament. (2010). *ELECTRONIC TRANSACTIONS ACT 2010 2020 REVISED EDITION*.
- Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review*, 42, 105575. <https://doi.org/10.1016/j.clsr.2021.105575>
- TAND huyện Bình Xuyên, tỉnh V. P. (2024). *Tranh chấp hợp đồng vay tài sản [Property loan contract dispute]*.
- Tran, Q. A. (2022). *Electronic Evidence in Civil and Commercial Dispute Resolution* (Vol. 27). Springer Nature Switzerland. <https://doi.org/10.1007/978-3-031-18572-4>
- Wang, X., Wu, Y. C., & Ma, Z. (2024). Blockchain in the courtroom: exploring its evidentiary significance and procedural implications in U.S. judicial processes. *Frontiers in Blockchain*, 7. <https://doi.org/10.3389/fbloc.2024.1306058>
- Wu, H., & Zheng, G. (2020). Electronic evidence in the blockchain era: New rules on authenticity and integrity. *Computer Law and Security Review*, 36. <https://doi.org/10.1016/j.clsr.2020.105401>
- Xiao, N., Wang, Z., Sun, X., & Miao, J. (2024). A novel blockchain-based digital forensics framework for preserving evidence and enabling investigation in industrial Internet of Things. *Alexandria Engineering Journal*, 86, 631-643. <https://doi.org/10.1016/j.aej.2023.12.021>