Economics, Law and Policy
ISSN 2576-2060 (Print) ISSN 2576-2052 (Online)
Vol. 9, No. 1, 2026
www.scholink.org/ojs/index.php/elp

Original Paper

The Application and Dilemma of Electronic Evidence in Maritime Fraud Cases

Yunting Xiao[1*] & Guang Yang[1]

[1] Dalian Ocean University, Dalian, Liaoning, China

[*] Corresponding Author

Received: March 20, 2026 Accepted: April 20, 2026 Online Published: April 22, 2026

doi:10.22158/elp.v9n1p322 URL: http://dx.doi.org/10.22158/elp.v9n1p322

Abstract

With the digital transformation of maritime trade, electronic evidence has gained increasing prominence in maritime litigation. Maritime fraud cases, characterized by cross-border, technical, and covert features, pose challenges to electronic evidence, including inconsistent authentication standards, conflicts between traditional evidence rules and new forms of evidence, and legislative lag. This study employs normative analysis, empirical research, and comparative law analysis to systematically categorize the basic types and characteristics of electronic evidence, examine the legal framework and practical difficulties of its authentication, explore technology-driven innovative approaches, and propose institutional recommendations. The findings reveal a paradigm shift in electronic evidence authentication from traditionalism to technocratism, with judicial applications of emerging technologies such as blockchain-based evidence storage offering potential pathways to overcome authentication difficulties. Future efforts should focus on establishing unified authentication rules for electronic evidence in the revision of the Special Maritime Procedure Law, advancing the development of a unified platform for maritime electronic evidence, and improving international cooperation mechanisms for cross-border electronic evidence collection.

Keywords

electronic evidence, law, Maritime fraud cases

1. Introduction

Since the 21st century, the digital transformation of maritime trade has profoundly reshaped the operation of the shipping industry. The widespread use of new commercial documents such as electronic bills of lading, electronic customs declarations, and electronic contracts has greatly enhanced trade efficiency, but has also brought new legal challenges. According to statistics, over 95% of

maritime cases involve electronic evidence, which has become a core basis for determining case facts in maritime litigation. In 2012, China's Civil Procedure Law was amended to establish "electronic data" as an independent type of evidence, providing a fundamental legal basis for the judicial application of electronic evidence. Subsequently, Article 116 of the Interpretation of the Supreme People's Court on the Application of the Civil Procedure Law of the People's Republic of China further clarified the scope of electronic data, including emails, electronic data interchange, online chat records, blogs, microblogs, SMS messages, electronic signatures, domain names, and other information formed or stored in electronic media.

Maritime fraud cases typically feature cross-border, technical, and covert characteristics. Fraud perpetrators often exploit the complexity of international trade chains, differences in legal systems across jurisdictions, and technical barriers in maritime transport to commit various forms of fraud, such as bill of lading fraud, marine insurance fraud, and freight forwarding fraud. In such cases, electronic evidence is not only a key means of proving fraudulent conduct, but its authentication has also become a difficult issue in judicial practice.

In current judicial practice, the authentication of electronic evidence faces three major challenges: first, inconsistent authentication standards, with significant differences in the acceptance of similar electronic evidence by different courts and judges; second, obvious conflicts between traditional evidence rules and new forms of evidence, as the traditional notarization-centered authentication model struggles to adapt to the technical characteristics of electronic evidence; third, legislative lag behind technological developments, as current legal norms provide insufficient regulation for new evidence-fixing technologies such as blockchain-based storage and trusted timestamps.

These challenges are particularly acute in maritime litigation. Maritime cases often involve cross-border elements, making the authentication and authenticity verification of electronic evidence generated abroad a prominent issue troubling judicial practice. Moreover, the covert nature of maritime fraud cases makes the collection and preservation of electronic evidence more difficult, highlighting the urgent need to establish specialized rules tailored to their characteristics.

Through a systematic study of electronic evidence authentication in maritime fraud cases, this paper aims to enrich the theory of electronic evidence authentication and provide practical material for the dialogue between traditionalist and technocratic perspectives on evidence. By examining the practical difficulties in the judicial application of electronic evidence and summarizing the pioneering practices of courts such as the Shanghai Maritime Court and the Xiamen Maritime Court, this paper seeks to offer actionable technical guidance and institutional recommendations for maritime judicial practice. The study employs normative analysis to systematically review the legal framework for electronic evidence authentication, empirical analysis to examine the actual situation and problems in judicial practice, and comparative analysis to draw on legislative experience and practical explorations of electronic evidence rules in other jurisdictions, thereby providing a reference for improving the relevant system in China.

2. Basic Types and Characteristics of Electronic Evidence in Maritime Fraud Cases

2.1 Definition and Classification of Electronic Evidence

Electronic data refers to information generated, sent, received, or stored by electronic, optical, magnetic, or similar means. Article 116 of the Interpretation of the Civil Procedure Law further specifies the scope of electronic data, including emails, electronic data interchange, online chat records, blogs, microblogs, SMS messages, electronic signatures, domain names, and other information formed or stored in electronic media.

From the perspective of evidence law, electronic evidence can be classified in various ways based on factors such as its method of generation, storage medium, and evidentiary content. For the purpose of this study, distinguishing between maritime-specific electronic evidence and ordinary electronic evidence helps reveal the special rules governing the application of electronic evidence in maritime fraud cases.

2.2 Types of Maritime-Specific Electronic Evidence

Maritime-specific electronic evidence refers to types of electronic evidence that are generated solely in the course of shipping trade activities and possess distinctive maritime professional characteristics. Based on a summary of existing judicial practice and academic research, maritime-specific electronic evidence mainly includes the following categories:

Table 1. Classification and Role of Maritime-Specific Electronic Evidence

Category	Specific types	Role in fraud cases
Shipping commercial electronic evidence	Electronic bill of lading, electronic customs declaration, electronic contract	Prove the authenticity of the transaction
Vessel navigation data	AIS data, VDR data, GPS track records	Prove the actual navigation status of the vessel
Maritime information system data	Ship registration information, crew certificates	Verify the identity of the relevant parties
Communication and payment records	Emails, WeChat records, bank statements	Prove communication and fund flows in the transaction

Electronic bill of lading is a typical type of shipping commercial electronic evidence. Compared with traditional paper bills of lading, electronic bills of lading offer advantages such as faster circulation, lower risk of loss, and easier verification, but they also raise new legal issues. In fraud cases, acts such as forging electronic bills of lading or tampering with bill information occur from time to time, making the authentication of the authenticity of electronic bills of lading a key issue.

Automatic Identification System (AIS) data constitutes important vessel navigation data. The AIS requires vessels to continuously transmit information such as position, course, and speed, which is received and stored by ground stations and satellites. In marine insurance fraud cases, AIS data can reveal the actual navigation track of a vessel and be compared with the statements of the policyholder to detect clues of fraud. Similarly, Voyage Data Recorder (VDR) data, analogous to an aircraft's "black box," records vessel operation commands, equipment status, and other information, and holds significant value in accident investigations and liability determinations.

Maritime information system data includes ship registration information, crew certificates, port State control inspection records, and the like. Such information is typically stored in the databases of maritime administration authorities and carries a relatively high degree of authority and reliability. In cases involving identity fraud, verifying the true status of ship ownership or mortgage often requires querying the ship registration system.

Communication and payment records serve as key evidence connecting the fraud perpetrator and the victim. Emails and WeChat chat records can prove the communications between the parties regarding transaction terms, while bank transfer records directly reflect the flow of funds. In freight forwarding fraud cases, records such as booking confirmations and fee acknowledgements sent by the freight forwarder via WeChat often become crucial evidence for determining liability.

2.3 Characteristics of Electronic Evidence in Maritime Fraud Cases

Electronic evidence in maritime fraud cases exhibits the following notable characteristics.

Technological dependence: The generation, storage, and transmission of electronic evidence all depend on specific technological systems, and its authenticity review requires the assistance of technical means. For example, the authenticity of AIS data depends on the operational status of the vessel's equipment and the integrity of data transmission; the authenticity of emails depends on the log records of the mail server.

Susceptibility to tampering: Compared with traditional evidence, electronic evidence is more vulnerable to tampering, and such tampering is often covert. By modifying file metadata, altering communication records, forging electronic signatures, or similar methods, a wrongdoer can change the content of electronic evidence without leaving obvious traces.

Cross-border nature: Maritime fraud cases often involve multiple jurisdictions, and the places where electronic evidence is generated or stored may be distributed across different countries. For instance, the server hosting an email may be located overseas, bank transfer records may involve foreign banks, and AIS data may be stored by an overseas entity. This cross-border nature creates additional difficulties for evidence collection and authentication.

Massive volume: The amount of electronic data generated in modern shipping trade activities is extremely large. The AIS data of a single vessel can accumulate millions of records over a year, and the number of email exchanges may also reach hundreds or thousands. How to screen out electronically stored information with evidentiary value from such massive data has become a technical challenge in

judicial practice.

3. Legal Framework and Practical Dilemmas of Electronic Evidence Authentication

3.1 Admissibility Rules for Electronic Evidence

For electronic evidence to serve as a basis for fact-finding, it must satisfy the three elements of admissibility: authenticity, legality, and relevance. The authentication rule for authenticity lies at the core of electronic evidence authentication. The best evidence rule in traditional evidence law requires the production of original documents; however, the special nature of electronic evidence makes the original document rule difficult to apply directly. Current legal norms have adopted a pragmatic approach, abandoning the traditional best evidence rule and shifting toward standards of content integrity and reliability. Specifically, authenticity authentication requires consideration of the following factors: whether the process of generating, storing, and transmitting the electronic evidence was proper; whether the integrity of the electronic evidence has been preserved; whether the electronic evidence has been tampered with; and whether the auxiliary information of the electronic evidence is complete.

There is a difference in authenticity authentication between electronic data from closed systems and that from open systems. A closed system refers to an environment with strict controls over the generation, storage, and transmission of data, such as an internal business system of an enterprise; an open system refers to an open environment such as the internet. For electronic evidence generated from a closed system, its authenticity may be presumed; for electronic evidence generated from an open system, stricter scrutiny is required.

The legality authentication rule primarily addresses whether the collection process of electronic evidence complies with legal norms. Article 106 of the Interpretation of the Civil Procedure Law provides that evidence formed or obtained by means that seriously infringe upon the lawful rights and interests of another person, violate prohibitive provisions of law, or seriously contravene public order or good morals shall not be used as a basis for determining case facts. Legality authentication requires examining whether the evidence-collecting subject is qualified, whether the method of collection is lawful, whether the scope of collection is appropriate, and whether the collection procedures are proper.

The relevance authentication rule requires that there be a substantial connection between the electronic evidence and the facts to be proved. In maritime fraud cases, it is necessary to examine whether the electronic evidence can prove key facts such as the existence of the fraudulent act, the nature of the fraud, and the losses caused by the fraud.

3.2 Empirical Examination of Judicial Practice

Based on an empirical analysis of adjudicative documents from selected maritime courts, the following trends in the application of electronic evidence in maritime litigation can be observed: the proportion of cases in which electronic evidence is submitted has been increasing year by year. Taking the case data from the Qingdao Maritime Court for the period 2016 to 2018 as an example, the proportion of cases in

which electronic data evidence was submitted rose from 8% to 15%. This trend reflects the rising status of electronic evidence in maritime litigation.

Maritime-specific electronic evidence accounts for approximately 50% of cases involving electronic evidence. Among maritime cases involving electronic evidence, about half use maritime-specific electronic evidence. Among these, electronic customs declarations and container movement records appear most frequently.

The admission rate of electronic evidence is closely related to the method by which it was fixed. Empirical data show that the admission rate for electronic evidence where the party merely submitted a printout is relatively low, whereas electronic evidence that has been notarized is almost always admitted. This phenomenon reflects an over-reliance on notarization in judicial practice and also reveals the absence of independent authentication rules for electronic evidence.

Different maritime courts exhibit differences in authenticating the same type of electronic evidence. Some courts adopt a stricter approach to authenticating WeChat chat records, requiring the production of complete chat logs and verification of the identity of the parties; other courts are relatively lenient, reviewing only the coherence of the chat record content.

3.3 Main Practical Dilemmas

At the institutional level, the legal regime for electronic evidence remains imperfect, with a lack of unified authentication standards. Since the 2012 Civil Procedure Law added electronic data as an independent statutory category of evidence, the legal status of electronic evidence has been established, yet its authentication rule system still contains significant gaps. Current legislation and judicial interpretations lack systematic and detailed provisions on the criteria for reviewing the authenticity of electronic evidence, leading to marked divergences in the handling of electronic evidence in judicial practice. Research has pointed out that in current civil litigation, the admissibility standards and review rules for electronic evidence suffer from fragmented authentication criteria, one-sided review of relevance, and ambiguous review of legality (Zhang, F., 2025, pp. 64-66). For instance, courts hold diametrically opposing views on the evidentiary competence of printouts from third-party financial and accounting systems: the Chengdu Intermediate People's Court recognizes and admits such printouts of electronic data stored on third-party platforms, whereas the Guangdong Higher People's Court rejects their authenticity, relevance, and legality in their entirety. Such inconsistent judgments arising from the absence of unified authentication standards seriously undermine the uniformity and predictability of judicial decisions.

The Special Maritime Procedure Law was enacted in 1999, a time when electronic evidence had not yet become a mainstream form of proof. The Law contains no special provisions on the collection, preservation, or authentication of electronic evidence, making it ill-suited to meet the review demands of emerging electronic evidence in maritime litigation, such as electronic navigation records and electronic bills of lading. Furthermore, the institutional design for electronic data forensics in the current criminal justice system is still premised on static storage media. Legislators and judicial

practitioners assume that forensic targets are relatively singular hard disks, servers, or mobile terminals, and that the evidence generation process can be fully reproduced through one-time mirroring, hash verification, and chain-of-custody documentation (Li, X. K., & Dai, S. J., 2026, pp. 46-62). This framework cannot effectively respond to the demands of cross-platform and cross-entity behavioral stream forensics in the big data era.

At the judicial level, the quality of electronic evidence admissibility is unsatisfactory, and the problem of insufficient reasoning in judgments is severe. Some judicial documents fail to provide sufficient grounds for admitting or excluding electronic evidence, merely stating that "the authenticity of the evidence is confirmed" or "the evidence is not admissible." This leaves parties unable to understand the court's reasoning and hinders supervisory review by higher courts. Such insufficient reasoning reflects both inadequate judicial grasp of electronic evidence authentication rules and a lack of capacity and willingness to elaborate reasoning. Where electronic data cannot be corroborated by other evidence, its authenticity remains uncertain, requiring the allocation of burden of proof to resolve adjudication. However, different courts apply divergent conceptions of burden of proof, often resulting in inconsistent rulings (Chen, Y. T., 2025).

Notably, with the popularization of generative artificial intelligence, an increasing number of cases involve parties submitting AI-generated content as evidence, posing greater challenges for courts in reviewing and authenticating such new forms of electronic evidence. In practice, no consensus has been reached on the boundaries between electronic data and other types of evidence or on the admissibility rules for electronic data, further exacerbating uncertainty in adjudication.

At the technical level, the inherent characteristics of electronic evidence—its susceptibility to tampering and loss—present fundamental difficulties for authentication. Electronic data features easy duplication, modification, and deletion (Xie, D. K., 2024, pp. 121-131). Without technical safeguards, it is often difficult to determine whether electronic evidence submitted by parties is authentic and complete. This is particularly true for electronic evidence generated in open systems, such as WeChat chat records and emails, which parties can easily delete or modify without leaving traces, posing severe challenges to authenticity review.

Significantly, on August 14, 2025, the Supreme People's Court formally issued the Provisions on Several Issues Concerning Electronic Evidence Rules in Online Litigation. For the first time in the form of judicial interpretation, it clarified the rules for reviewing the validity of electronic evidence stored and fixed through blockchain technology. It stipulates that electronic data stored on qualified third-party blockchain evidence platforms and complying with relevant technical and regulatory requirements shall be presumed by the people's courts to be untampered, unless rebutted by sufficient evidence to the contrary. This provision provides clear judicial recognition and legal protection for blockchain evidence storage and will substantially reduce parties' burden of proving the authenticity of electronic evidence and their litigation costs.

Nonetheless, current rules on blockchain evidence remain notably limited. No closed-loop protection has been established for the original authenticity and storage security of pre-chain data. Pre-chain data in blockchain storage does not benefit from the presumption of authenticity and must satisfy stricter requirements for review, including clear provenance of electronic data and traceability of collection and storage processes. This effectively strengthens the producing party's burden of proof at the stages of data generation and fixation.

Beyond the difficulties in the three dimensions mentioned above, the application of electronic evidence also faces two special challenges.

First, the authentication of cross-border electronic evidence is difficult. Electronic evidence generated abroad encounters legal obstacles to cross-border collection. Based on the principle of sovereignty, cross-border collection of electronic data mainly relies on international criminal judicial assistance mechanisms. However, this traditional model suffers from extremely low efficiency. Given that electronic evidence critical to cross-border cybercrime is prone to tampering and deletion, it may be permanently lost if not promptly extracted and preserved. Scholars have noted that the easy transfer and vulnerability of electronic data render traditional judicial assistance inefficient due to delays, while unilateral collection is restricted by sovereignty concerns. Cross-border electronic evidence also requires cumbersome notarization and authentication procedures, which are time-consuming and labor-intensive, further increasing authentication difficulties (Han, X. L., 2025, pp. 44-55).

Second, the identification of user identities in instant messaging applications is problematic. In applications such as WeChat and QQ, users often use nicknames rather than real names, making it a widespread practical difficulty to link online identities with real-world persons. Instant messaging records constitute an evidence system composed of various types of evidence classified by different standards (Chen, H., 2024, pp. 121-131). Existing general legislation tends to overlook internal typological differences and fails to resolve issues such as the authentication of communicators' identities, the protection of privacy in communications, and the interpretation of non-verbal symbols. In judicial practice, WeChat chat records used as evidence must satisfy requirements of genuine identity, complete content, and clear expression. Confirming the identity of the chat participant becomes a primary issue, requiring parties to submit screenshots containing avatars, nicknames, and account numbers to link the correspondent to the party concerned.

The difficulties at the institutional, judicial, and technical levels, together with the special challenges, are intertwined and jointly shape the complex landscape of judicial application of electronic evidence at present.

4. Technology Empowerment: Innovative Paths for Electronic Evidence Authentication

4.1 Development of Evidence-Fixing Technologies for Electronic Evidence

Faced with the practical dilemmas of electronic evidence authentication, technological developments offer potential pathways to resolve the difficulties. Currently, the following key technologies have been developed in the field of electronic evidence fixing:

Trusted timestamp (TSA) technology, by binding the hash value of electronic data to an exact time and issuing a timestamp certificate from an authoritative timestamp service provider, can prove that the electronic data existed before a specific point in time and has not been tampered with. This technology has been applied in judicial practice in China, and some courts have admitted electronic evidence fixed using trusted timestamps.

Hash value verification technology generates a unique digital "fingerprint" for each electronic file by calculating its hash value. Any change in the content of the electronic data will alter its hash value. By comparing hash values at different points in time, it is possible to determine whether the electronic data has been tampered with. Hash value verification is the foundation for technologies such as blockchain-based evidence storage and trusted timestamps.

Blockchain-based evidence storage technology utilizes the technical characteristics of blockchain, including distributed storage, immutability, and traceability, to achieve reliable storage of electronic evidence. Blockchain-based evidence storage records the hash value of electronic data on the blockchain and protects the integrity and security of the data through a consensus mechanism among distributed nodes. In 2018, the Hangzhou Internet Court confirmed for the first time the evidentiary effect of blockchain-based evidence storage, opening a new path for electronic evidence authentication.

4.2 Blockchain Evidence Review Practice of the Shanghai Maritime Court

In September 2022, the Shanghai Maritime Court issued the Guidelines for Reviewing Blockchain Evidence, becoming the first maritime court in China to issue a judicial document specifically addressing the review of blockchain evidence. The Guidelines specify the key points for reviewing blockchain evidence, include judicial blockchain platforms, third-party evidence storage platforms, and shipping blockchain application platforms within the scope of review, and set out corresponding review standards for different types of blockchain evidence.

In a typical case, the Shanghai Maritime Court admitted electronic evidence fixed using a trusted timestamp. In a dispute over a maritime freight forwarding contract, the plaintiff used trusted timestamp technology to fix WeChat chat records. After review, the court held that the process of generating and storing the evidence complied with technical specifications, and that its authenticity could be established, thereby using it as a basis for decision.

The Shanghai Maritime Court's exploration reflects the judiciary's open attitude toward technological innovation and demonstrates the practical possibility of using technology to empower electronic evidence authentication. By formulating clear review standards, the court provides parties with predictable guidance on evidence preservation and offers technology service providers a direction for

regulated development.

4.3 Xiamen Maritime Court's Innovations in Foreign Evidence Collection

In August 2022, the Xiamen Maritime Court issued the Guidelines on Several Issues Concerning the Collection and Review of Foreign Evidence, the first judicial guideline in China specifically addressing foreign evidence. The Guidelines propose six methods for collecting foreign evidence, including innovative practices such as using blockchain technology to verify the "original" electronic data and online "live evidence collection." The Guidelines clarify that parties may use blockchain technology to verify foreign electronic data, and the verification results may serve as a basis for determining the authenticity of the evidence. Additionally, the Guidelines permit parties to use online "live evidence collection" – real-time retrieval and verification of foreign electronic data under the supervision of a judge – to solve the problems of cumbersome procedures and long processing times associated with traditional notarization and legalization.

The innovative practices of the Xiamen Maritime Court provide valuable explorations for cross-border electronic evidence authentication. Simplifying the procedure for collecting foreign evidence through technical means reduces the burden of proof on parties and improves judicial efficiency.

5. Legal Scrutiny of Technology Application

While technology empowers electronic evidence authentication, rational scrutiny of technology application must be maintained. First, the principle of technological neutrality should be upheld: the use of a particular technology should not automatically establish the authenticity of the evidence, nor should the absence of emerging technologies negate the value of the evidence. Technology is merely a tool; the ultimate determination of evidence must return to legal standards.

Second, a balance must be struck between technological self-validation and judicial review. Although technologies such as blockchain-based evidence storage and trusted timestamps can prove that electronic data has not been tampered with after a specific point in time, they cannot guarantee the authenticity of the electronic data at the time of its generation, nor can they guarantee the authenticity of data before it is uploaded to the chain. Therefore, judicial review must still comprehensively assess the entire process of generating and storing the electronic evidence.

Third, the alignment of technical standards with legal rules should be advanced. Technology service providers should follow uniform technical standards to ensure the regularity and reliability of the evidence-fixing process; judicial rules should evaluate compliance with technical standards, thereby creating an institutional environment of positive interaction.

6. Building a Regulatory System for Electronic Evidence Adapted To Maritime Fraud Cases

6.1 Recommendations for Legislative Improvement

Establish electronic evidence authentication rules in the revision of the Special Maritime Procedure Law. The revision of the Special Maritime Procedure Law has been placed on the legislative agenda. This opportunity should be seized to incorporate electronic evidence authentication rules into the scope of revision. It is recommended to add specific provisions on electronic evidence authentication, clarifying the definition of electronic evidence, standards for authenticity review, requirements for legality review, and related matters.

Formulate unified standards for the review and authentication of electronic evidence. On the basis of the Civil Procedure Law and its judicial interpretations, the Supreme People's Court may issue a specialized judicial interpretation on the review and authentication of electronic evidence, providing uniform provisions on the key points and standards for reviewing different types of electronic evidence, thereby resolving the problem of inconsistent standards in current judicial practice.

Establish graded authentication standards. Based on the technical characteristics and application scenarios of electronic evidence, graded authentication standards should be established. For electronic evidence generated from closed systems, a presumption of authenticity may apply; for electronic evidence generated from open systems, stricter scrutiny is required; for electronic evidence fixed using technologies such as blockchain-based storage, the difficulty of authentication may be appropriately reduced after reviewing technical compliance.

6.2 Recommendations for Judicial Improvement

Improve guidelines for the production and examination of electronic evidence. Maritime courts may formulate operational guidelines for the production and examination of electronic evidence, clarifying the form of submission, content requirements, technical specifications, etc., to guide parties in producing evidence properly. At the same time, they may provide technical guidance on the collection and fixing of electronic evidence to lawyers and parties, thereby improving the quality of evidence production.

Strengthen the obligation to state reasons in adjudicative documents. When a court decides to admit or reject electronic evidence, it should explain its reasons in the adjudicative document. For admitted electronic evidence, the court should state the reasons why the requirements of authenticity, legality, and relevance are satisfied; for rejected electronic evidence, the court should state the specific reasons for rejection.

Establish a system of typical case guidance for electronic evidence authentication. The Supreme People's Court and the higher people's courts may periodically publish typical cases on electronic evidence authentication, using case guidance to unify adjudicative standards and provide reference for lower courts.

6.3 Recommendations for Technical and Infrastructure Improvement

Promote the construction of a unified platform for maritime electronic evidence. It is recommended to build a unified evidence storage platform for maritime electronic evidence, relying on the informatization construction of maritime courts. The platform should have functions for uploading, storing, verifying, and retrieving electronic evidence, and should interface with shipping blockchain application platforms to achieve "one-stop" management of electronic evidence.

Standardize the judicial application standards for blockchain-based evidence storage. Drawing on the pioneering experience of the Shanghai Maritime Court and others, unified judicial application standards for blockchain-based evidence storage should be formulated, clarifying the scope of application, technical specifications, review points, etc., to provide regulatory guidance for the application of blockchain technology in the judicial field.

Interface with shipping blockchain application platforms. As the digital transformation of the shipping industry advances, shipping blockchain application platforms continue to emerge. Judicial platforms should interface with these application platforms to achieve interoperability of electronic evidence. For example, for an electronic bill of lading generated from an electronic bill of lading platform, the court could directly retrieve and verify it from the platform, avoiding the need for the parties to produce evidence repeatedly.

7. Conclusion

The application and regulation of electronic evidence in maritime fraud cases is an important issue facing maritime justice in the digital era. Through a systematic analysis of the basic types and characteristics of electronic evidence in maritime fraud cases, an examination of the legal framework and practical dilemmas of electronic evidence authentication, and an exploration of technology-empowered innovative paths for authentication, this paper draws the following main conclusions:

First, electronic evidence in maritime fraud cases is diverse and exhibits characteristics such as technological dependence, susceptibility to tampering, cross-border nature, and massive volume, which pose special difficulties for judicial authentication.

Second, current electronic evidence authentication faces a triple dilemma at the institutional, judicial, and technical levels: at the institutional level, a lack of uniform authentication standards; at the judicial level, low quality of admission decisions and a serious lack of reasoning; at the technical level, the prominent problems of electronic evidence being easily tampered with or lost.

Third, the judicial application of new technologies such as blockchain-based evidence storage and trusted timestamps provides innovative paths for electronic evidence authentication. The issuance of the Shanghai Maritime Court's Guidelines for Reviewing Blockchain Evidence and the Xiamen Maritime Court's Guidelines on Several Issues Concerning the Collection and Review of Foreign Evidence reflects the judiciary's open attitude toward technological innovation and also offers valuable

explorations for technology-empowered electronic evidence authentication.

Fourth, improving the regulatory system for electronic evidence requires coordinated efforts at four levels: legislative, judicial, technical, and international cooperation. At the legislative level, the opportunity to revise the Special Maritime Procedure Law should be seized to construct unified electronic evidence authentication rules; at the judicial level, guidelines for evidence production and examination should be improved, and reasoning in adjudicative documents strengthened; at the technical level, the construction of a unified platform for maritime electronic evidence should be advanced; at the international cooperation level, mechanisms for cross-border electronic evidence collection should be improved and international mutual recognition of electronic evidence promoted.

This paper has certain limitations. Due to constraints in obtaining empirical data, the statistical analysis of electronic evidence admission rates is not fully comprehensive; comparative research on foreign electronic evidence authentication systems needs further deepening. Future research may, on this basis, further expand the scope of empirical research and deepen comparative law studies, thereby providing a more solid theoretical foundation and practical reference for improving China's regulatory system for electronic evidence.

References

Chen, H. (2024). A Study on the Authentication Rule System of Instant Messaging Records: Based on the Logical Premise of Type Definition. *Journal of Shenzhen University*, *41*(03), 121-131.

Chen, Y. T. (2025). *Admissibility and Weight of Electronic Data in Civil Litigation*. Retrieved September 12, 2025, from https://www.chengrulaw.cn/viewpoint/1502.html

Han, X. L. (2025). Practical Dilemmas and Adjustment Paths for Electronic Data Forensics in Cross-Border Cybercrime. *Journal of Guizhou Police College*, *37*(05), 44-55.

Li, X. K., & Dai, S. J. (2026). From "Large-Scale Data" to "Big Data": Paradigm Shift and Model Construction in Electronic Data Forensics and Examination. *Journal of National Prosecutors College*, *34*(01), 46-62.

Xie, D. K. (2024). On Legal Effect and Judicial Review of Electronic Data Authenticated by Trusted Timestamp. *Journal of Law Application*, *41*(03), 121-131.

Zhang, F. (2025). On the Admissibility Standards and Optimization of Review Rules for Electronic Evidence in Civil Litigation. *Legality Vision*, *2025*(24), 64-66.