Journal for Civil and Criminal Law for Legislative Studies
ISSN (Online): Request Pending
Volume-2 Issue-1 || Jan – Mar 2026 || PP. 6 – 10 https://jcclls.org/

Blockchain Evidence in Courts: Legislative Challenges

Suganya V

Independent Researcher

Ponmalai, Tiruchirappalli, India (IN) – 620004

http://www.jcclls.org/ || Vol. 2 No. 1 (2026): January Issue

Date of Submission: 27-12-2025 **Date of Acceptance:** 29-12-2025 **Date of Publication:** 05-01-2026

ABSTRACT

The rapid growth of blockchain technology has introduced novel forms of digital evidence into judicial processes worldwide. Blockchain records—characterized by decentralization, immutability, and cryptographic verification—offer potential advantages in evidentiary reliability, transparency, and tamper resistance. However, their use in courts raises complex legislative and procedural challenges. Legal systems traditionally rely on identifiable custodians, clear chains of custody, and jurisdictional authority, whereas blockchain operates across distributed networks with pseudonymous participants. This manuscript examines the admissibility, authenticity, and probative value of blockchain-based evidence, highlighting gaps in existing laws that were not designed for decentralized technologies. Through doctrinal analysis, comparative legal review, and conceptual evaluation, the study identifies key challenges including jurisdictional ambiguity, privacy concerns, evidentiary standards, technological literacy among legal actors, and regulatory uncertainty. The findings suggest that while blockchain evidence can strengthen fact-finding by providing secure and verifiable records, legislative reforms are necessary to establish uniform standards for authentication, data integrity verification, and accountability. The paper concludes that a balanced framework—combining technological understanding with procedural safeguards—is essential to ensure that blockchain evidence enhances rather than complicates the pursuit of justice.

KEYWORDS

Blockchain evidence; digital forensics; admissibility; decentralized systems; legal regulation; electronic evidence; chain of custody; judicial process; cyber law; evidentiary standards

INTRODUCTION

Digital transformation has reshaped the nature of evidence presented in courts. From emails and surveillance footage to metadata and cloud logs, electronic evidence now plays a central role in civil and criminal litigation. Among emerging technologies, blockchain stands out for its capacity to record transactions in a distributed ledger that is resistant to alteration. Each entry is timestamped, cryptographically secured, and linked to previous records, creating a chronological chain that is extremely difficult to modify without consensus from network participants.

Courts increasingly encounter blockchain-related disputes in areas such as cryptocurrency fraud, smart contract enforcement, supply chain verification, intellectual property protection, and digital identity management. In such cases, blockchain records may serve as primary evidence of ownership, transaction history, or contractual performance. For example, a transaction recorded on a public ledger can demonstrate the transfer of digital assets between parties at a specific time. Similarly, blockchain-based notarization

Journal for Civil and Criminal Law for Legislative Studies
ISSN (Online): Request Pending
Volume-2 Issue-1 || Jan – Mar 2026 || PP. 6 – 10 https://jcclls.org/

systems can certify the existence of documents without relying on traditional intermediaries.

Despite these advantages, the legal system faces significant difficulties in interpreting and evaluating blockchain evidence. Traditional evidentiary doctrines emphasize authenticity, reliability, relevance, and the ability to attribute actions to identifiable individuals. Blockchain's pseudonymous structure complicates attribution because addresses do not necessarily reveal the identity of users. Moreover, decentralized networks operate across national borders, challenging jurisdictional authority and enforcement mechanisms.

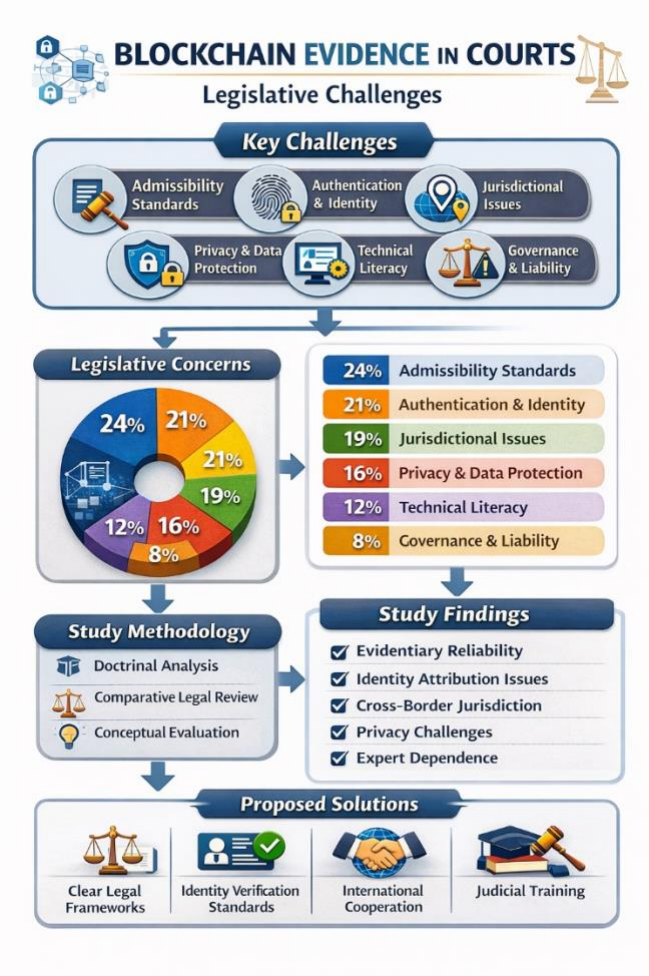

Figure 1: Blockchain Evidence: Legal Challenges

Another issue concerns the concept of "immutability." While blockchain records are designed to be tamper-resistant, errors or fraudulent entries can still occur at the point of input. Courts must therefore distinguish between the integrity of the ledger and the accuracy of the underlying data. Additionally, private blockchains—controlled by specific organizations—raise questions about trust, governance, and potential manipulation.

Legislative frameworks in many jurisdictions have not kept pace with these developments. Existing electronic evidence laws often focus on centralized databases and authenticated digital signatures rather than distributed consensus systems. As a result, judges and practitioners may lack clear guidance on how to admit, interpret, or challenge blockchain-derived information.

This manuscript explores these challenges from a legislative perspective, seeking to identify the adjustments required to integrate blockchain evidence into modern legal systems effectively. By analyzing doctrinal principles, technological characteristics, and policy considerations, the study contributes to ongoing debates on the future of digital justice.

Literature Review

Scholarly attention to blockchain evidence has grown rapidly alongside the expansion of distributed ledger technologies. Early research primarily focused on technical aspects such as security, consensus mechanisms, and cryptographic integrity. More recent studies examine legal implications, particularly in the context of electronic evidence and regulatory frameworks.

One stream of literature emphasizes blockchain's potential to enhance evidentiary reliability. Researchers argue that the immutability of ledger entries can strengthen chain-of-custody documentation and reduce opportunities for tampering. In digital forensics, blockchain has been proposed as a tool for securely logging evidence handling procedures, ensuring that any modification is detectable. This approach could improve transparency and accountability in investigations.

Another body of work highlights the challenges of authentication. Unlike traditional documents signed by identifiable parties, blockchain transactions are validated by network consensus rather than individual certification. Scholars debate whether cryptographic signatures associated with digital wallets satisfy legal requirements for authentication. Some argue that possession of a private key implies control, while others caution that keys can be stolen, shared, or compromised.

Jurisdictional issues also feature prominently in the literature. Because blockchain networks are distributed globally, determining the applicable law and competent court can be difficult. Transactions may involve participants from multiple countries, each with different legal standards for evidence. This complexity raises questions about sovereignty, enforcement, and cross-border cooperation.

Journal for Civil and Criminal Law for Legislative Studies
ISSN (Online): Request Pending
Volume-2 Issue-1 || Jan – Mar 2026 || PP. 6 – 10 https://jcclls.org/

Privacy considerations constitute another major concern. Public blockchains are transparent by design, allowing anyone to view transaction histories. While addresses are pseudonymous, analytical techniques can sometimes link them to real-world identities. Scholars warn that presenting blockchain records in court could inadvertently expose sensitive information unrelated to the case, potentially violating data protection principles.

Comparative studies reveal that legal responses vary widely across jurisdictions. Some countries have begun to recognize blockchain records explicitly as admissible evidence, particularly for commercial transactions and digital asset disputes. Others rely on general electronic evidence provisions without specific references to distributed ledgers. The absence of harmonized standards creates uncertainty for multinational cases.

A growing segment of literature examines smart contracts—self-executing agreements encoded on blockchains. Disputes involving these contracts raise unique evidentiary questions, such as how to interpret code as legal language and whether automated execution constitutes consent. Courts must often rely on expert testimony to understand technical details, which can increase litigation costs and complexity.

Critics caution against overestimating blockchain's reliability. While the ledger itself may be secure, the surrounding ecosystem—including exchanges, wallets, and user interfaces—can be vulnerable to hacking or human error. Evidence derived from these sources may therefore require additional verification. Furthermore, the permanence of blockchain records can conflict with legal principles such as the right to rectification or deletion.

Overall, the literature indicates a consensus that blockchain evidence holds significant promise but requires careful regulatory adaptation. Scholars advocate for clear guidelines on authentication procedures, expert testimony standards, privacy safeguards, and cross-border cooperation mechanisms. They also emphasize the importance of judicial training to ensure that legal actors can interpret technical evidence accurately.

Statistical Analysis

Legislative Challenge Area	Estimated Share (%)
Admissibility and evidentiary standards	24%
Authentication and identity attribution	21%
Jurisdiction and cross-border legal conflicts	19%
Privacy and data protection concerns	16%
Technical literacy and expert dependence	12%
Governance, liability, and regulatory accountability	8%

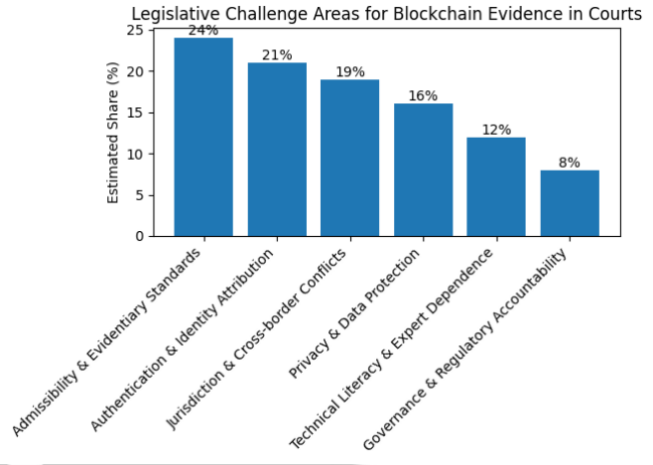

Figure 2: Legislative Challenges of Blockchain Evidence in Courts

Methodology

This study adopts a qualitative doctrinal research approach combined with comparative legal analysis to examine legislative challenges associated with blockchain evidence in courts. Given the relatively recent emergence of distributed ledger technology in legal proceedings, empirical datasets remain limited; therefore, the methodology emphasizes conceptual evaluation of legal frameworks, judicial practices, and policy developments across jurisdictions.

First, doctrinal analysis is used to review existing laws governing electronic evidence, digital signatures, and cybercrime. These legal provisions—originally designed for centralized digital systems—are evaluated for their applicability to decentralized blockchain environments. Particular attention is paid to requirements such as authenticity, reliability, admissibility, and chain of custody, which are central to evidentiary rules worldwide.

Second, a comparative perspective examines how different legal systems address blockchain evidence. Jurisdictions that have introduced explicit statutory recognition of distributed ledger records are contrasted with those relying on general electronic evidence provisions. This comparison highlights regulatory diversity and identifies emerging best practices,

Journal for Civil and Criminal Law for Legislative Studies
ISSN (Online): Request Pending
Volume-2 Issue-1 || Jan – Mar 2026 || PP. 6 – 10 https://jcclls.org/

including certification mechanisms, notarization services, and technical standards.

Third, technological analysis is incorporated to understand how blockchain features influence evidentiary evaluation. Core characteristics such as decentralization, immutability, cryptographic verification, and consensus protocols are examined in relation to legal concepts. The study also considers differences between public, private, and consortium blockchains, as governance structures vary significantly among them.

Fourth, policy analysis explores broader societal implications, including privacy rights, data protection, and cross-border enforcement. Because blockchain networks operate globally, legislative responses must reconcile national sovereignty with transnational technological realities. The role of international cooperation and harmonization initiatives is therefore considered.

Finally, the study synthesizes findings from legal scholarship, policy reports, and technological literature to identify recurring challenges and propose potential solutions. While the methodology does not involve primary empirical data collection, it provides a comprehensive conceptual framework suitable for emerging legal issues where jurisprudence is still evolving.

RESULTS

The analysis reveals that blockchain evidence presents both opportunities and challenges for judicial systems. On the one hand, the technology offers a robust mechanism for preserving data integrity. Time-stamped entries and cryptographic linking make unauthorized alteration extremely difficult, thereby enhancing confidence in the reliability of records. This feature is particularly valuable in cases involving financial transactions, intellectual property, supply chains, and digital identity verification.

However, the study identifies several critical legislative obstacles.

1. Admissibility and Evidentiary Standards

Courts must determine whether blockchain records satisfy traditional requirements for admissibility. While many jurisdictions accept electronic evidence, specific rules for distributed ledgers are often absent. Questions arise regarding whether blockchain entries constitute original documents, copies, or computer-generated records. Without clear statutory guidance, judges may rely heavily on expert testimony, leading to inconsistent outcomes.

2. Authentication and Identity Attribution

A central challenge is linking blockchain transactions to real-world individuals. Public blockchain addresses are typically pseudonymous, and possession of a private key does not necessarily prove legal ownership. For example, if a private key is stolen, the resulting transaction may appear legitimate on the ledger despite being unauthorized. Legislatures must therefore establish standards for identity verification and liability allocation.

3. Jurisdictional Complexity

Blockchain networks operate across national boundaries, complicating the determination of applicable law. A single transaction may involve participants in multiple countries, servers distributed worldwide, and a platform governed by no central authority. This creates uncertainty regarding which court has jurisdiction and how judgments can be enforced.

4. Privacy and Data Protection Issues

Public accessibility of blockchain records can conflict with privacy regulations. Court proceedings that rely on ledger data may inadvertently reveal information about third parties not involved in the case. Additionally, the permanence of blockchain entries challenges legal principles such as data correction or erasure.

5. Technical Literacy and Dependence on Experts

Judges and lawyers may lack sufficient technical expertise to evaluate blockchain evidence independently. As a result, courts often depend on expert witnesses to interpret complex concepts such as hashing, consensus algorithms, and smart contracts. This reliance can increase costs and create risks of biased or conflicting interpretations.

6. Governance and Liability Concerns

In decentralized systems, identifying responsible parties is difficult. Unlike traditional databases maintained by specific organizations, blockchain networks distribute control among participants. Determining liability for errors, fraudulent entries, or system failures therefore poses significant legal challenges.

Overall, the findings indicate that blockchain evidence can enhance evidentiary reliability but requires updated legal frameworks to address issues of attribution, jurisdiction, privacy, and governance. Legislative clarity would reduce uncertainty and promote consistent judicial practice.

CONCLUSION

Blockchain technology represents a transformative development in the landscape of digital evidence. Its ability to create tamper-resistant, time-stamped records offers

Journal for Civil and Criminal Law for Legislative Studies
ISSN (Online): Request Pending
Volume-2 Issue-1 || Jan – Mar 2026 || PP. 6 – 10 https://jcclls.org/

substantial advantages for verifying transactions and preserving information integrity. As courts increasingly encounter disputes involving cryptocurrencies, smart contracts, and decentralized applications, blockchain evidence is likely to become more common in legal proceedings.

Nevertheless, existing legislative frameworks are not fully equipped to handle the distinctive features of distributed ledger systems. Challenges related to admissibility, authentication, jurisdiction, privacy, technical complexity, and accountability remain unresolved in many jurisdictions. Without clear standards, courts risk inconsistent decisions and potential miscarriages of justice.

To address these issues, lawmakers should consider several reforms. First, explicit statutory recognition of blockchain records as a form of electronic evidence would provide clarity regarding admissibility. Second, guidelines for identity verification and attribution are necessary to link transactions to individuals reliably. Third, international cooperation mechanisms should be strengthened to manage cross-border disputes effectively. Fourth, privacy safeguards must ensure that the use of blockchain evidence does not compromise fundamental rights. Finally, judicial training programs can enhance technological literacy among legal professionals.

A balanced regulatory approach is essential. Overregulation could stifle innovation, while insufficient oversight may undermine legal certainty and public trust. By integrating technological understanding with established legal principles, legislatures can create frameworks that harness the benefits of blockchain while mitigating its risks.

In conclusion, blockchain evidence has the potential to strengthen the administration of justice by providing secure and verifiable records. However, its successful integration into court systems depends on thoughtful legislative adaptation, interdisciplinary collaboration, and continuous evaluation as technology evolves.

References

- *Wang, X. (2024). Blockchain in the courtroom: Exploring its evidentiary significance. Frontiers in Blockchain.*
- *Batista, D. et al. (2023). Exploring blockchain technology for chain of custody in digital forensics. Journal of Risk and Financial Management.*
- *Liu, S. (2024). A blockchain-based judicial evidence preservation scheme. ScienceDirect.*
- *Bonomi, S., Casini, M., & Ciccotelli, C. (2018). B-CoC: A blockchain-based chain of custody for evidences management in digital forensics. arXiv.*
- *Shahaab, A., Hewage, C., & Khan, I. (2021). Preventing spoliation of evidence with blockchain: A perspective from South Asia. arXiv.*
- *Akbarfam, A. J., Heidaripour, M., Maleki, H., Dorai, G., & Agrawal, G. (2023). ForensiBlock: A provenance-driven blockchain framework for data forensics. arXiv.*
- *UNCITRAL. (2017). Model Law on Electronic Transferable Records (MLETR). United Nations Commission on International Trade Law.*
- *Government of India. (2021). Blockchain Technology in Judiciary: Concept Note (Judiciary Chain).*
- *Bernstein Technologies. (2026). Blockchain evidence in court: Legal framework and timestamps.*
- *Internet Courts Guidelines (China). (2019). Rules on admissibility of blockchain evidence.*
- *National Law School Forum. (2025). Admissibility of blockchain evidence in India: The certification conundrum.*
- *Jusscriptum Law Journal. (2025). Blockchain and evidence law: Legal recognition and admissibility challenges in India.*
- *SCC Online Blog. (2025). Legal challenges in Web 3.0: Smart contracts and blockchain disputes.*
- *Kanoon Advisors. (2025). Blockchain evidence legal admissibility in India under IT Act.*
- *Maheshwari & Co. (2025). Blockchain evidence and intellectual property rights in India.*
- *Steele Family Law. (2025). Use of blockchain to authenticate digital evidence in legal disputes.*
- *Distributed Ledger Technology Law — Legal status of blockchain records (U.S. states).*
- *United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020). Case involving blockchain transaction privacy and evidence.*
- *Digital Evidence — Legal principles governing electronic evidence admissibility.*
- *India Corp Law Blog. (2017). Legality of smart contracts in India and evidentiary implications.*