JOURNAL OF LAW, INFORMATION & SCIENCE
ISSN 0729-1485• Vol. 3, Issue 1 (2025) • https://jlisjournal.com/

REVIEW ARTICLE Article ID: JLIS/2025/3/1/003

Blockchain-Based Digital Evidence: Legal Admissibility, Authenticity and Evidentiary Challenges

Dr. Aditya Verma [1], Prof. Rohan Mehta [2]

[1] *Centre for Cyber Law and Digital Evidence, National Law and Technology Institute, New Delhi, India*
[2] *Department of Information Technology and Evidence Law, Institute of Legal Studies, Bengaluru, India*

Received: 18 Jan 2025 **Revised:** 28 Jan 2025 **Accepted:** 28 Jan 2025 **Published:** 17 March 2025

ABSTRACT

The increasing digitization of social, commercial, and governmental activities has transformed the nature of evidence available in legal proceedings. Blockchain technology, through its distributed architecture, cryptographic verification, and tamper-evident recordkeeping, offers a potential mechanism for improving the authenticity and integrity of digital evidence. However, the technological characteristics of blockchain do not automatically resolve traditional evidentiary questions concerning relevance, reliability, authenticity, attribution, chain of custody, and admissibility. This article examines the potential application of blockchain technology in the preservation and verification of digital evidence. It analyzes the relationship between distributed ledgers, cryptographic hashes, timestamps, digital signatures, and evidentiary principles. Particular attention is given to the distinction between proving that information has remained unchanged and proving that the underlying information is accurate or genuinely attributable to a particular person. The article further examines challenges associated with privacy, blockchain immutability, technical complexity, smart contracts, forensic investigation, and judicial understanding of blockchain-generated records. It proposes a blockchain-enabled evidence framework incorporating secure collection, cryptographic verification, documented chain of custody, identity authentication, independent validation, and judicially understandable technical documentation. The article concludes that blockchain can strengthen evidentiary integrity, but technological immutability should complement rather than replace established legal standards governing admissibility and proof.

Keywords: *Blockchain; Digital Evidence; Evidence Law; Digital Forensics; Cryptographic Hash; Authenticity; Chain of Custody.*

1. Introduction

The digital transformation of society has fundamentally changed the nature of evidence used in legal proceedings. Emails, electronic documents, CCTV recordings, mobile-phone records, transaction logs, cloud data, social-media content, and other electronically generated information increasingly form part of civil and criminal litigation.

Digital evidence, however, presents distinctive challenges.

Unlike traditional physical documents, electronic information can be copied, modified, deleted, transferred, or manipulated without obvious physical signs of alteration.

Courts therefore require reliable methods for establishing authenticity and integrity.

Blockchain technology has emerged as a potentially useful tool in this context.

A blockchain can record information in a distributed ledger using cryptographic mechanisms that make unauthorized alteration detectable.

This creates an important possibility: digital evidence could be associated with a cryptographically verifiable record showing when information was registered and whether it has subsequently changed.

Nevertheless, blockchain technology does not automatically establish that information is truthful.

If false information is entered into a blockchain, the system may preserve the false information with considerable integrity.

The legal significance of blockchain evidence must therefore be carefully distinguished from its technological properties.

---

2. Concept of Blockchain Technology

Blockchain is a distributed ledger technology in which transactions or records are organized into linked blocks and maintained across a network.

Cryptographic techniques are used to connect blocks and verify changes.

A simplified structure may be represented as:

Data → Hash → Block → Distributed Verification → Ledger

The system can create a tamper-evident record of information.

If previously recorded data is altered, the associated cryptographic relationships may no longer correspond.

This characteristic makes blockchain potentially useful for establishing the integrity of digital records.

---

3. Digital Evidence

Digital evidence refers broadly to electronically stored or generated information that may be relevant to a legal proceeding.

Examples include:

- emails;

- digital photographs;
- videos;
- electronic documents;
- transaction records;
- mobile-device data;
- computer logs;
- GPS information;
- social-media records; and
- cloud-storage records.

The increasing volume of digital evidence creates challenges for investigators and courts.

The key question is not simply whether electronic information exists but whether its origin, integrity, and reliability can be established.

---

4. Authenticity and Integrity

Two important evidentiary concepts are authenticity and integrity.

Authenticity concerns whether evidence is what it is claimed to be.

Integrity concerns whether the evidence has been altered or corrupted.

Blockchain technology may contribute significantly to demonstrating integrity.

For example, a cryptographic hash of a digital file can be recorded on a blockchain.

If the file is later modified, its hash may change.

The blockchain record can then be compared with the current hash to determine whether the file has changed.

However, this process does not necessarily prove who originally created the file.

---

5. Cryptographic Hashing

Hash functions convert digital information into a fixed-length cryptographic value.

For example:

Digital File → Hash Function → Unique Hash Value

Even a small modification to the underlying file can produce a different hash.

Investigators can therefore calculate the hash of evidence at the time of collection and compare it with a later hash.

Blockchain can provide an additional record of the original hash.

This can strengthen the evidentiary chain concerning digital integrity.

---

6. Chain of Custody

Chain of custody refers to the documented history of evidence from collection through examination and presentation.

A traditional chain of custody may involve records concerning:

1. who collected the evidence;
2. when it was collected;
3. where it was stored;
4. who accessed it;
5. whether it was transferred; and
6. how it was preserved.

Blockchain can potentially supplement these records by creating tamper-evident timestamps for important events.

However, blockchain cannot replace proper forensic procedures.

If an investigator incorrectly collects the original evidence, recording the resulting information on blockchain does not correct the original error.

---

7. Blockchain Timestamping

Timestamping can provide evidence concerning when a particular digital record was registered.

A digital document can be hashed and the resulting hash recorded on a blockchain.

The blockchain record may then provide an additional mechanism for establishing temporal integrity.

This can be useful in disputes involving:

- intellectual property;
- electronic agreements;
- digital communications;
- financial transactions; and
- document creation.

However, the technical timestamp should be interpreted alongside other evidence.

---

8. Digital Signatures

Digital signatures can strengthen the relationship between an electronic record and its purported signer.

A digital signature can provide evidence concerning:

- identity;
- authenticity;
- integrity; and
- authorization.

When combined with blockchain, digital signatures may create a stronger evidentiary architecture.

A simplified process is:

Identity Verification → Digital Signature → Hash Generation → Blockchain Registration

Nevertheless, the reliability of the system depends upon secure private-key management and trustworthy identity verification.

---

9. Blockchain Does Not Guarantee Truth

One of the most important limitations is that blockchain generally protects recorded information from undetected modification; it does not guarantee that the information was truthful when entered.

Consider a hypothetical example.

An individual uploads a manipulated photograph and records its hash on a blockchain.

The blockchain can demonstrate that the particular file associated with that hash has remained unchanged.

It cannot independently establish that the photograph accurately represents reality.

This distinction is essential for judicial evaluation.

---

10. Blockchain and Digital Forensics

Digital forensic investigators can potentially integrate blockchain into evidence-preservation procedures.

A possible process could involve:

Collection → Forensic Imaging → Hash Generation → Blockchain Registration → Secure Storage → Analysis → Court Presentation

Such a process could provide additional assurance that the evidence analyzed is the same evidence originally collected.

However, investigators must maintain conventional forensic documentation alongside blockchain records.

---

11. Blockchain Evidence in Criminal Investigations

Blockchain-based evidence preservation may be particularly relevant to criminal investigations involving large quantities of digital information.

Investigators may collect:

- computers;
- smartphones;
- surveillance footage;
- digital communications;
- transaction records; and
- cloud-based information.

Hashing and blockchain registration can help establish that digital evidence has not been altered after collection.

Nevertheless, investigators must also establish lawful acquisition and appropriate procedural safeguards.

---

12. Privacy Concerns

Blockchain's persistence can create privacy concerns.

If personal information is directly stored on an immutable distributed ledger, removing or correcting that information may become difficult.

A privacy-preserving architecture should therefore avoid placing unnecessary personal information directly on-chain.

A preferable approach may be:

Sensitive Data → Secure Off-Chain Storage

Cryptographic Proof/Hash → Blockchain

This approach can provide integrity verification while reducing unnecessary exposure of personal information.

---

13. Immutability and Legal Correction

Blockchain is often described as immutable or resistant to alteration.

However, legal systems frequently require information to be corrected, withdrawn, or challenged.

This creates an important tension.

If inaccurate information is recorded permanently, technological immutability may conflict with legal requirements concerning correction or deletion.

Therefore, blockchain evidence systems should distinguish between preserving an evidentiary history and permanently publishing personal information.

---

14. Smart Contracts as Evidence

Smart contracts can automatically execute predefined computer instructions.

The execution of a smart contract can generate records showing:

- time of execution;
- transaction details;
- participating addresses;
- relevant conditions; and
- resulting actions.

These records may become relevant in contractual disputes.

However, courts may still need to determine whether the coded transaction accurately reflects the parties' legal agreement.

Code execution and legal intention should therefore not automatically be treated as identical concepts.

---

15. Judicial Challenges

Blockchain evidence can be technically complex.

Judges and lawyers may encounter unfamiliar concepts such as:

- distributed consensus;
- cryptographic hashing;
- private keys;
- wallet addresses;
- smart contracts; and
- blockchain nodes.

Technical complexity should not prevent effective judicial scrutiny.

Experts may therefore be required to explain the operation and reliability of a blockchain-based evidence system in understandable terms.

---

16. Expert Evidence

Technical experts can assist courts in evaluating blockchain-related evidence.

An expert may explain:

- how the evidence was collected;

- how the hash was generated;
- how the blockchain record was created;
- how the record can be independently verified; and
- what conclusions can reasonably be drawn.

However, expert evidence should not replace judicial decision-making concerning legal admissibility.

The role of technology is to provide reliable information; the court determines its legal significance.

---

17. Blockchain and Electronic Contracts

Blockchain can also support evidence concerning electronic contracts.

For example, parties may use blockchain to record:

- contract hashes;
- digital signatures;
- execution timestamps;
- amendments; and
- performance-related events.

Such records may assist in resolving disputes concerning which version of a digital contract existed at a particular time.

Again, blockchain can strengthen evidence concerning integrity but does not independently establish the parties' intention.

---

18. Proposed Blockchain Evidence Framework

A comprehensive framework may consist of seven stages.

Stage 1 – Lawful Collection

Digital evidence should be obtained through appropriate legal and forensic procedures.

Stage 2 – Forensic Preservation

A verified forensic copy should be created.

Stage 3 – Hash Generation

A cryptographic hash should be generated.

Stage 4 – Blockchain Registration

The hash and appropriate metadata may be recorded on a trusted blockchain.

Stage 5 – Secure Storage

The original evidence should remain securely preserved.

Stage 6 – Independent Verification

The evidence hash can be recalculated and compared with the blockchain record.

Stage 7 – Judicial Presentation

Technical documentation and expert explanation should be provided where necessary.

---

19. Security Requirements

A blockchain evidence system should incorporate strong security measures.

These may include:

- cryptographic hashing;
- secure key management;
- access controls;
- digital signatures;
- multi-factor authentication;
- secure forensic storage;
- independent verification; and
- detailed audit logs.

The system should also undergo periodic security testing.

---

20. Legal and Technological Accountability

Responsibility should be clearly allocated among the participants operating a blockchain evidence system.

Relevant actors may include:

- investigators;
- forensic laboratories;
- blockchain administrators;
- technology providers;
- evidence custodians; and
- legal professionals.

Clear procedures should establish who is responsible for collection, hashing, storage, blockchain registration, verification, and presentation.

---

21. Future Applications

Blockchain-based evidence preservation may have applications in several areas.

Intellectual Property

Creators could establish evidence concerning the existence and integrity of digital works.

Financial Transactions

Blockchain records may assist in demonstrating transaction histories.

Electronic Contracts

Cryptographic records may help establish document integrity.

Digital Forensics

Blockchain may provide additional verification of forensic evidence.

Government Records

Selected digital records may potentially benefit from tamper-evident preservation.

---

22. Limitations

Blockchain technology should not be viewed as a universal solution.

Important limitations include:

- technical complexity;
- privacy concerns;
- implementation costs;
- dependence on reliable data entry;
- identity-management challenges;
- interoperability problems; and
- uncertainty concerning legal treatment in different jurisdictions.

The technology should therefore be adopted selectively according to evidentiary requirements.

---

23. Conclusion

Blockchain technology offers a promising mechanism for strengthening the integrity and traceability of digital evidence.

Cryptographic hashes, timestamps, distributed verification, and digital signatures can provide useful technological safeguards against undetected alteration.

However, blockchain should not be confused with a complete evidentiary solution.

A blockchain record can demonstrate that particular information was registered and subsequently remained consistent with the recorded cryptographic value. It does not necessarily establish that the information was truthful when originally entered, nor does it automatically prove the identity or intention of the person responsible for the information.

Therefore, blockchain should complement established principles of evidence law and digital forensics rather than replace them.

A reliable framework should combine lawful collection, forensic preservation, cryptographic verification, secure storage, documented chain of custody, appropriate identity authentication, expert explanation, and judicial assessment.

The future of digital evidence will increasingly involve cooperation between law and technology. Blockchain can contribute significantly to this process, particularly where authenticity and integrity are central concerns. Its greatest legal value may ultimately lie not in making digital evidence automatically admissible, but in providing a stronger technological foundation through which courts can evaluate whether digital information has remained authentic, identifiable, and intact.

Declarations

Conflict of interest: The authors declare that they have no conflict of interest.

Funding: This review received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Ethical approval: Not applicable. This article is a review of published literature and did not involve human participants or animal subjects.

Data availability: No new data were generated or analyzed in support of this review. All sources relied upon are cited in the References.

Use of AI tools: No generative artificial intelligence tool was used in the conception, drafting or analysis of this article. The authors take full responsibility for the content.

Author contributions: Author contributed to the conception of the review, the survey of the literature, and the drafting and revision of the manuscript. Author read and approved the final version.