JOURNAL OF LAW, INFORMATION & SCIENCE
ISSN 0729-1485• Vol. 4, Issue 1 (2026) • https://jlisjournal.com/

REVIEW ARTICLE Article ID: JLIS/2026/4/1/011

Blockchain-Based Digital Evidence: Technological Transformation of Evidence Management in the Modern Justice System

Dr. Nethmi Perera [1], Dr. Nethmi Perera [2]

[1] *Faculty of Law and Technology, University of Colombo, Colombo, Sri Lanka*
[2] *Centre for Digital Evidence and Cybersecurity, Indian Institute of Legal Technology, Bengaluru, India*

Received: 18 Nov 2025 **Revised:** 28 Feb 2026 **Accepted:** 28 March 2025 **Published:** 29 April 2026

ABSTRACT

The rapid digitization of legal and judicial processes has resulted in the increasing use of electronic records as evidence. However, ensuring the authenticity, integrity, and traceability of digital evidence remains a significant technological challenge. Blockchain technology, through its distributed architecture, cryptographic verification, and tamper-resistant recordkeeping, offers a potential mechanism for strengthening digital evidence management. This article examines the application of blockchain technology in the collection, preservation, verification, transfer, and storage of digital evidence. It explores how blockchain-based systems can create a transparent and verifiable record of evidence handling while reducing the risk of unauthorized modification. The article further examines the integration of blockchain with digital forensic systems, cloud storage, electronic records, and judicial evidence-management platforms. Particular attention is given to chain of custody, cryptographic hashing, access control, timestamping, interoperability, scalability, and privacy. The study proposes a blockchain-enabled evidence-management framework in which every significant interaction with digital evidence is securely recorded. The article concludes that blockchain can strengthen technological reliability and accountability in evidence management, although technical limitations, privacy concerns, interoperability issues, and implementation costs require careful consideration.

Keywords: *Blockchain; Digital Evidence; Chain of Custody; Digital Forensics; Evidence Management; Cryptographic Hashing; Judicial Technology.*

1. Introduction

The digital transformation of society has fundamentally changed the nature of information used in legal proceedings. Emails, electronic documents, CCTV recordings, smartphone data, cloud records, social-media communications, digital photographs, videos, and blockchain transactions are increasingly relevant to investigations and litigation.

Unlike traditional physical evidence, digital evidence can be copied, transmitted, modified, deleted, or manipulated with relative ease. Consequently, demonstrating that digital evidence

has remained unchanged from the time of collection to the time of presentation has become an important technological challenge.

Traditional chain-of-custody mechanisms depend heavily upon human documentation. Investigators record who collected the evidence, when it was collected, where it was stored, and who subsequently accessed it. Although such procedures can be effective, manual records may themselves be incomplete, altered, or incorrectly maintained.

Blockchain technology provides a potential technological solution. By recording cryptographically verifiable information concerning evidence handling on a distributed ledger, blockchain can create a transparent and tamper-resistant history of digital evidence.

This article examines how blockchain technology can be integrated into digital evidence-management systems and evaluates its potential benefits, limitations, and future applications.

2. Digital Evidence in the Modern Justice System

Digital evidence refers to information stored or transmitted in digital form that may be relevant to a legal investigation or proceeding.

It can originate from numerous sources, including:

- computers;
- smartphones;
- surveillance cameras;
- cloud platforms;
- email systems;
- social-media applications;
- GPS devices;
- IoT systems;
- financial platforms; and
- blockchain networks.

The increasing number of digital sources creates both opportunities and challenges.

Investigators may obtain large amounts of information, but determining whether that information is authentic and has remained unaltered can be difficult.

Evidence-management systems must therefore provide mechanisms for integrity verification, controlled access, and reliable documentation.

3. Blockchain Technology

Blockchain is a distributed ledger technology that records transactions or other information across a network.

Depending on the architecture, blockchain records can be cryptographically linked, making unauthorized alteration detectable or technically difficult.

Three characteristics are particularly relevant to digital evidence:

Immutability: Previously recorded information can be resistant to unauthorized modification.

Timestamping: Transactions can provide a chronological record of when information was recorded.

Traceability: Subsequent interactions with the system can be documented and verified.

These characteristics make blockchain potentially suitable for maintaining evidence-management records.

However, blockchain does not automatically guarantee that the original evidence is genuine. It primarily helps establish what information was recorded and whether the blockchain record itself has subsequently been altered.

---

4. Blockchain and Chain of Custody

Chain of custody is a fundamental concept in evidence management.

It represents the documented history of an item of evidence from its initial collection to its presentation or final disposition.

In a traditional system, an investigator may manually record:

1. evidence collection;
2. transfer to forensic personnel;
3. forensic examination;
4. storage;
5. transfer to another authority; and
6. presentation before a court.

A blockchain-based system could digitally record each of these events.

For example:

Evidence Collected → Hash Generated → Blockchain Record Created → Forensic Examination → Transfer → Storage → Court Presentation

Each event can be associated with a timestamp and authorized digital identity.

This can create a verifiable chronological record of evidence handling.

---

5. Cryptographic Hashing

Cryptographic hashing is particularly important in blockchain-based evidence management.

A hash function converts digital information into a fixed-length output commonly referred to as a hash value.

If the underlying file changes, its hash value will generally also change.

Investigators can therefore calculate a hash of a digital evidence file at the time of acquisition and record that hash within the blockchain.

When the evidence is later examined, the hash can be recalculated.

If the values correspond, this provides evidence that the examined file is consistent with the recorded version.

Blockchain can therefore function as a trusted record for evidence-integrity verification.

---

6. Evidence Acquisition

The first stage of digital evidence management is acquisition.

Evidence may be acquired from computers, smartphones, servers, cloud systems, or other digital devices.

At acquisition, investigators should document relevant information concerning:

- source device;
- acquisition time;
- investigator identity;
- acquisition method;
- file characteristics;
- cryptographic hash; and
- storage location.

A blockchain system can record selected metadata and the hash value without necessarily storing the complete evidence file on the blockchain.

This distinction is important because storing large files directly on a blockchain may create scalability and storage problems.

---

7. Off-Chain and On-Chain Storage

A practical blockchain evidence system should generally distinguish between **evidence storage** and **evidence verification**.

The actual digital evidence can be stored in a secure forensic repository or encrypted cloud environment.

The blockchain can store:

- evidence identifier;
- cryptographic hash;
- timestamp;
- authorized user;
- transaction history; and
- relevant metadata.

This creates a hybrid architecture:

Digital Evidence → Secure Storage

and

Evidence Hash + Metadata → Blockchain Ledger

When evidence is subsequently accessed, its hash can be compared with the blockchain record.

This approach can reduce blockchain storage requirements while retaining verification capabilities.

---

8. Access Control

Evidence repositories may contain highly sensitive information. Unauthorized access could compromise investigations or violate privacy.

Blockchain systems can be integrated with identity and access-control mechanisms.

Different users may receive different permissions.

For example:

- investigators may collect evidence;
- forensic experts may analyze evidence;
- administrators may manage storage;
- prosecutors may review selected information; and
- judicial authorities may access relevant records.

Role-based access control can reduce unauthorized activity.

Every authorized interaction can also be recorded for future auditing.

---

9. Blockchain-Based Timestamping

Establishing when digital evidence existed in a particular form can be important.

Blockchain-based timestamping can provide a chronological record of when a hash or metadata record was added to the ledger.

For example, an investigator may generate the hash of a CCTV file immediately after collection and record that hash in the blockchain.

A later party can verify that the same hash was recorded at a particular point in the evidence-management process.

This can strengthen the technical documentation surrounding digital evidence.

---

10. Digital Forensics and Blockchain

Blockchain can complement rather than replace digital-forensic techniques.

Digital forensic experts may still need to examine the underlying evidence, recover deleted information, analyze metadata, reconstruct timelines, and identify signs of manipulation.

Blockchain provides an additional layer of integrity verification.

A complete forensic process could therefore involve:

Acquisition → Forensic Imaging → Hash Generation → Blockchain Registration → Examination → Analysis → Verification

This integration can improve traceability throughout the forensic lifecycle.

---

11. Cloud-Based Evidence

Cloud computing has made evidence acquisition more complicated because information may be distributed across multiple servers and locations.

A blockchain-enabled evidence system can record information concerning the acquisition and subsequent handling of cloud-based evidence.

For example, when evidence is obtained from a cloud platform, its hash and acquisition metadata can be registered.

If the evidence is subsequently transferred between investigators or forensic laboratories, each transfer can be recorded.

This can create a transparent history despite the distributed nature of the original evidence.

---

12. Mobile Evidence

Smartphones contain large quantities of potentially relevant information.

Messages, photographs, application data, location records, browser information, and device logs can all become relevant to investigations.

Mobile evidence may also change automatically because applications continuously update information.

Blockchain-based timestamping and hash registration can therefore provide useful integrity records immediately following forensic acquisition.

However, the blockchain should not be viewed as a substitute for proper forensic acquisition procedures.

---

13. Artificial Intelligence Integration

Blockchain-based evidence systems can potentially be combined with artificial intelligence.

AI may assist in:

- evidence classification;
- duplicate detection;
- document analysis;
- anomaly detection;
- metadata analysis;
- timeline reconstruction; and
- prioritization of relevant files.

Blockchain can then record the integrity-related information associated with AI-assisted processing.

This combination creates a potential technological architecture:

Digital Evidence → AI Analysis → Forensic Verification → Blockchain Recording

However, AI-generated findings should remain subject to human verification because automated systems may produce errors.

---

14. Privacy Challenges

Although blockchain can improve transparency, excessive transparency may create privacy concerns.

A blockchain record may remain available for an extended period depending on the network architecture.

Sensitive information should therefore not automatically be placed directly on a public blockchain.

A privacy-conscious architecture can store only minimal information on-chain, such as cryptographic hashes and non-sensitive identifiers.

Actual evidence can remain within controlled and encrypted storage systems.

Permissioned blockchain networks may also be more appropriate for judicial evidence management than unrestricted public networks.

15. Security Considerations

A blockchain evidence-management system itself must be secure.

Potential risks include:

- compromised user credentials;
- malicious administrators;
- smart-contract vulnerabilities;
- endpoint compromise;
- unauthorized access;
- incorrect data entry; and
- attacks against connected storage systems.

Blockchain provides integrity to recorded information, but it does not automatically protect the entire technological ecosystem.

Security must therefore be implemented across devices, networks, applications, identity systems, and storage infrastructure.

16. Smart Contracts in Evidence Management

Smart contracts can automate certain evidence-management processes.

For example, a smart contract could automatically record that evidence has been transferred from one authorized investigator to another.

It could also enforce predefined access conditions.

A simplified process could be:

Evidence Transfer Request → Identity Verification → Permission Check → Evidence Access → Blockchain Record

This can reduce manual administrative work.

However, smart contracts must be carefully designed because programming errors may affect automated operations.

17. Interoperability Challenges

Different law-enforcement agencies and forensic laboratories may use different evidence-management platforms.

A blockchain solution must therefore support interoperability.

The system should be capable of communicating with:

- forensic tools;

- case-management systems;
- cloud platforms;
- evidence repositories;
- identity-management systems; and
- judicial information systems.

Without interoperability, blockchain may create another isolated technological environment rather than improving the overall evidence-management ecosystem.

---

18. Proposed Blockchain-Based Evidence Framework

A practical framework can be divided into five layers.

Layer 1: Evidence Collection

Investigators acquire digital evidence using validated forensic procedures.

Layer 2: Evidence Processing

The evidence is examined and a cryptographic hash is generated.

Layer 3: Secure Storage

The original evidence is stored in an encrypted forensic repository.

Layer 4: Blockchain Verification

The evidence identifier, hash, timestamp, and selected metadata are recorded on a permissioned blockchain.

Layer 5: Judicial Verification

Authorized users can verify whether the presented evidence corresponds to the originally registered digital record.

This architecture separates evidence storage from evidence-integrity verification.

---

19. Advantages of Blockchain-Based Evidence Management

The proposed approach may provide several benefits.

Enhanced Integrity

Changes to evidence can potentially be detected through hash comparison.

Improved Traceability

Evidence transfers and interactions can be systematically recorded.

Reduced Dependence on Manual Records

Blockchain can automate certain aspects of evidence documentation.

Greater Transparency

Authorized participants can independently verify relevant blockchain records.

Better Auditability

Investigators and institutions can review the history of evidence handling.

Increased Efficiency

Automated workflows may reduce administrative burdens.

These benefits, however, depend on correct system implementation.

---

20. Limitations

Blockchain is not a universal solution to digital evidence problems.

The technology cannot determine whether the original evidence was truthful or whether a recording accurately represents an event.

It can primarily help establish the integrity and history of a digital record.

Other limitations include:

- implementation costs;
- scalability;
- interoperability;
- privacy concerns;
- technical complexity;
- blockchain governance; and
- dependence on secure input systems.

The principle of **"garbage in, garbage out"** remains relevant. If false or manipulated evidence is registered initially, blockchain cannot automatically transform it into authentic evidence.

---

21. Future Directions

Future research can explore the integration of blockchain with advanced digital-forensic technologies.

Potential developments include AI-assisted evidence verification, decentralized identity systems, secure hardware-based evidence acquisition, automated chain-of-custody management, and privacy-preserving blockchain architectures.

Zero-knowledge technologies may also provide mechanisms for verifying certain claims without unnecessarily exposing sensitive information.

Interoperable standards could allow different forensic laboratories and judicial institutions to exchange verification information more efficiently.

The combination of blockchain, AI, cloud computing, and digital forensics could therefore create increasingly sophisticated evidence-management ecosystems.

22. Conclusion

The growing importance of digital evidence has created an urgent need for reliable technological mechanisms capable of preserving evidence integrity and documenting its history.

Blockchain technology offers a promising approach because its cryptographic structure, timestamping capabilities, distributed architecture, and traceability can strengthen the technological foundations of chain-of-custody management.

A practical system should not attempt to store all evidence directly on the blockchain. Instead, original evidence can remain in secure forensic repositories while cryptographic hashes and selected metadata are recorded on a permissioned blockchain.

Such an architecture can provide an additional layer of verification without unnecessarily exposing sensitive information.

Nevertheless, blockchain cannot independently establish the truthfulness of evidence. It can help demonstrate that a particular digital record corresponds to a previously registered record, but the authenticity and evidentiary value of the underlying material must still be assessed through appropriate forensic and legal procedures.

The future of digital evidence management is therefore likely to involve the integration of blockchain with digital forensics, artificial intelligence, secure cloud storage, cryptographic technologies, and judicial information systems.

When appropriately designed, blockchain can transform evidence management from a predominantly manual documentation process into a more automated, traceable, and technologically verifiable system. Its successful implementation, however, will depend upon careful attention to privacy, cybersecurity, interoperability, scalability, and institutional governance.

1. Introduction

The digital transformation of society has fundamentally changed the nature of information used in legal proceedings. Emails, electronic documents, CCTV recordings, smartphone data, cloud records, social-media communications, digital photographs, videos, and blockchain transactions are increasingly relevant to investigations and litigation.

Unlike traditional physical evidence, digital evidence can be copied, transmitted, modified, deleted, or manipulated with relative ease. Consequently, demonstrating that digital evidence has remained unchanged from the time of collection to the time of presentation has become an important technological challenge.

Traditional chain-of-custody mechanisms depend heavily upon human documentation. Investigators record who collected the evidence, when it was collected, where it was stored, and who subsequently accessed it. Although such procedures can be effective, manual records may themselves be incomplete, altered, or incorrectly maintained.

Blockchain technology provides a potential technological solution. By recording cryptographically verifiable information concerning evidence handling on a distributed ledger, blockchain can create a transparent and tamper-resistant history of digital evidence.

This article examines how blockchain technology can be integrated into digital evidence-management systems and evaluates its potential benefits, limitations, and future applications.

2. Digital Evidence in the Modern Justice System

Digital evidence refers to information stored or transmitted in digital form that may be relevant to a legal investigation or proceeding.

It can originate from numerous sources, including:

- computers;
- smartphones;
- surveillance cameras;
- cloud platforms;
- email systems;
- social-media applications;
- GPS devices;
- IoT systems;
- financial platforms; and
- blockchain networks.

The increasing number of digital sources creates both opportunities and challenges.

Investigators may obtain large amounts of information, but determining whether that information is authentic and has remained unaltered can be difficult.

Evidence-management systems must therefore provide mechanisms for integrity verification, controlled access, and reliable documentation.

3. Blockchain Technology

Blockchain is a distributed ledger technology that records transactions or other information across a network.

Depending on the architecture, blockchain records can be cryptographically linked, making unauthorized alteration detectable or technically difficult.

Three characteristics are particularly relevant to digital evidence:

Immutability: Previously recorded information can be resistant to unauthorized modification.

Timestamping: Transactions can provide a chronological record of when information was recorded.

Traceability: Subsequent interactions with the system can be documented and verified.

These characteristics make blockchain potentially suitable for maintaining evidence-management records.

However, blockchain does not automatically guarantee that the original evidence is genuine. It primarily helps establish what information was recorded and whether the blockchain record itself has subsequently been altered.

---

4. Blockchain and Chain of Custody

Chain of custody is a fundamental concept in evidence management.

It represents the documented history of an item of evidence from its initial collection to its presentation or final disposition.

In a traditional system, an investigator may manually record:

1. evidence collection;
2. transfer to forensic personnel;
3. forensic examination;
4. storage;
5. transfer to another authority; and
6. presentation before a court.

A blockchain-based system could digitally record each of these events.

For example:

Evidence Collected → Hash Generated → Blockchain Record Created → Forensic Examination → Transfer → Storage → Court Presentation

Each event can be associated with a timestamp and authorized digital identity.

This can create a verifiable chronological record of evidence handling.

---

5. Cryptographic Hashing

Cryptographic hashing is particularly important in blockchain-based evidence management.

A hash function converts digital information into a fixed-length output commonly referred to as a hash value.

If the underlying file changes, its hash value will generally also change.

Investigators can therefore calculate a hash of a digital evidence file at the time of acquisition and record that hash within the blockchain.

When the evidence is later examined, the hash can be recalculated.

If the values correspond, this provides evidence that the examined file is consistent with the recorded version.

Blockchain can therefore function as a trusted record for evidence-integrity verification.

---

6. Evidence Acquisition

The first stage of digital evidence management is acquisition.

Evidence may be acquired from computers, smartphones, servers, cloud systems, or other digital devices.

At acquisition, investigators should document relevant information concerning:

- source device;
- acquisition time;
- investigator identity;
- acquisition method;
- file characteristics;
- cryptographic hash; and
- storage location.

A blockchain system can record selected metadata and the hash value without necessarily storing the complete evidence file on the blockchain.

This distinction is important because storing large files directly on a blockchain may create scalability and storage problems.

---

7. Off-Chain and On-Chain Storage

A practical blockchain evidence system should generally distinguish between **evidence storage** and **evidence verification**.

The actual digital evidence can be stored in a secure forensic repository or encrypted cloud environment.

The blockchain can store:

- evidence identifier;

- cryptographic hash;
- timestamp;
- authorized user;
- transaction history; and
- relevant metadata.

This creates a hybrid architecture:

Digital Evidence → Secure Storage

and

Evidence Hash + Metadata → Blockchain Ledger

When evidence is subsequently accessed, its hash can be compared with the blockchain record.

This approach can reduce blockchain storage requirements while retaining verification capabilities.

---

8. Access Control

Evidence repositories may contain highly sensitive information. Unauthorized access could compromise investigations or violate privacy.

Blockchain systems can be integrated with identity and access-control mechanisms.

Different users may receive different permissions.

For example:

- investigators may collect evidence;
- forensic experts may analyze evidence;
- administrators may manage storage;
- prosecutors may review selected information; and
- judicial authorities may access relevant records.

Role-based access control can reduce unauthorized activity.

Every authorized interaction can also be recorded for future auditing.

---

9. Blockchain-Based Timestamping

Establishing when digital evidence existed in a particular form can be important.

Blockchain-based timestamping can provide a chronological record of when a hash or metadata record was added to the ledger.

For example, an investigator may generate the hash of a CCTV file immediately after collection and record that hash in the blockchain.

A later party can verify that the same hash was recorded at a particular point in the evidence-management process.

This can strengthen the technical documentation surrounding digital evidence.

---

10. Digital Forensics and Blockchain

Blockchain can complement rather than replace digital-forensic techniques.

Digital forensic experts may still need to examine the underlying evidence, recover deleted information, analyze metadata, reconstruct timelines, and identify signs of manipulation.

Blockchain provides an additional layer of integrity verification.

A complete forensic process could therefore involve:

Acquisition → Forensic Imaging → Hash Generation → Blockchain Registration → Examination → Analysis → Verification

This integration can improve traceability throughout the forensic lifecycle.

---

11. Cloud-Based Evidence

Cloud computing has made evidence acquisition more complicated because information may be distributed across multiple servers and locations.

A blockchain-enabled evidence system can record information concerning the acquisition and subsequent handling of cloud-based evidence.

For example, when evidence is obtained from a cloud platform, its hash and acquisition metadata can be registered.

If the evidence is subsequently transferred between investigators or forensic laboratories, each transfer can be recorded.

This can create a transparent history despite the distributed nature of the original evidence.

---

12. Mobile Evidence

Smartphones contain large quantities of potentially relevant information.

Messages, photographs, application data, location records, browser information, and device logs can all become relevant to investigations.

Mobile evidence may also change automatically because applications continuously update information.

Blockchain-based timestamping and hash registration can therefore provide useful integrity records immediately following forensic acquisition.

However, the blockchain should not be viewed as a substitute for proper forensic acquisition procedures.

---

13. Artificial Intelligence Integration

Blockchain-based evidence systems can potentially be combined with artificial intelligence.

AI may assist in:

- evidence classification;
- duplicate detection;
- document analysis;
- anomaly detection;
- metadata analysis;
- timeline reconstruction; and
- prioritization of relevant files.

Blockchain can then record the integrity-related information associated with AI-assisted processing.

This combination creates a potential technological architecture:

Digital Evidence → AI Analysis → Forensic Verification → Blockchain Recording

However, AI-generated findings should remain subject to human verification because automated systems may produce errors.

---

14. Privacy Challenges

Although blockchain can improve transparency, excessive transparency may create privacy concerns.

A blockchain record may remain available for an extended period depending on the network architecture.

Sensitive information should therefore not automatically be placed directly on a public blockchain.

A privacy-conscious architecture can store only minimal information on-chain, such as cryptographic hashes and non-sensitive identifiers.

Actual evidence can remain within controlled and encrypted storage systems.

Permissioned blockchain networks may also be more appropriate for judicial evidence management than unrestricted public networks.

---

15. Security Considerations

A blockchain evidence-management system itself must be secure.

Potential risks include:

- compromised user credentials;
- malicious administrators;
- smart-contract vulnerabilities;
- endpoint compromise;
- unauthorized access;
- incorrect data entry; and
- attacks against connected storage systems.

Blockchain provides integrity to recorded information, but it does not automatically protect the entire technological ecosystem.

Security must therefore be implemented across devices, networks, applications, identity systems, and storage infrastructure.

---

16. Smart Contracts in Evidence Management

Smart contracts can automate certain evidence-management processes.

For example, a smart contract could automatically record that evidence has been transferred from one authorized investigator to another.

It could also enforce predefined access conditions.

A simplified process could be:

Evidence Transfer Request → Identity Verification → Permission Check → Evidence Access → Blockchain Record

This can reduce manual administrative work.

However, smart contracts must be carefully designed because programming errors may affect automated operations.

---

17. Interoperability Challenges

Different law-enforcement agencies and forensic laboratories may use different evidence-management platforms.

A blockchain solution must therefore support interoperability.

The system should be capable of communicating with:

- forensic tools;
- case-management systems;
- cloud platforms;

- evidence repositories;
- identity-management systems; and
- judicial information systems.

Without interoperability, blockchain may create another isolated technological environment rather than improving the overall evidence-management ecosystem.

---

18. Proposed Blockchain-Based Evidence Framework

A practical framework can be divided into five layers.

Layer 1: Evidence Collection

Investigators acquire digital evidence using validated forensic procedures.

Layer 2: Evidence Processing

The evidence is examined and a cryptographic hash is generated.

Layer 3: Secure Storage

The original evidence is stored in an encrypted forensic repository.

Layer 4: Blockchain Verification

The evidence identifier, hash, timestamp, and selected metadata are recorded on a permissioned blockchain.

Layer 5: Judicial Verification

Authorized users can verify whether the presented evidence corresponds to the originally registered digital record.

This architecture separates evidence storage from evidence-integrity verification.

---

19. Advantages of Blockchain-Based Evidence Management

The proposed approach may provide several benefits.

Enhanced Integrity

Changes to evidence can potentially be detected through hash comparison.

Improved Traceability

Evidence transfers and interactions can be systematically recorded.

Reduced Dependence on Manual Records

Blockchain can automate certain aspects of evidence documentation.

Greater Transparency

Authorized participants can independently verify relevant blockchain records.

Better Auditability

Investigators and institutions can review the history of evidence handling.

Increased Efficiency

Automated workflows may reduce administrative burdens.

These benefits, however, depend on correct system implementation.

---

20. Limitations

Blockchain is not a universal solution to digital evidence problems.

The technology cannot determine whether the original evidence was truthful or whether a recording accurately represents an event.

It can primarily help establish the integrity and history of a digital record.

Other limitations include:

- implementation costs;
- scalability;
- interoperability;
- privacy concerns;
- technical complexity;
- blockchain governance; and
- dependence on secure input systems.

The principle of **"garbage in, garbage out"** remains relevant. If false or manipulated evidence is registered initially, blockchain cannot automatically transform it into authentic evidence.

---

21. Future Directions

Future research can explore the integration of blockchain with advanced digital-forensic technologies.

Potential developments include AI-assisted evidence verification, decentralized identity systems, secure hardware-based evidence acquisition, automated chain-of-custody management, and privacy-preserving blockchain architectures.

Zero-knowledge technologies may also provide mechanisms for verifying certain claims without unnecessarily exposing sensitive information.

Interoperable standards could allow different forensic laboratories and judicial institutions to exchange verification information more efficiently.

The combination of blockchain, AI, cloud computing, and digital forensics could therefore create increasingly sophisticated evidence-management ecosystems.

---

22. Conclusion

The growing importance of digital evidence has created an urgent need for reliable technological mechanisms capable of preserving evidence integrity and documenting its history.

Blockchain technology offers a promising approach because its cryptographic structure, timestamping capabilities, distributed architecture, and traceability can strengthen the technological foundations of chain-of-custody management.

A practical system should not attempt to store all evidence directly on the blockchain. Instead, original evidence can remain in secure forensic repositories while cryptographic hashes and selected metadata are recorded on a permissioned blockchain.

Such an architecture can provide an additional layer of verification without unnecessarily exposing sensitive information.

Nevertheless, blockchain cannot independently establish the truthfulness of evidence. It can help demonstrate that a particular digital record corresponds to a previously registered record, but the authenticity and evidentiary value of the underlying material must still be assessed through appropriate forensic and legal procedures.

The future of digital evidence management is therefore likely to involve the integration of blockchain with digital forensics, artificial intelligence, secure cloud storage, cryptographic technologies, and judicial information systems.

When appropriately designed, blockchain can transform evidence management from a predominantly manual documentation process into a more automated, traceable, and technologically verifiable system. Its successful implementation, however, will depend upon careful attention to privacy, cybersecurity, interoperability, scalability, and institutional governance.

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.