FORENSIC - BLOCKCHAIN-BASED EVIDENCE MANAGEMENT AND VERIFICATION SYSTEM

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE AND SUSTAINABLE TECHNOLOGIES
VOL 1 (01), JULY-DECEMBER 2026

Anubhav K. Kesharwani
Department of Information Technology
JSS Academy of Technical Education Noida, India
Email: anubhavkesharwani38gmail.com
Krishna Murari
Department of Information Technology
JSS Academy of Technical Education Noida, India
Email: Krishna.murari@jssaten.ac.in
Amit Kumar
Department of Information Technology
JSS Academy of Technical Education Noida, India
Email: akft6055@gmail.com
Atharv Arya
Department of Information Technology
JSS Academy of Technical Education Noida, India
Email: Atharvaryawork@gmail.com
Atharva Gautam
Department of Information Technology
JSS Academy of Technical Education Noida, India
Email: xitopnotch@gmail.com
Devendra Pratap Singh
Department of Information Technology
JSS Academy of Technical Education Noida, India
Email: Kvdev21@gmail.com

ABSTRACT

The accuracy and reliability of the evidentiary material are of considerable significance in legal investigation and judicial trials. Conventional evidence management systems rely heavily on central database management systems and documentation, which has often been found to result in security breaches, loss of data, and ambiguity in the custody of the evidence. Such problems often lead to arguments over the admissibility of the evidence, and in extreme cases, miscarriages of justice. This study proposes a Blockchain-Based Evidence Management and Verification System, which would address the problems of conventional systems by leveraging the benefits of blockchain technology. The proposed system will store the cryptographic hashes of the digital evidence on the blockchain, while the actual digital files will be stored in decentralized storage. Smart contracts will also be used to create automated verification processes that ensure security, access control, and audit trails for all interactions with the digital evidence. Therefore, it will be ensured that all interactions with the digital evidence are timestamped and recorded to detect any changes to the digital evidence. As illustrated by the preceding experimental results, the integrity of digital evidence can be ensured, traceability can be increased, and trust can be established between all stakeholders in the investigation and legal systems.

Keywords— *Blockchain, Digital Evidence, Evidence Management, Chain of Custody, Smart Contracts*

1. INTRODUCTION

In modern legal proceedings and law enforcement practices, the authenticity and integrity of digital evidence are of paramount importance. Evidence such as CCTV footage, digital photographs, forensic reports, or scanned legal documents often serves as a cornerstone in proving or disproving claims in courts of law. Evidence is the cornerstone of criminal proceedings and guarantees the quality of case handling **[1].** However, traditional evidence management systems are still heavily dependent on centralized databases or manual handling methods. Such systems suffer from major drawbacks including vulnerability to tampering, unauthorized access, data breaches, accidental loss, and limited transparency in

the chain of custody. Blockchain technology has revolutionized various industries by providing a decentralized and immutable ledger system **[2]**. Blockchain technology has emerged as a disruptive innovation, providing a decentralized and transparent environment across various domains. Blockchain can be understood as a distributed ledger technology that enables secure and immutable record-keeping of digital transactions **[3]**. These shortcomings not only compromise the credibility and admissibility of evidence in court but also undermine public confidence in the judicial system.

With the rising adoption of digital media in investigations, these limitations have become more pressing. A single instance of tampering or mishandling of evidence can lead to miscarriage of justice, wrongful convictions, or the acquittal of guilty parties. Hence, there is a strong need for a reliable, secure, and tamper- proof system that can safeguard digital evidence from the moment of collection until its presentation in court.

To address these challenges, our project proposes the development of a Blockchain-Based Evidence Management and Verification System. Blockchain, by its very nature, provides immutability, transparency, and decentralization. By leveraging Ethereum smart contracts, decentralized storage through the Inter Planetary File System (IPFS), and cryptographic SHA-256 hashing, our system ensures that once evidence is uploaded, it cannot be altered or deleted without detection.

The system is designed with role-based access control, allowing police officers, court officials, and administrators to perform functions according to their authorization levels. Police officers can securely upload digital evidence along with metadata such as case ID, timestamp, 4 and officer details. Court officials can verify the authenticity of submitted files by cross-checking their cryptographic hashes with blockchain records.

A blockchain-enabled chain-of-custody concept designed especially for legal and law enforcement organisations is presented by Tesma **[4]**. Basically, the problem in digital evidence are authentication and chain of custody (CoC) **[5]**. Digital Chain of Custody is a procedure to handle digital evidence in investigations. It is used to maintain and document digital evidence in chronological order right from when the incident took place until it is presented to the court. In this process, it goes through different levels of hierarchy right from the first evidence collector to the higher authority court. By utilizing smart contracts written in Solidity, it becomes feasible to establish and efficiently manage the digital evidences in chain of custody **[6]. [7]** Proof of Work (PoW) Consensus Mechanism. PoW was introduced by the Bitcoin blockchain technology. PoW assumes that each peer uses computing power to solve the proof of work in stances and construct the appropriate blocks for voting.

Over the past few years, businesses across various sectors have increasingly invested in blockchain technology, recognizing its transformative potential. The market for blockchain technology is increasing exponentially. In 2022, the worldwide market for blockchain technology was estimated at USD 11.14 billion. It is anticipated to expand from USD 17.57 billion in 2023 to USD 469.49 billion by 2030, demonstrating a Compound Annual Growth Rate (CAGR) of 59.9 percent throughout the forecast period. In terms of market share, North America was the leading region in 2022, holding 47.13 percent of the global market **[8]**.

2. RELATED WORK

Satoshi Nakamoto is the name of an individual or group of individuals who have been credited for the innovation of the Blockchain Technology in the year 2008. We take inspiration from Satoshi Nakamoto's pioneering work for securing Electronic cash transactions using blockchain. We intend to implement a similar framework for securing the Chain of Custody for Digital Evidence Management. Blockchain is a decentralized, trustworthy distributed ledger on a peer-to-peer network that consists of a list of chronologically ordered blocks **[9]**. Peer-to-peer (P2P) networking, which permits decentralized communication between nodes, is a fundamental component of this project **[2]**. This survey analyzed the benefits and challenges of blockchain in digital forensics. It provided conceptual insights but no implementation. We contributed a working system based on those insights **[13]**. There is an increasing interest in the academic community in the application of blockchain technology in the management of evidence and digital forensic activities, owing to the persisting concerns about the trustworthiness, transparency, and reliability of the current processes. Digital Forensics (DF) is defined as the method that includes identifying, investigating, preserving, analyzing, validating and presenting digital evidence in a way that is

traditionally permitted by the law in any legal proceedings i.e. the Court of Law **[9]**. A considerable percentage of the studies have concentrated on the application of blockchain technology in the maintenance of the integrity of the evidence custody chain. The system improved blockchain scalability using sharding and stored data in IPFS to reduce storage costs. Deployment complexity was high. We adopted an IPFS-inspired approach while maintaining simplicity**[11]**. In the past, the main focus of the studies has been the management of evidence files by hashing and then recording the files on the blockchain. This has provided low storage requirements and the ability to validate the integrity of the files at any stage of the investigation. Most of the studies have concentrated on the non- repudiation and traceability capabilities of blockchain technology, which are important for the admissibility of the evidence. There is ongoing research on the use of blockchain in log management to facilitate forensic analysis. The concept is that by using a blockchain, investigators and analysts would be made more accountable for the handling of evidence. The problem with many such studies, however, is that they often involve the use of public blockchains, which creates issues with respect to privacy and access when thinking about law enforcement. There is also ongoing research on the use of permissioned blockchain systems, such as Hyperledger Fabric and Cryptographic hashing ensures that once information is entered, any attempt to change it would leave a visible trace, preserving the integrity of the evidence **[12]** in forensic data. This system uses role-based access control and allows investigators to grant permissions when needed. While it provides better privacy, it also introduces implementation complexities.

B-DEC: Digital Evidence Cabinet based on Blockchain for Evidence Management This paper introduces the Blockchain Digital Evidence Cabinet (B-DEC), which combines the Digital Evidence Bag (DEB) concept with Ethereum-based smart contracts. The system ensures integrity and authenticity of digital evidence by recording chain-of-custody documents on blockchain. It follows forensic standards such as ISO/IEC 27037 and emphasizes proper documentation throughout the forensic lifecycle **[5]**.

Several studies extended the applicability of blockchain technology by incorporating smart contracts into the validation and transfer of custody of the evidence. Smart contracts can assist in reducing the number of steps and defining rules for accessing the evidence. However, several studies indicate difficulties that can occur with the performance of the system, especially with large volumes of metadata or high-frequency transactions. Other studies explored the possibility of combining blockchain technology with decentralized storage. This means that the actual files of the evidence are not stored on the blockchain, but instead, they are stored on a decentralized file system.

New research points to the potential of blockchain in helping to significantly enhance the security of digital evidence. However, most of the solutions proposed only address one part of the equation—be it security or access control—leaving the other part unaddressed. What we require is a solution that not only provides security but also addresses the issue in a more comprehensive manner. It must not only store digital evidence securely, authenticate it, but also prove the presence of all the required features in the system. Smart contracts, as well as blockchain, can help in achieving this.

Figure 1: Features Importance Chart

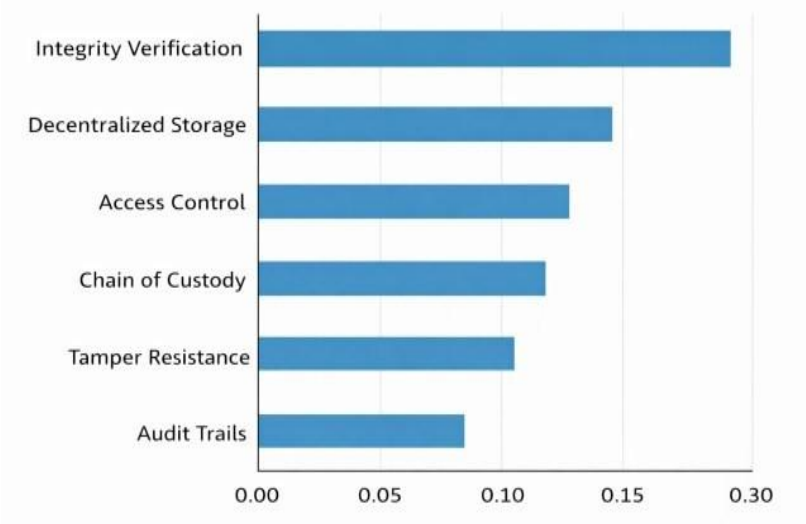
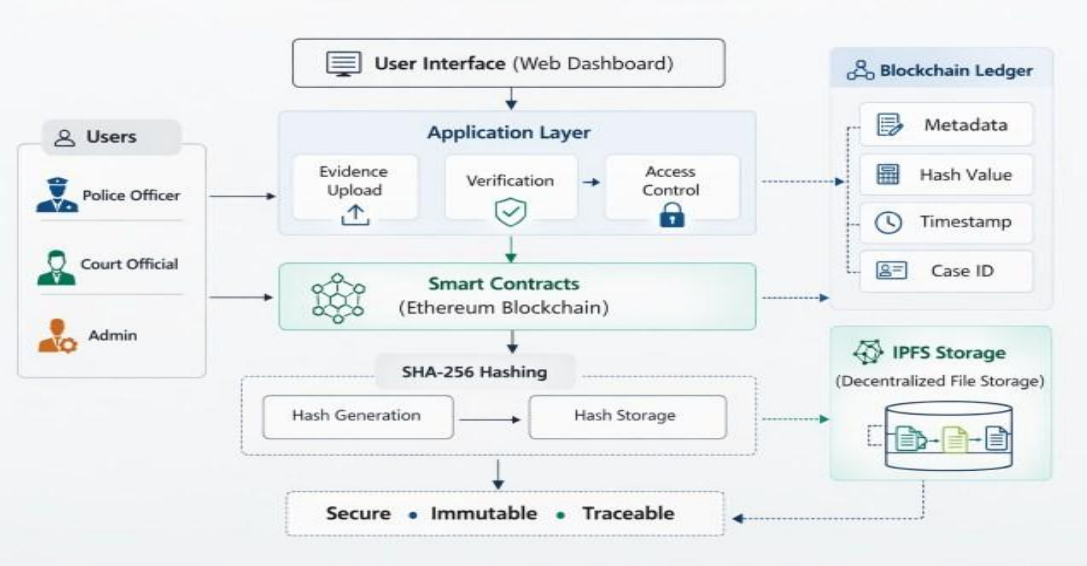


Figure 2 System Architecture diagram



3. METHODOLOGY

The proposed Blockchain-Based Evidence Management and Verification System attempt to provide a secure, transparent, and tamper-resistant system for the management of digital evidence. The system attempts to address the limitations and disadvantages associated with traditional centralized evidence management processes by utilizing the advantages associated with decentralized evidence management processes.

System Overview

The system utilizes a hybrid model that combines blockchain technology with decentralized file storage. Direct storage of digital evidence files on the blockchain is not preferred due to storage capacity considerations. In this context, the hash function, as a cryptographic primitive, is used to generate a hash value for the evidentiary documents. Subsequently, the generated hash value along with other relevant metadata such as the case ID, timestamp, and uploader identity is stored on the blockchain. The actual evidence files are stored using a decentralized storage model to reduce the storage overhead. Changes to the evidence files are detected through a mismatch in the hash value.

System Architecture

The architecture of the Blockchain-Based Evidence Management and Verification System is designed to provide a secure, transparent, and tamper-proof environment for handling digital evidence. It integrates blockchain, IPFS decentralized storage, smart contracts, hashing functions, and a role-based access control mechanism.

The architecture of the proposed system consists of six primary layers:

User Interface Layer:

This layer provides a web interface for authorized users, which include investigators, administrators, and judicial authorities. Users can upload evidence, check the authenticity of the evidence, and view the transaction history.

Application Layer:

The application layer manages all the logical aspects of the system related to the submission of evidence, verification of evidence, and validation of access. The application layer acts as a mediator between the user interface and the blockchain.

Blockchain Layer:

The blockchain layer manages all the immutable transactions related to the management of the evidence. Smart contracts in the blockchain define all the rules related to the management of the evidence.

Decentralized Storage Layer:

The decentralized storage layer stores the actual evidence in a decentralized manner. The blockchain stores only the cryptographic representations of the actual evidence.

Cryptographic Hashing Module

Cryptographic hash functions are mathematical algorithms that transform input data into a fixed-length sequence of characters, referred to as a hash value. Cryptographic hash functions are intended to be fast, deterministic, and one-way, meaning that even a minor change in input yields a very different hash.

Authentication and Role-Based Access Control

Role-Based Access Control (RBAC) is a security model that authorizes end-user access to systems, applications, and data based on predefined roles. For example, a security analyst can configure a firewall but cannot view customer data, while a sales representative can access customer accounts but not the firewall settings.

Methodology

The methodology outlines the step-by-step process followed by the system from evidence submission to verification:

Evidence Collection & Upload Phase

- **User Authentication:** Police officers log into the system using secure credentials (JWT/Web3 authentication).
- **Metadata Entry:** Officer enters details such as Case ID, evidence type, timestamp, and officer ID.
- **Hash Generation:** The system generates a **SHA-256 hash** of the evidence file. This hash serves as a digital fingerprint.
- **Store File on IPFS:** Evidence is uploaded to IPFS, which returns a CID (Content Identifier).This CID changes if the file is altered, ensuring tamper detection.
- **Record Metadata on Blockchain:** The smart contract stores, Evidence hash, IPFS CID, Timestamp, Case ID, Uploaded by (Officer address). This makes the evidence entry immutable and publicly verifiable.

Evidence Storage & Management Phase

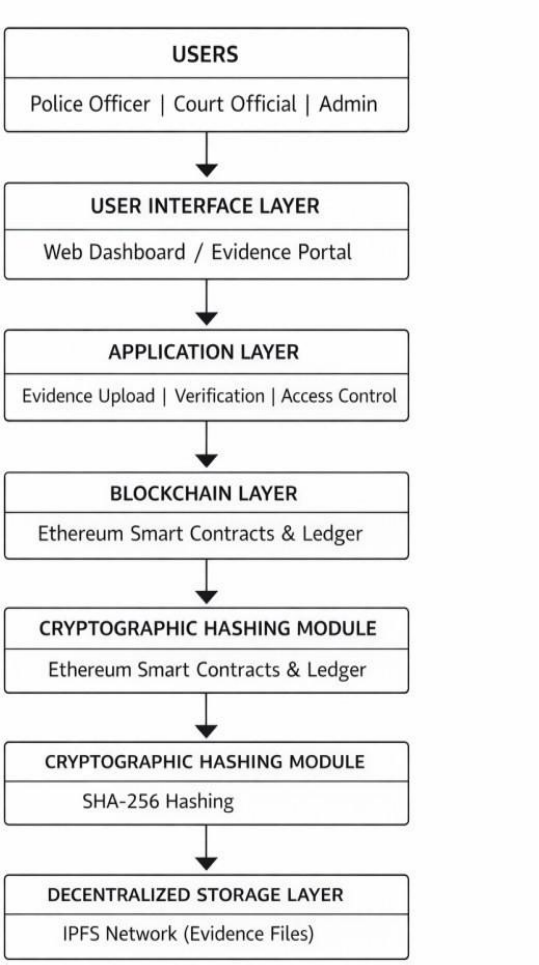
- **Decentralized Storage (IPFS):** The evidence file is stored across distributed nodes, preventing data loss or unauthorized modification.
- **Blockchain Ledger (Ethereum):**Stores metadata in an append-only format. No entity can modify or delete previous records.
- **Role-Based Access Control:** Smart contracts and backend checks enforce access restrictions:
  - Police → Upload
  - Court officials → Verify
  - Admin → Monitor & manage accounts

Evidence Verification Phase

- **Upload File for Verification:** Court officials upload the received file.
- **Re-Hashing Process:** The system generates a fresh **SHA-256 hash** of the uploaded file.
- **Hash Comparison:** The newly generated hash is compared with the blockchain-stored hash.
  - If both match → Evidence is authentic.
  - If mismatched → Evidence has been tampered with.

Retrieve Original File via IPFS CID (Optional)
The official can retrieve and compare the original file stored in IPFS. This ensures accuracy, transparency, and legal credibility.

Figure 3 Layer Architecture diagram



4. DISCUSSION & RESULTS

The proposed Blockchain-Based Evidence Management and Verification System has been subject to functional testing and controlled experiments to test the system's efficiency in the maintenance of the integrity, transparency, and traceability of evidence. This includes the accuracy of the evidence, evidence tampering, and access control. The blockchain-based judicial evidence preservation scheme uses FISCO BOCS as the underlying blockchain platform **[15]**.

Evidence Integrity and Verification

An analysis shows that integrity of the evidence is upheld from the time of upload to the system, through to the time of verification. This is done by ensuring that the hash value of the evidence file remains constant throughout from the time of upload. During the verification process, integrity is ensured by comparing the newly generated hash value with the original evidence file.

Chain of Custody Transparency

All activities involving the evidence are recorded in the ledger, thus enhancing traceability, especially compared to tamper-prone databases.

Access Control and Automation

Role-based access control is implemented using smart contracts that limit the interactions between

the evidence and users based on their respective roles. The validation process carried out by the smart contracts minimizes the need for human factors and the associated errors in the process. In moderate workload conditions, the system showed acceptable performance in enforcing the access control rules.

Performance Observations

In the case of standard scenarios concerning the management of evidence, the system functioned properly; however, the increased rate of transactions caused a slight level of latency in the confirmation of the blockchain. This does not refer to the evidence's integrity; rather, it is a scalability-related issue. Furthermore, the use precision of each model.

Forensic Evidence Management System

A The management of forensic evidence represents a critical of modern investigative practices, encapsulating the meticulous handling, documentation, and preservation of evidentiary materials throughout the course of an investigation. At its core, a forensic evidence management system is tasked with safeguarding the integrity and authenticity of evidentiary items, ensuring that they remain unaltered and admissible in legal proceedings. In today's rapidly evolving digital landscape, the challenges associated with forensic evidence management are compounded by the proliferation of digital data and the increasing sophistication of cyber threats. As digital footprints and online profiles become integral components of data, the management of digital forensic evidence takes on added significance, requiring robust systems and protocols to address the unique complexities of digital evidence collection, analysis, and preservation **[10]**. Institutions corresponding to the national police agency, local police agency, cyber analysis team, prosecutor's office, and courts—which are the peers in the channel—would form a consortium in order to participate in blockchain channels and share the identity and investigation information in the hot blockchain using the process **[14]**.

Processing Speed:

the speed at which evidence submissions, retrievals, and transactions are processed is a critical performance metric. Blockchain sharding's parallel processing capability can significantly improve processing speed, enabling multiple transactions to be processed simultaneously across different shards **[11]**.

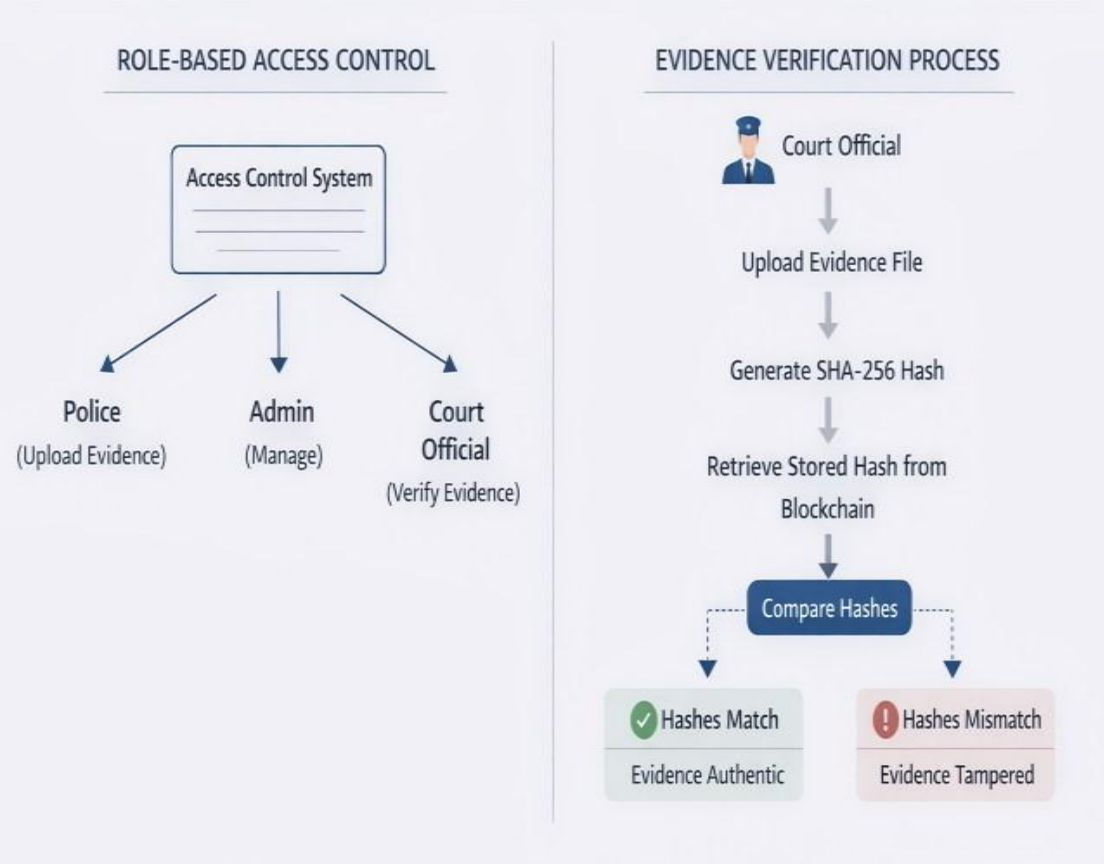
Storage Efficiency:
This metric evaluates how efficiently the framework stores digital evidence. With the integration of IPFS, the framework should provide secure and decentralized storage while minimizing redundancy and optimizing memory usage.

Data Retrieval Time:
The time it takes to retrieve evidence when needed is crucial, especially in forensic investigations where quick access to evidence can impact case outcomes. IPFS should facilitate fast and reliable data retrieval.

Scalability:
Scalability is a key consideration, as the framework should be able to handle a growing volume of evidence submissions and retrievals. Sharding allows for horizontal scalability by dividing the blockchain network into smaller partitions, accommodating more transactions.

Gas Efficiency:
in Ethereum-based implementations, gas consumption is a critical metric. Gas represents the computational effort required for transactions. The framework should aim to minimize gas consumption to reduce operational costs **[11]**.

Figure 4 Role-Based Access & Evidence Verification



5. CONCLUSION

The rapid digitalization of law enforcement and judicial processes demands secure and transparent mechanisms for managing digital evidence. Traditional evidence storage and verification methods suffer from vulnerabilities such as tampering, unauthorized access, data loss, and an unreliable chain of custody. These issues can deeply impact the fairness and credibility of legal proceedings. The proposed Blockchain-Based Evidence Management and Verification System address these challenges by integrating blockchain's immutability, IPFS's decentralized storage capabilities, and cryptographic hashing for authenticity verification. Through Ethereum smart contracts, the system ensures tamper-proof logging, transparent tracking of evidence, and automated role-based access control. The use of SHA-256 hashing guarantees that any alteration in evidence is immediately detectable, thereby upholding integrity throughout the evidence lifecycle **[14]**.

This system enhances trust, accountability, and efficiency in evidence handling while reducing the risk of manipulation or accidental data loss. By providing a secure, decentralized, and verifiable platform, the solution strengthens the credibility of digital evidence in courts and contributes to a more transparent and reliable justice system. It represents a significant advancement toward modernizing judicial workflows and safeguarding the integrity of legal processes in the digital era.

REFERENCES

J. Guo *et al.*, "Antitampering Scheme of Evidence Transfer Information in Judicial System Based on Blockchain," *Security and Communication Networks*, vol. 2022, 2022, doi: 10.1155/2022/5804109.

M. M. Sudhakar, K. Madanu, B. M. Kumar, V. S. Sankeerthana, D. Sai, and K. Naik, "Block Chain Based Evidence Management System."

D. Batista *et al.*, "Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review," Aug. 01, 2023, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/jrfm16080360.

S. Gaikwad, A. Ponde, V. Bhogade, and V. Chavan, "Evidence Management System Using Blockchain", [Online]. Available: www.ijsart.com

E. Yunianto, Y. Prayudi, and B. Sugiantoro, "B-DEC: Digital Evidence Cabinet based on Blockchain for Evidence Management," 2019.

M. M. Gaikwad, "DEVELOPMENT OF BLOCKCHAIN BASED SMART CONTRACTS FOR DIGITAL FORENSIC," 2024. [Online]. Available: www.ijnrd.org

M. S. Rahman, I. Khalil, P. C. Mahawaga, A. Bouras, and X. Yi, "A novel architecture for tamper proof electronic health record management system using blockchain wrapper," in *BSCI 2019 - Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure, co-located with AsiaCCS 2019*, Association for Computing Machinery, Inc, Jul. 2019, pp. 97–105. doi: 10.1145/3327960.3332392.

S. S. Alqahtany and T. A. Syed, "ForensicTransMonitor: A Comprehensive Blockchain Approach to Reinvent Digital Forensics and Evidence Management," *Information (Switzerland)*, vol. 15, no. 2, Feb. 2024, doi: 10.3390/info15020109.

S. Rao, S. Syed, S. Fernandes, and S. Raorane, "A Novel Approach for Digital Evidence Management using Blockchain." [Online]. Available: https://ssrn.com/abstract=3683280

B. Mbimbi, D. Murray, and M. Wilson, "Private Blockchain-Driven Digital Evidence Management Systems: A Collaborative Mining and NFT-Based Framework," *Information (Switzerland)*, vol. 16, no. 7, Jul. 2025, doi: 10.3390/info16070616.

V. Shiva Kumar, N. Udayasree, G. Savitha, M. Sravani, and A. Professor, "BLOCKCHAIN BASED EVIDENCE MANAGEMENT SYSTEM."

S. Liu and Q. Zheng, "A study of a blockchain-based judicial evidence preservation scheme," *Blockchain:Research and Applications*, vol. 5, no. 2, Jun. 2024, doi: 10.1016/j.bcra.2024.100192.

M. Mustafa M, K. T C, K. N, and L. Bharathi M, "Forensic Evidence Management Using Blockchain Technology," *International Journal of Innovative Science and Research Technology (IJISRT)*, pp. 268–273, Apr. 2024, doi: 10.38124/ijisrt/ijisrt24apr354.

.