ISSN: 3107-6513

Crime Evidence Management System using Blockchain Technology

G. Deepthi[1], Y. Vani2, B. Sai Vinay[3]

[1-3]IV Year Student, Dept. of IT, Malla Reddy Engineering College Secunderabad, Telangana, India.

Corresponding_author: hodaiml439@gmail.com

Abstract - One of the major problems in crime investigation today is the lack of security and transparency in how crime evidence is stored. Traditional systems use centralized databases, which can be easily tampered with by administrators or unauthorized users. This can lead to false evidence, wrongful judgments, and a lack of trust in the justice system. In the existing system, police departments store all crime records in one central location. If someone changes or deletes data, there is usually no way to detect it. There is also no proper tracking or verification method to ensure the evidence is genuine. To overcome these problems, we propose a Blockchain-Based Crime Evidence System. This system uses Ethereum blockchain to store crime evidence in a decentralized and tamper-proof way. Each piece of evidence is recorded as a blockchain transaction, making it impossible to change without detection. Smart contracts written in Solidity are used to manage how data is added and accessed, ensuring that only authorized users can interact with the system.

Keywords: *Blockchain, Crime Evidence, Ethereum, Smart Contracts, Solidity, Decentralization, Data Security, Tamper-Proof System, Transparency, Evidence Management System*

I. INTRODUCTION

The secure management of crime evidence is a cornerstone of every justice system. The authenticity, integrity, and traceability of evidence directly influence the accuracy of investigations, fairness of trials, and public trust in law enforcement institutions. Digital transformation has significantly increased the volume and variety of evidence, including documents, images, videos, CCTV footage, communication records, and sensor data. While this shift has improved investigative capabilities, it has also introduced serious challenges related to data security, unauthorized access, manipulation, and lack of transparency in evidence handling processes.

Traditional crime evidence management systems rely primarily on centralized databases controlled by a single authority. Although such systems offer ease of access and basic security controls, they remain highly vulnerable to insider threats, cyberattacks, accidental data loss, and unauthorized modifications. The absence of a verifiable and tamper-proof audit trail weakens the chain of custody and raises concerns about the admissibility of digital evidence in court. Once data is altered or deleted, proving its originality becomes extremely difficult, creating legal disputes and undermining trust in judicial outcomes.

As modern investigations become increasingly data-driven, there is a growing need for systems that can ensure evidence integrity, accountability, and transparency throughout the entire evidence lifecycle—from collection and storage to analysis and courtroom presentation. Recent advancements in blockchain technology have opened new opportunities for transforming digital evidence management. Blockchain is a decentralized and cryptographically secured ledger system in which records are stored in immutable blocks linked through hash values. Its distributed nature eliminates single points of failure and ensures that no individual entity can alter stored data without detection.

By integrating blockchain with smart contracts and secure web applications, a Blockchain-Based Crime Evidence Management System can provide a robust, transparent, and tamper-proof platform for handling digital evidence. Smart contracts automate evidence registration, access control, and verification processes, while cryptographic hashing ensures that any unauthorized modification is instantly detected. This approach not only strengthens the chain of custody but also enhances accountability and trust among law enforcement agencies, forensic departments, and courts.

This project proposes a blockchain-driven framework that leverages decentralized storage, cryptographic security, and role-based access control to create a secure evidence management ecosystem. By ensuring transparency, traceability, and data integrity, the proposed system aims to modernize crime evidence handling and provide a reliable foundation for digital forensics and legal proceedings.

II. LITERATURE REVIEW

Research on secure digital evidence management, blockchain applications in forensics, and decentralized data security has increased significantly in recent years. The following review highlights key contributions that form the foundation for the proposed Blockchain-Based Crime Evidence Management System.

The study by Kshetri (2018) examines how blockchain technology can improve transparency and accountability in law enforcement and public sector data systems [1]. The author highlights blockchain's ability to provide immutable audit trails and eliminate single points of failure found in centralized systems. The research emphasizes that cryptographic hashing and distributed ledgers significantly reduce data tampering and insider threats. However, the study remains theoretical and does not propose a full evidence management framework. This limitation motivates the present project to design a practical, application-level blockchain evidence system.

Zyskind et al. (2015) proposed a decentralized data ownership model using blockchain to control access to sensitive information [2]. Their framework uses smart contracts to regulate permissions and data sharing, ensuring that only authorized users can access protected records. Although their work focuses on personal data privacy, its access control and trust model directly supports the secure sharing of crime evidence in forensic systems. However, it does not address large file handling or legal audit requirements, which are covered in the proposed system.

Li et al. (2020) developed a blockchain-based digital forensics framework that ensures integrity and traceability of evidence across multiple agencies [3]. Their system stores cryptographic hashes of evidence on the blockchain while maintaining actual files in off-chain storage. This hybrid approach improves scalability and performance. While effective, their solution lacks a user-friendly interface and role-based access management, which are key features implemented in the present project.

Zhang and Wen (2017) explored the use of blockchain to secure Internet of Things (IoT) forensic data [4]. Their study demonstrates how blockchain prevents evidence manipulation by maintaining an immutable transaction history. The authors highlight that timestamps and cryptographic signatures enhance chain-of-custody verification. However, the system focuses only on IoT data sources and does not support manual evidence uploads or legal workflows. The proposed project extends these ideas to a broader crime evidence management context.

Dorri et al. (2017) proposed a blockchain-based security framework for access control and data authentication [5]. Their model shows how decentralized identity and permission mechanisms can prevent unauthorized system access. Although not developed for crime evidence, the access control architecture directly inspires the membership and role-based security features used in the current system.

Azaria et al. (2016) introduced smart contracts for automated record management and auditing [6]. Their work demonstrates that smart contracts can enforce rules without human intervention. This concept is directly adopted in the proposed system, where smart contracts manage evidence submission, verification, and access logging.

TABLE 1. Summary of Key Studies and Comparison with the Proposed Paper

The reviewed studies demonstrate that blockchain provides a strong foundation for secure, tamper-proof, and transparent digital record management. However, existing systems either lack practical deployment, user-friendly design, role-based access control, or legal workflow integration. The proposed Blockchain-Based Crime Evidence Management System addresses these gaps by combining decentralized storage, smart contracts, cryptographic hashing, secure identity management, and a web-based interface. This approach ensures integrity, accountability, and trust throughout the crime evidence lifecycle.

III. PROBLEM FORMULATION

In the criminal justice system, crime evidence plays a crucial role in determining judicial outcomes. Digital evidence such as images, videos, forensic reports, call logs, and official documents is traditionally stored in centralized databases or physical repositories. However, centralized evidence management systems are highly vulnerable to data tampering, unauthorized access, cyberattacks, insider manipulation, and single-point failures. Any alteration, deletion, or unauthorized modification of evidence can compromise investigations and affect court verdicts.

Existing systems lack a secure and transparent mechanism to guarantee evidence integrity and proper chain-of-custody tracking. There is insufficient traceability to monitor who accessed, transferred, or modified evidence records. Moreover, limited auditability and accountability create trust issues among stakeholders, including law enforcement agencies, forensic departments, and judicial authorities.

Therefore, the core problem addressed in this research is the absence of a decentralized, tamper-proof, and transparent crime evidence management system that ensures integrity, traceability, and secure access control while eliminating centralized vulnerabilities.

To address these challenges, this research proposes a Blockchain-Based Crime Evidence Management System that leverages the decentralized and immutable nature of blockchain technology. In the proposed system, digital evidence is securely stored in off-chain storage, while its cryptographic hash and related metadata are recorded on the blockchain to ensure integrity and traceability. Every evidence-related action, such as uploading, accessing, or transferring, is logged as a blockchain transaction, creating a permanent and auditable record. Smart contracts are used to enforce access control policies and automate chain-of-

custody tracking. By eliminating centralized vulnerabilities and ensuring transparency, the proposed system enhances security, accountability, and trust in the management of digital crime evidence.

IV. METHODOLOGY

To address the security, integrity, and transparency challenges in crime evidence management, this research proposes a secure, decentralized, and tamper-resistant blockchain-based framework. The methodology integrates secure evidence acquisition, cryptographic hashing, distributed ledger technology, smart contract–based access control, and automated chain-of-custody tracking. The proposed framework is designed to operate efficiently within law enforcement agencies, forensic departments, and judicial systems while ensuring scalability and data integrity.

The methodology follows a modular and layered architecture, ensuring transparency, immutability, and secure interoperability between different stakeholders. Each module transforms raw digital evidence into a secure, verifiable, and court-admissible record while maintaining a complete audit trail.

A. System Architecture Overview

The proposed system architecture consists of five interconnected layers:

1. Evidence Acquisition Layer
2. Cryptographic Processing Layer
3. Blockchain Network Layer
4. Smart Contract and Access Control Layer
5. Verification and Audit Layer

This layered structure enables continuous monitoring, secure storage, and real-time verification of crime evidence throughout its lifecycle.

B. Evidence Acquisition and Integration

The first stage involves collecting digital evidence from multiple sources such as CCTV footage, mobile devices, forensic laboratories, police reports, and digital surveillance systems. Each collected evidence file is assigned a unique Evidence ID along with associated metadata such as case ID, officer ID, timestamp, and location.

The system ensures that only authenticated personnel can upload evidence. This prevents unauthorized data insertion and ensures traceability from the moment of evidence collection. The acquisition layer aggregates data into a unified secure interface for further processing.

C. Cryptographic Hashing and Secure Storage

Once the evidence is collected, a cryptographic hashing algorithm (such as SHA-256) is applied to generate a unique digital fingerprint of the file. This hash value uniquely represents the content of the evidence. Even a minor alteration in the original file results in a completely different hash value, enabling tamper detection.

The actual evidence file is stored in secure off-chain storage, such as IPFS or a protected cloud database, to ensure scalability and efficient storage management. Only the hash value and metadata are transmitted to the blockchain network. This hybrid storage approach ensures both performance efficiency and strong integrity guarantees.

D. Blockchain Network and Transaction Management

The blockchain layer records evidence metadata as immutable transactions. Each transaction contains the evidence hash, timestamp, and user information. Transactions are validated by participating nodes using a consensus mechanism and grouped into blocks. Each block is cryptographically linked to the previous block, forming a secure and immutable chain.

Since every block contains the hash of the previous block, any modification attempt would invalidate the chain structure. This ensures data immutability, prevents tampering, and eliminates centralized vulnerabilities.

The decentralized nature of blockchain removes single-point failure risks and ensures that evidence records remain permanently accessible and verifiable.

E. Smart Contract–Based Access Control and Chain of Custody

Smart contracts are deployed to automate access control and evidence lifecycle management. These contracts define predefined rules such as:

- Only authorized officers can upload evidence.
- Evidence cannot be deleted or modified.
- Every access or transfer request is logged.
- Ownership transfer between departments is recorded.

Whenever evidence is accessed, transferred, or verified, a new blockchain transaction is generated. This creates a transparent and immutable chain of custody, ensuring accountability and preventing disputes regarding evidence handling.

F. Verification and Audit Mechanism

During investigations or court proceedings, the stored evidence file is retrieved from off-chain storage and reprocessed through the hashing algorithm. The newly generated hash is compared with the hash stored on the blockchain ledger. If both values match, the evidence is confirmed as authentic and untampered.

The system also provides a complete audit trail, enabling authorized stakeholders to review the history of evidence interactions. This enhances trust, transparency, and legal reliability.

The explainability aspect of the system ensures that every action performed on evidence is traceable and interpretable, supporting human oversight and judicial validation.

ISSN: 3107-6513

V. RESULTS AND DISCUSSIONS

The proposed Blockchain-Based Crime Evidence Management System was evaluated using a prototype implementation to analyze its effectiveness in improving security, transparency, and integrity of digital evidence handling. The system was tested under various simulated scenarios that replicate real-world evidence management processes within law enforcement environments. The performance of the proposed framework was compared with a conventional centralized evidence storage system to assess improvements in operational efficiency and tamper resistance. The evaluation considered scenarios such as evidence upload, verification, transfer between departments, unauthorized access attempts, and audit inspections. In the traditional system, evidence records were maintained in a centralized database with manual logging mechanisms. In contrast, the proposed system stored evidence files in secure off-chain storage while recording cryptographic hash values and metadata on a blockchain ledger. Smart contracts were used to automate access control and maintain an immutable chain of custody.

Evidence ID	Investigating Officer	Reported Crime	Crime Details	Evidence Details	Crime Area	Witness Name	Witness Phone	Crime Date	Evidence Image
1	kumar	Burglary	two unidentified men covered in black mask looted gold shop at 3a.m	collected finger print and cctv footage from crime scene	12-23-890 Floor no 3, Ameerpet, hyd	shyam	9876543212	2025-01-16	

The results indicate that the proposed system significantly enhances evidence integrity and traceability. During tampering simulations, any modification made to stored evidence was immediately detected through hash mismatch verification, demonstrating high tamper detection accuracy. The blockchain ledger ensured that every interaction with evidence was permanently recorded, thereby providing complete audit traceability. This eliminated ambiguity regarding who accessed or transferred evidence at any given time. Additionally, the decentralized architecture improved system reliability by reducing dependency on a single server, thereby minimizing risks associated with single-point failure attacks. Access control enforcement was more secure due to smart contract–based authorization mechanisms, which prevented unauthorized modifications and maintained strict accountability. Overall, the experimental evaluation confirms that the proposed blockchain-based framework offers superior security, transparency, and reliability compared to traditional centralized evidence management systems. The results validate the feasibility of implementing blockchain technology in digital crime evidence management to strengthen judicial trust and ensure evidence authenticity.

VI. CONCLUSION AND FUTURE SCOPE

This research presented a Blockchain-Based Crime Evidence Management System designed to enhance the security, transparency, and integrity of digital evidence handling within the criminal justice system. Traditional centralized evidence storage mechanisms are vulnerable to tampering, unauthorized access, and single-point failures, which may compromise investigations and judicial outcomes. To address these challenges, the proposed framework integrates cryptographic hashing, decentralized blockchain technology, secure off-chain storage, and smart contract–based access control to ensure immutability and reliable chain-of-custody tracking. The experimental evaluation demonstrated that the system effectively detects evidence tampering, maintains a transparent and permanent audit trail, and improves accountability among stakeholders such as law enforcement agencies and judicial authorities. By leveraging blockchain's decentralized architecture, the proposed system eliminates centralized vulnerabilities and strengthens trust in digital evidence management processes. Although the results validate the feasibility and effectiveness of the proposed framework, further enhancements can be explored in future work. The system can be extended by deploying it on a permissioned blockchain network specifically tailored for law enforcement environments to improve performance and regulatory compliance. Advanced encryption techniques may be integrated to enhance confidentiality of sensitive metadata. Additionally, Artificial Intelligence techniques can be incorporated for automated evidence classification, tagging, and analysis to support faster investigations. Future research may also focus on large-scale real-world deployment, interoperability between multiple agencies, and legal validation studies to examine admissibility of blockchain-based evidence across different judicial systems. These improvements will further strengthen the proposed system as a scalable and reliable solution for modern digital crime evidence management.

REFERENCES

[1]. N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 1027–1038, 2018.

[2]. G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Security and Privacy Workshops (SPW)*, San Jose, CA, USA, 2015, pp. 180–184.

[3]. X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, pp. 841–853, 2020.

[4]. Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the internet of things," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 983–994, 2017.

[5]. A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: Challenges and solutions," *IEEE Access*, vol. 6, pp. 8078–8090, 2017.

[6]. A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open and Big Data (OBD)*, Vienna, Austria, 2016, pp. 25–30.