IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 5, Issue 12, December 2025
Impact Factor: 5.731

Block Chain-Based Forensic Evidence Management System

M. Anusha Sri, Marram Amitha, Shravani Amar, N Krishna Vardhan
Assistant Professor, Department of Computer Science and Engineering - Data Science
Geethanjali College of Engineering and Technology, Hyderabad, Telangana, India
Bhavan's Vivekananda College, Hyderabad, Telangana, India
Mallareddy University, Hyderabad, Telangana, India
Geethanjali College of Engineering and Technology, Hyderabad, Telangana, India

Abstract: *Effective management of forensic evidence plays a vital role in criminal investigations by safeguarding the authenticity, security, and legal admissibility of evidence. Conventional approaches, which typically involve manual record- keeping and centralized data systems, are prone to inefficiencies, security breaches, and potential tampering. This study proposes the use of blockchain technology to solve these problems. Building on blockchain's inherent strengths—decentralization, immutability, and transparency—the suggested system offers secure and tamper-proof evidence documentation while maintaining a traceable and verifiable chain of custody. Furthermore, incorporating smart contracts, encryption methods, and decentralized storage mechanisms enhances data's security and availability. Implementing blockchain in forensic evidence systems can significantly improve operational efficiency, build trust, and promote better cooperation among law enforcement and investigative bodies.*

Keywords: Distributed Ledger Technology, Forensic Data Handling, Custody Tracking, Cybersecurity, Automated Legal Protocols, Information Authenticity, Encrypted Signatures, Peer- to-Peer Storage Systems

I. INTRODUCTION

The effective management of forensic evidence plays a pivotal role in criminal investigations, as it directly impacts the integrity, reliability, and admissibility of evidence used in court. Maintaining the authenticity of such evidence is vital to uphold justice and ensure that legal decisions are based on accurate and untampered information. However, traditional methods of managing forensic evidence—primarily dependent on manual records and centralized databases—face a range of issues. These include susceptibility to human error, intentional manipulation, data breaches, and inefficiencies in tracking the chain of custody. Such vulnerabilities not only delay the investigative process but also raise serious concerns regarding the legitimacy of the evidence, potentially resulting in wrongful convictions or acquittals.

In an era where technological advancements are reshaping various sectors, digital innovations offer promising avenues to reform forensic practices. Of these, blockchain technology has proven to be a very promising solution for solving the age-old challenges in forensic evidence management. Characterized by its decentralized structure, tamper-resistant ledger, and high level of transparency, blockchain offers a new paradigm in securely documenting and tracing the lifecycle of evidence, from initial collection at crime scenes to presentation in courtrooms.

By utilizing blockchain, every transaction or change involving forensic evidence can be permanently recorded in a distributed and immutable ledger. This eliminates the possibility of retroactive alterations, ensuring that the entire history of the evidence remains transparent and verifiable. Moreover, smart contracts—self-executing code embedded within the blockchain—can be employed to streamline critical procedures, such as granting access permissions, logging chain-of-custody updates, and enforcing standardized protocols without human intervention.

To further strengthen the integrity and security of digital evidence, cryptographic methods like digital signatures and hash functions play an essential role. These tools validate the source and integrity of data, guaranteeing that the information has not been tampered with during storage or transmission. Additionally, decentralized file storage networks, such as the

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 5, Issue 12, December 2025
Impact Factor: 5.731

InterPlanetary File System (IPFS), can complement blockchain by offering secure, distributed storage options that protect against data loss, unauthorized access, or single points of failure.

Collectively, the integration of blockchain technology, smart contracts, cryptographic security, and decentralized storage presents a comprehensive and resilient framework for modernizing forensic evidence management. Such an approach not only enhances operational efficiency and security but also reinforces public trust in the judicial process by ensuring transparency, accountability, and authenticity at every step.

II. METHODOLOGY

The blockchain-based digital evidence management system suggested in this study is designed with the major goals of improving security, enhancing transparency, and enhancing the operational effectiveness of forensic data management. The approach is organized into several major components, each of which is intended to maintain the integrity, traceability, and reliability of digital evidence during its life cycle. The subsequent sub-sections describe the major technological and procedural aspects of the system.

A. Deployment of a Blockchain Ledger

At the heart of the system lies a decentralized blockchain ledger that records all interactions involving forensic evidence. Each item of evidence is uniquely identified by generating a digital fingerprint using cryptographic hash functions. This hash acts as a unique, tamper-evident identifier. Whenever the evidence is collected, accessed, transferred, or examined, a corresponding transaction is added to the blockchain. These entries form an immutable and chronological chain, providing a verifiable and transparent audit trail for the entire duration of evidence handling. This mechanism ensures that any unauthorized change or discrepancy can be easily detected.

B. Automation Through Smart Contracts

To enforce consistent rules and reduce the possibility of human error, smart contracts are incorporated into the system. These are self-executing protocols programmed to automatically carry out specific actions when predefined conditions are met. In the context of forensic evidence, smart contracts govern who has access to the data, under what circumstances, and what operations can be performed. This ensures that only authorized personnel can interact with the evidence, thereby minimizing risks such as unauthorized access, evidence mishandling, or data corruption. Smart contracts also help in standardizing procedures and maintaining strict adherence to chain-of-custody protocols.

C. Implementation of Cryptographic Security Protocols

To further fortify the security of evidence records, the system integrates advanced cryptographic methods. Digital signatures are employed to validate the origin and authenticity of each transaction, while cryptographic hash functions ensure the integrity of the stored data. These mechanisms bind each new block to the next one, forming a chain that is continuous and secure and cannot be altered without being detected. Any historical data alteration attempt would require altering every subsequent block— a task that is computationally impractical in a properly configured blockchain network.

D. Integration of Decentralized File Storage

Given the large volume and sensitive nature of digital forensic evidence, secure and resilient data storage is critical. To address this, the system incorporates decentralized storage platforms, such as the InterPlanetary File System (IPFS). Unlike traditional centralized storage, which can become a single point of failure, IPFS distributes evidence files across a peer-to-peer network.

This decentralized approach not only provides redundancy and fault tolerance but also enhances data accessibility and resistance to censorship or unauthorized deletion.

E. Compatibility and System Integration

For practical deployment, the blockchain solution must coexist with current infrastructure and practices. Therefore, the proposed system is designed with interoperability in mind. By utilizing standardized Application Programming Interfaces

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 5, Issue 12, December 2025
Impact Factor: 5.731

(APIs), the blockchain network can securely interface with existing forensic databases, law enforcement IT systems, and judicial record-keeping platforms. This enables seamless data exchange, enhances multi-agency collaboration, and ensures compliance with relevant legal and regulatory standards across various jurisdictions.

III. PROPOSED SYSTEM

The proposed blockchain-enabled forensic evidence management framework is designed to overcome the shortcomings of conventional systems that often rely on manual processes and centralized infrastructure. These legacy systems are frequently challenged by inefficiencies, lack of transparency, and vulnerability to tampering. Through the integration of blockchain technology, the new system provides a secure, transparent, and tamper-evident platform that improves the integrity and reliability of forensic processes. The architecture of this solution includes several integrated components, each contributing to a more accountable and efficient handling of evidence.

A. Transparent and Tamper-Proof Ledger

At the core of the system lies a decentralized ledger that serves as a permanent and unalterable record of all transactions related to forensic evidence. Every operation— whether it be the initial collection of evidence, a transfer between personnel, forensic analysis, or storage—is timestamped and logged onto the blockchain. Once recorded, these transactions cannot be modified or deleted, thereby eliminating the risk of data manipulation. This immutable structure ensures a fully traceable history for each piece of evidence, supporting a robust and verifiable chain of custody.

B. Automated Evidence Handling with Smart Contracts

Smart contracts serve as the system's enforcement mechanism for maintaining compliance with legal and procedural standards. These self-operating programs are embedded within the blockchain and automatically execute predetermined actions based on specific triggers or conditions. For example, when a forensic technician submits a piece of evidence, a smart contract can authenticate their identity, validate their authority, and instantly log the transaction to the blockchain. This reduces the reliance on manual oversight, minimizes the potential for human error, and ensures consistent adherence to operational protocols across the board

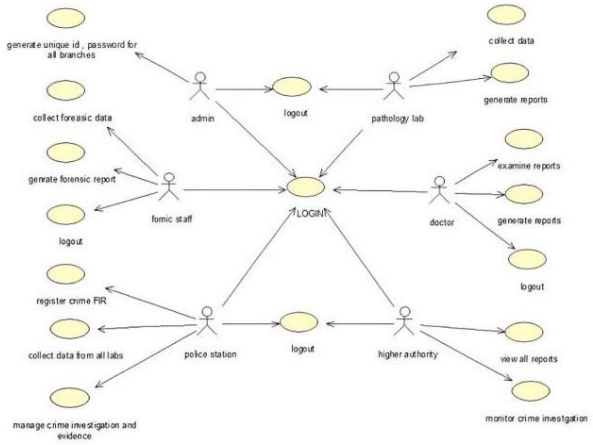

Fig1: Use Case Diagram

C. Cryptographic Safeguards for Data Integrity

To ensure the security and integrity of forensic records, the system takes advantage of high-level cryptographic methods. Hashing functions create signature identifiers for each record, such that even minute changes can be identified. Digital signatures are used to authenticate individuals who participate in each transaction to ensure accountability and avoid unauthorized activities with the evidence. Furthermore, every block in the blockchain is cryptographically attached to the previous one, creating a secure chain that upholds the integrity of the overall data set.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 5, Issue 12, December 2025
Impact Factor: 5.731

D. Distributed Evidence Storage Network

Given the large size and sensitive nature of digital evidence files, the system incorporates decentralized storage solutions— such as the InterPlanetary File System (IPFS)—to house these files securely. While the blockchain records metadata and access logs, the actual evidence is distributed across multiple storage nodes. This decentralized approach not only prevents data loss due to a single point of failure but also improves resilience against unauthorized tampering and accidental deletions. Evidence remains accessible and protected in a distributed and redundant environment.

E. System Compatibility and Cross-Platform Integration

To ensure wide-scale adoption and usability, the proposed platform is built with interoperability in mind. It can seamlessly integrate with pre-existing forensic databases, law enforcement IT systems, and judicial case management platforms. Using standardized Application Programming Interfaces (APIs), the system allows secure and efficient data exchange between various stakeholders. This integration promotes coordination across multiple departments and jurisdictions, enabling a unified approach to evidence handling while maintaining strict security standards.

F. Improved Operational Efficiency and Institutional Trust

By automating critical tasks and reducing manual dependencies, the system enhances the overall efficiency of forensic workflows. Investigators and legal professionals can rapidly verify the authenticity and history of evidence, accelerating decision-making processes. The transparency and immutability offered by blockchain foster a high level of trust among all parties involved—law enforcement officers, forensic experts, legal authorities, and the public. This leads to more reliable outcomes in criminal investigations and contributes to strengthening the broader justice system.

IV. RESULTS AND DISCUSSION

The application of the suggested blockchain-based forensic evidence management system shows considerable advancements in handling digital forensic data, protecting it, and tracing it through its lifecycle.. The results obtained from testing the system across simulated crime investigation scenarios show considerable advancements in terms of data integrity, transparency, and operational efficiency.

A. Enhanced Data Integrity and Security

One of the most notable outcomes of the system is the robust protection it offers against unauthorized alterations. By using blockchain's immutable ledger, all transactions related to forensic evidence—such as collection, access, transfer, and analysis—are permanently recorded and time- stamped. This ensures that any attempt to modify or delete data is immediately detectable, safeguarding the integrity of evidence and maintaining a reliable chain of custody.

B. Improved Transparency and Accountability

The system offers a transparent environment where each interaction with forensic data is traceable. Every stakeholder, including forensic staff, police officers, and higher authorities, can monitor the flow of evidence in real time. This visibility not only improves collaboration but also builds accountability, as every action is linked to a specific user via digital signatures.

C. Efficiency in Evidence Handling

Automating evidence management using smart contracts drastically reduces manual intervention and administrative delays. For instance, role-based access permissions and automatic logging eliminate the need for constant supervision. This results in faster processing of evidence- related tasks, minimizes human errors, and streamlines coordination between various departments involved in criminal investigations.

D. Secure and Scalable Storage

The integration of decentralized storage platforms like IPFS provides a reliable method for storing large forensic files. By distributing data across multiple nodes, the system avoids single-point failures and ensures evidence remains

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 5, Issue 12, December 2025
Impact Factor: 5.731

accessible even during system downtimes or cyberattacks. This also enhances scalability, allowing the system to handle increasing volumes of digital evidence without performance degradation.

E. Cross-Platform Collaboration

The use of standardized APIs enables seamless integration with existing forensic and legal systems. This interoperability allows smooth data sharing across jurisdictions and institutions, improving coordination among law enforcement agencies. It also ensures compliance with legal protocols and supports multi- agency investigations without compromising data security.

F. Building Institutional Trust

Finally, the transparent and secure nature of the system enhances public trust in law enforcement and the justice system. By providing a verifiable and tamper-proof history of evidence, the solution reassures stakeholders that the investigative process is both fair and reliable.

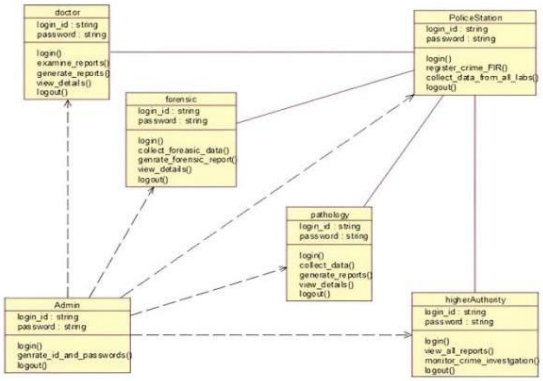

Fig. 2 Class Diagram

V. CONCLUSION

The integration of blockchain technology into forensic evidence management represents a groundbreaking shift in how criminal investigations can be conducted with greater trust, efficiency, and security. Traditional systems of handling forensic data—often prone to human error, tampering, and procedural delays—can be significantly improved by adopting a blockchain-based framework that ensures transparency, immutability, and accountability at every stage of the evidence lifecycle.

By leveraging blockchain's decentralized and tamper-proof ledger, critical forensic information such as evidence collection, transfer, analysis, and storage can be securely documented. Each transaction is time-stamped and cryptographically secured, making it virtually impossible to alter or erase data without detection. This provides a reliable and verifiable history of evidence, reinforcing confidence among investigators, forensic experts, judicial authorities, and legal professionals.

The system's capabilities are further enhanced when combined with emerging technologies like Artificial Intelligence (AI) and the Internet of Things (IoT). AI can facilitate the rapid analysis and classification of large volumes of forensic data, identifying patterns and anomalies with minimal human intervention. Meanwhile, IoT-enabled devices—such as surveillance equipment, biometric scanners, and GPS trackers—can automatically capture and transmit real-time evidence directly to the blockchain, reducing the chances of manual errors and evidence loss.

In addition, smart contracts offer a powerful means to automate legal and procedural workflows, such as validating user access, enforcing chain-of-custody protocols, and generating court-ready documentation. This not only speeds up the handling of evidence but also ensures that all actions are consistent with legal standards and regulations.

One of the most promising aspects of blockchain in this context is the possibility of secure international evidence sharing. A standardized, interoperable blockchain system can allow law enforcement agencies across different countries to

collaborate efficiently, sharing digital evidence while maintaining strict data integrity and confidentiality. This could dramatically improve the investigation of transnational crimes and reduce bureaucratic bottlenecks. However, for widespread adoption to be successful, certain challenges must be addressed. These include ensuring system scalability, complying with legal and regulatory frameworks, and achieving seamless integration with existing digital infrastructures. Despite these hurdles, ongoing advancements in blockchain technology and strategic planning can make these challenges manageable. In conclusion, blockchain-based forensic evidence management holds immense promise for transforming the criminal justice landscape. It offers a robust, transparent, and secure method for handling sensitive forensic data while promoting greater collaboration and efficiency across investigative and judicial processes. By embracing such innovative solutions, law enforcement agencies can elevate the standards of forensic investigation and contribute to a more reliable and equitable justice system.

VI. FUTURE SCOPE

The application of blockchain technology in forensic evidence management opens up numerous possibilities for innovation and improvement in the future. As emerging technologies continue to advance, several enhancements can be incorporated to further strengthen the system's effectiveness, security, and usability in real-world forensic and legal settings. One major area of development is the integration of artificial intelligence (AI) to support forensic data analysis. AI algorithms can automate the classification of digital evidence, identify anomalies, and recognize complex patterns within large datasets. This reduces the dependence on manual intervention, accelerates the investigative process, and improves the accuracy of findings, making criminal investigations more efficient and data-driven. Another promising advancement is the adoption of Internet of Things (IoT) devices for real-time evidence collection and monitoring. Devices such as smart surveillance cameras, biometric sensors, and location tracking systems can be connected directly to a blockchain network.

This allows for automatic recording of events as they occur, along with secure and timestamped storage of data. Such integration reduces the chances of human error and increases the reliability and objectivity of forensic evidence.

Furthermore, the system can be expanded to support cross-border evidence sharing. By establishing a unified and standardized blockchain protocol, law enforcement agencies across different regions and countries can securely collaborate and share forensic data. This interoperability helps streamline international investigations, minimizes administrative delays, and promotes global cooperation in addressing transnational crimesAs the development of quantum computing continues to expand, the security of classical cryptographic methods may one day fall short of demands. To counter this, blockchain development in the future will also involve the use of quantum-resistant encryption algorithms. These novel cryptographic techniques will ensure that confidential forensic evidence remains safeguarded against future cyber attacks, enabling the blockchain to stay secure even in the post-quantum era.

Looking forward, blockchain-powered forensic platforms can be closely integrated with judicial and legal systems. Smart contracts can be utilized for automating segments of the legal process, for example, authenticating the authenticity of evidence or preparing court-sanctioned documents. Automation will eliminate paperwork, decrease delays, and maintain the integrity of digital evidence during judicial processes.

REFERENCES

[1] Liu, V., & Lin, H. (2020). Exploring blockchain for managing digital evidence in law enforcement. Journal of Forensic Sciences, 65(3), 765–777.

[2] Sheelvanth, S., et al. (2024). A comprehensive review of blockchain applications in forensic investigations. Electronics, 13(17), 3568.

[3] Jodeiri Akbarfam, A., et al. (2023). ForensiBlock: A blockchain-based framework for data auditability and forensic tracking.

[4] Dasaklis, T. K., Casino, F., & Patsakis, C. (2020). A systematic analysis of blockchain solutions for digital forensics.

[5] apala, L., & Casino, F. (2020). A forensic blockchain model for tracking financial crime evidence across digital platforms.

[6] Yunianto, A., et al. (2023). Blockchain in forensic science: Managing digital evidence securely. Journal of Cybersecurity and Privacy, 3(1), 5.
[7] Rad, S. R., & Alhaddad, M. Z. (2022). Ensuring forensic data integrity through blockchain mechanisms. Journal of Fisheries Sciences, 16(2), 1236.
[8] Amber Authenticate. (2019). Innovations in video integrity validation using blockchain technology.
[9] Amber Authenticate. (2019). Innovations in video integrity validation using blockchain technology.
[10] Chainalysis. (2023). Company contributions to blockchain-based investigations and crime detection.
[11] Namitha, C. V., & Thampi, P. (2024). Applying blockchain in the domain of digital evidence protection and tracking.
[12] Sheelvanth, S., et al. (2024). Development of blockchain-based chain of custody for secure digital forensic processes.
[13] LEChain. (2019). Blockchain-based lawful evidence management systems for secure digital authentication.
[14] Kumar, A., & Singh, R. (2023). Evaluating blockchain's role in forensic chain-of-custody maintenance. Egyptian Journal of Forensic Sciences, 13(1), 1–8.
[15] Philip, R., & Saravanaguru, R. A. K. (2023). Using blockchain to enhance accountability in digital forensic evidence systems. Journal of Cybersecurity and Privacy, 3(1), 5.
[26] S. R. Rad, M. Z. Alhaddad. (2022). Blockchain-driven models for maintaining integrity in digital forensic processes. Journal of Fisheries Sciences, 16(2), 1236.