Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

Decentralized Forensic Evidence Tracking using Blockchain and Smart Contracts

Bhoyi Gautami Ravi
Information Science and Engineering
Don Bosco Institute of Technology
Bengaluru

Bhoomika K
Information Science and Engineering
Don Bosco Institute of Technology
Bengaluru

Chandana R
Information Science and Engineering
Don Bosco Institute of Technology
Bengaluru

Hruthishree R
Information Science and Engineering
Don Bosco Institute of Technology
Bengaluru

Amulya M P
Assistant Professor
Information Science and Engineering
Don Bosco Institute of Technology
Bengaluru

Divyashree G
Assistant Professor
Information Science and Engineering
Don Bosco Institute of Technology
Bengaluru

Abstract **-** The rise of digital technology has led to an increase in cybercrime. This has made the management of digital forensic evidence more complicated. Traditional evidence management systems utilize manual methods and centralized databases. Methods like these are vulnerable to data tampering, unauthorized access, and human error. These issues threaten the integrity of the evidence and the chain of custody during the investigation process.

In this paper, we introduce a system that utilizes blockchain technology, smart contracts, and a decentralized system for the tracking of forensic evidence. Security and transparency will be guaranteed. In our system, evidence records are stored as ERC-721 Non-Fungible Tokens. A private Ethereum blockchain was developed using Ganache and combined with wallet-based authentication and Role-Based Access Control to ensure that only authorized personnel have the ability to view and manage evidence. Smart contracts facilitate the registration, verification, transfer, and auditing of evidence, thus, considerably reducing the manual work and greatly increasing the trustworthiness of the system. We proposed a hybrid system of storage whereby evidence and its forensic files are stored off chain, and the evidence metadata and its forensic files are stored on chain. This paper presents the design and architecture of the system,implementation and evaluation are in progress.Our system will be a trusted, efficient, and effective system of evidence management.

Keywords - Blockchain, Digital Forensics, Chain of Custody, Smart Contracts, NFT, ERC-721, Ganache, Role-Based Access Control (RBAC), Evidence Integrity, Digital Evidence Management

INTRODUCTION

The advancement of digital technology has resulted in more crime ,making the need for digital forensics a crucial role in modern law enforcement. Maintaining the integrity of digital evidence from the time of collection until it is presented in court is crucial to the legality of the evidence. This process of securing evidence is known as the chain of custody. Digital evidence can easily be compromised and manipulated, which can affect the outcome of the investigation.

Most traditional evidence management systems rely on a centralized database in which manual documentation records the activities of evidence management. Even with the widespread acceptance of these systems, they are still limited by the risks of tampering, inadequate reliability, lack of traceability, and limited transparency. Because of these risks, it has become imperative to have a management system for digital forensic evidence that is more reliable.

The attributes of blockchain technology have made it specially well suited to manage digital forensic evidence. Every data entry is securely documented in a way that cannot be altered, and provides a permanent history of all the documented evidence activities. Because every documentation entry is time stamped, blockchain is also a very secure way of describing the chain of custody.

The proposed system will use an NFT to represent each item of evidence uniquely. This system will use tokens to unambiguously locate evidence. Tokens will be authenticated and transferred from wallets, with access to evidence controlled using Role-Based Access Control techniques. Access to evidence will be controlled using RBAC techniques as well. Forensic scientists, investigators, and system administrators will have different access privileges as determined by their role within the system.

The proposed system will use smart contracts to automate the evidence registration, transfer and verification processes. Smart contracts will automate the registration, verification, and transfer of evidence. Advanced methods will be used to ensure the efficient storage of evidence. Important transactions, their metadata, and timestamps will be stored on the blockchain with evidence substantively stored in off-chain storage. This strategy will enhance the integrity of the evidence without sacrificing efficiency of the system.

The aim is to create a tracking system that improves the integrity and reliability of the forensic evidence process using blockchain technologies and smart contracts. By using a

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

decentralized approach to secure record management, automated access control, and transaction control, the system intends to strengthen the custody chain and the traceability of forensic evidence. While limitations of existing systems have been taken into account, the system continues to be developed and is expected to be an adaptable solution to address the current needs of the forensic evidence management system.

I. LITERATURE SURVEY

Digital forensic investigations require secure methods to preserve evidence integrity, maintain an unbroken chain of custody, and ensure that digital evidence remains admissible in legal proceedings. Traditional evidence management systems often face challenges such as data tampering, unauthorized access, and lack of transparency. To overcome these issues, many researchers have explored blockchain technology, smart contracts, cryptographic algorithms, and decentralized storage for secure forensic evidence management. The following studies summarize the major developments in this area.

Faizal Nujumudeen et al. presented an adaptive blockchain framework for the secure authentication and preservation of digital forensic evidence. The proposed framework combines adaptive cryptographic techniques with a lightweight Proof-of-Authority (PoA) consensus mechanism to reduce computational overhead while supporting real-time evidence processing. It also introduces interoperability features that enable secure collaboration between different forensic organizations. The study demonstrates that the proposed approach improves evidence integrity, scalability, and authentication without compromising forensic standards [1].

Aparna Rajesh Atmakuri et al. introduced ChainProof, a blockchain-based framework developed to strengthen the digital chain of custody. The system integrates Ethereum smart contracts, SHA-256 hashing, and AI-based anomaly detection to monitor evidence throughout its lifecycle. It verifies the authenticity of evidence while identifying suspicious activities that may occur during handling or transfer. The proposed framework improves transparency, accountability, and trust in digital forensic investigations [2].

Saranya et al. developed a blockchain-based evidence tracking system that focuses on secure ownership and traceability of digital evidence. The framework utilizes Ethereum ERC-721 tokenization, wallet-based authentication, and role-based access control to ensure that only authorized users can access evidence. Smart contracts automate evidence verification and custody transfer, reducing manual intervention. Blockchain maintains a permanent record of every transaction, making the investigation process more transparent and reliable [3].

Renu Mishra et al. proposed a blockchain-enhanced chain-of-custody framework for efficient digital forensic evidence management. The system uses a permissioned blockchain network along with forensic-specific smart contracts to automate evidence tracking and documentation. It supports secure collaboration between multiple investigation agencies while maintaining tamper-proof custody records. The framework also improves the legal admissibility of digital evidence by ensuring complete and accurate documentation [4].

Leandro Loffi et al. designed a blockchain-based chain-of-custody system using Hyperledger Fabric to improve the management of digital evidence. Smart contracts are used to record every stage of evidence handling, including collection, storage, transfer, and verification. This approach creates an immutable audit trail that helps investigators verify the authenticity of digital evidence. The proposed solution significantly reduces the possibility of evidence tampering during judicial proceedings [5].

B. Varija et al. presented a digital forensic investigation model that combines Hyperledger Fabric with AES encryption and SHA hashing techniques. The framework secures digital evidence using a permissioned blockchain while cryptographic algorithms protect data confidentiality and integrity. It supports multiple forensic stakeholders by providing controlled access to evidence throughout the investigation process. The proposed model strengthens the chain of custody and ensures secure evidence management [6].

B. Abisha et al. proposed a secure cyber forensic framework by integrating Practical Byzantine Fault Tolerance (PBFT), threshold cryptography, and AI-driven integrity verification. The framework stores forensic logs securely on the blockchain and uses an optimized XGBoost classifier to identify tampered evidence. This combination improves the accuracy of evidence verification while maintaining immutable forensic records. The study demonstrates that blockchain and artificial intelligence together can increase the reliability of forensic investigations [7].

Hao Li et al. proposed the BCDT-File framework to provide secure document traceability across multiple organizations. The system combines Hyperledger Fabric with smart contracts to record document lifecycle events on the blockchain, while actual files are stored securely off-chain. This approach improves document verification, version management, and auditability without increasing blockchain storage requirements. The framework offers a practical solution for secure document governance and accountability [8].

M. Imrankhan et al. presented a blockchain-based digital forensic data management system using Ethereum smart contracts to automate forensic operations. The proposed framework simplifies evidence tracking, user authentication, and access control while maintaining a transparent chain of custody. Blockchain ensures that forensic records remain tamper-resistant and permanently available for verification. The study highlights the advantages of decentralized technologies in improving the security of digital investigations [9].

A. Vijayaraj et al. proposed a blockchain-enabled legal documentation system by integrating Ethereum blockchain with the InterPlanetary File System (IPFS). Smart contracts are used to manage document permissions and verify access requests, while IPFS provides secure decentralized storage for legal records. The framework improves document

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

transparency, integrity, confidentiality, and accessibility throughout legal proceedings. This approach offers a secure and efficient method for managing sensitive legal documents [10].

II. METHODOLOGY

The intended system combines blockchain technology and smart contracts to formulate a secure, transparent, and tamper-proof system to manage digital forensic evidence. This system focuses on maintaining the integrity and entirety of evidence with a verifiable and unbroken chain of custody during the forensic investigation.

The first step in the process occurs when the user has authenticated themselves in the system. This is achieved via login using a digital Ethereum wallet. In addition to system login via digital wallet, ease of access is also maintained by the implementation of Role Based Access Control (RBAC) in the system. Under RBAC, users in the system, including but not limited to forensic investigators, forensic experts, and system administrators, can only perform actions corresponding to their defined role. This mitigates the risk of unauthorized access and diminishes abuse of the system.

In the following step, users can register forensic evidence in the system by inputting relevant details of the case and uploading corresponding digital files. Along with the files, the system creates a digital fingerprint in the form of a unique cryptographic hash.

In the interest of secure provenance, it is proposed that each evidence record be represented as a non-fungible token (NFT) conforming to the ERC-721 standards. NFT use enables documented provenance of evidence along with the secure transfer of evidence to authorized users.

Smart contracts automate system functions. Evidence registration, ownership transfer, integrity verification, and audit logging are done automatically if conditions in smart contracts are met. The blockchain timestamps and stores the conditions that are met and the authorized operations. As a result, a permanent and intact record of evidence transfer is created. The history of evidence can be tracked by investigators whenever necessary.

A hybrid storage model is introduced in the framework to optimize the storage and the load on the blockchain. The ownership, timestamp, and transaction details along with the integrity verification are retained on the blockchain, while the actual digital evidence files are kept in off-chain secure storage. This model retains the security and the traceability of the evidence.

Integrity of evidence files is verified by generating a new hash of the evidence and comparing it with the hash stored on the blockchain. If the two hashes are the same, then the evidence is verified to be authentic and the integrity is intact. If the hashes are not the same, then the evidence is possibly compromised and the system notifies investigators of the possible tampering of evidence.

The method integrates many systems, blockchain, smart contracts, NFTs, role-based access control, and hybrid storage, to create a digital forensics management system for evidentiary data built on security and transparency. Various components of the method will be used to build the solution. As the project is currently being developed, the method will help construct a system that is trustworthy, easy to use and scalable, and tamper-proof while retaining the integrity of the evidence through the entire forensics investigation process.

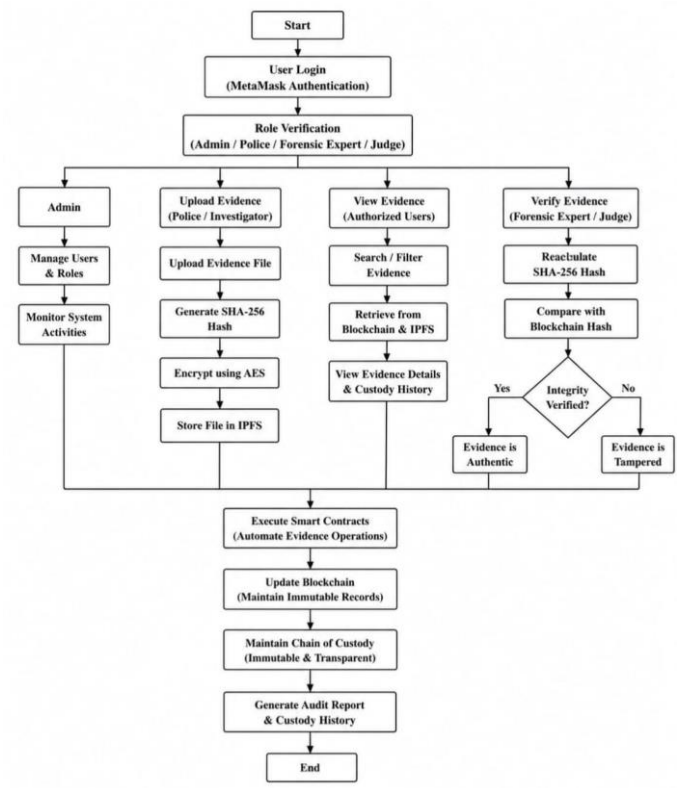

Figure 1: Workflow Diagram

III. EXPECTED OUTCOME

The focus is placed on a digital forensic evidence tracking system that emphasizes security and transparency for the management of digital evidence. The system framework applies a private Ethereum ledger and smart contracts to automate the process of digital evidence management while safeguarding the integrity of all digital evidence management operations.

Along with process integrity, the system incorporates role based access control. Only authorized personnel can access or perform these operations. The system further implements ERC-721 tokens, which provide an NFT framework, for both the digital evidence and the processes for the custody of digital evidence.

The integration of these technologies improves how evidence is managed. Transparency increases, and custody of evidence becomes more trustworthy. The system, therefore, improves the transparency of the digital management of evidence and the custody of evidence is more likely to be trusted. Inherent

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

to the use of blockchain technology, unalterable management audit trails of digital evidence are generated. Thus, all operations carried out through the framework are secure and each instance of forced intrusion is identifiable.

To track ownership of digital evidence, the digital evidence will be saved as NFTs. This will allow transparency and accountability during digital evidence management. NFT contracts will allow custody to be transferred seamlessly, simplifying the overall process. NFT contracts are flexible and programmable. The creation of smart contracts will automate many of the tasks necessary for digital evidence management. This will improve overall efficiency and reduce the number of manual steps required.

A hybrid digital evidence storage framework will be used, in which the evidence is stored off the blockchain, and the metadata of the evidence is stored on the blockchain. This will greatly reduce the costs of creating and maintaining digital evidence on the blockchain. Hybrid digital evidence storage will greatly improve the cost and the capacity of the digital evidence management system for large scale digital evidence cases, which may be large scale digital forensic investigations. This research will implement a system based on blockchain, smart contracts, hybrid storage, and NFTs

CONCLUSION

The decentralized forensic evidence tracking system proposal utilizes blockchain and smart contracts to create a reliable and advanced management system of digitally forensic evidence. It aims to solve and improve traceability of evidence, reliability of a chain of custody, and the unauthorized entry and manipulation of evidence. The combination of wallet authentication, Role-Based Access Control (RBAC), evidence identification through ERC-721 NFTs, and cryptographic hashing, creates a considerably stronger and more secure evidence management system.

One way to automate evidence registration, ownership transfer, and integrity verification is through the use of smart contracts. Further improvement would involve smart contracts for these operations. Besides, the framework employs a hybrid storage model in which all large evidence files are safely stored in an off-chain storage facility, while essential metadata and hash values are stored on-chain. Storage efficiency and scalability are enhanced while maintaining digital evidence's authenticity and integrity.

The current development of the project uses the existing structure to create a practical blockchain based forensic evidence management system. After the system is fully functional, it will allow forensic specialists and investigators to manage digital evidence, using the system throughout the investigation and providing users with a secure and fully auditable tamper-proof system.

The designed framework is enhanced through integrative techniques of forensic analysis, techniques of cognitive and intelligent analytics, a system that could assist investigators in evidence examination and decision-making processes could be designed. This proposed system will focus on digital evidence, advanced analysis techniques, and broader ranges of digital evidence. The system will be designed for effective, efficient, scalable and will meet the needs of forensic investigations.

REFERENCES

[1] F. Nujumudeen, D. M. N. Mubarak, T. Hussain, and P. K. Pinjala, "Adaptive Blockchain Framework for Reliable Authentication and Preservation of Digital Forensic Evidence," Discover Computing, vol. 29, no. 158, 2026.

[2] A. R. Atmakuri et al., "Enhancing Digital Forensic Chain-of-Custody Integrity Through Blockchain," IEEE, 2026.

[3] G. Saranya et al., "Blockchain-Based Evidence Tracking System for Forensic Integrity and Secure Chain of Custody," Proceedings of RFCoN, 2025.

[4] R. Mishra et al., "Blockchain-Enhanced Chain of Custody for Digital Forensic Evidence Management," IEEE, 2025.

[5] L. Loffi, G. L. Camillo, C. M. Westphall, and C. B. Westphall, "Blockchain-Based Chain of Custody for Digital Evidence with Hyperledger Fabric," IEEE, 2025.

[6] B. Varija et al., "Digital Forensic Investigation Model Leveraging Blockchain Technology," 2025.

[7] B.Abisha et al., "PBFT-Integrated Blockchain and AI-Driven Integrity Verification for Digital Forensic Evidence," 2025.

[8] H. Li et al., "Blockchain Smart Contract-Based Traceability and Trustworthy Verification for Secure Digital Documents (BCDT-File)," 2025.

[9] M. Imrankhan et al., "Blockchain Based Digital Forensic Data for Unbreakable Trust and Security," 2024.

[10] A. Vijayaraj et al., "Legal Documentation System Using Blockchain and IPFS," 2024.