

A Secure Blockchain-Based Framework for Digital Evidence Preservation and Verification Using IPFS

Tanmay Sadanshiv¹, Aryan Patil², Shreyash Trimbake³, Shivam Naladkar⁴, Prof. S. H. Thengil⁵

¹Department of Information Technology, Sinhgad College of Engineering, Pune, Maharashtra, India

²Department of Information Technology, Sinhgad College of Engineering, Pune, Maharashtra, India

³Department of Information Technology, Sinhgad College of Engineering, Pune, Maharashtra, India

⁴Department of Information Technology, Sinhgad College of Engineering, Pune, Maharashtra, India

⁵Department of Information Technology, Sinhgad College of Engineering, Pune, Maharashtra, India

Abstract - The growing dependence on digital evidence in criminal investigations, cybercrime analysis, and judicial proceedings has highlighted the need for secure and trustworthy evidence management mechanisms. Conventional evidence storage systems typically depend on centralized infrastructures that are vulnerable to unauthorized modifications, insider threats, and single-point failures. Such limitations can compromise the authenticity and admissibility of digital evidence during legal proceedings.

This paper presents a Blockchain-Based Evidence Preservation Framework that combines Ethereum blockchain technology with the InterPlanetary File System (IPFS) to provide a decentralized, transparent, and tamper-resistant environment for digital evidence management. The proposed system stores evidence metadata and verification records on the blockchain while maintaining the actual evidence files within IPFS. Smart contracts are employed to automate evidence registration, integrity verification, and access control operations.

The framework establishes an immutable chain of custody by recording every evidence-related activity as a blockchain transaction. Furthermore, cryptographic hashing techniques ensure that any unauthorized modification of stored evidence can be immediately detected. The implementation demonstrates improved transparency, traceability, and security when compared with traditional centralized

evidence repositories. Experimental observations indicate that the proposed approach effectively maintains evidence integrity while providing efficient storage and retrieval operations.

Keywords: Blockchain, Digital Forensics, Evidence Preservation, Ethereum, Smart Contracts, IPFS, Chain of Custody, Decentralized Storage, Data Integrity, Cybercrime Investigation.

1. INTRODUCTION

The rapid advancement of information technology and digital communication platforms has transformed the way information is created, stored, and exchanged. Alongside these developments, cybercrimes and digital offenses have increased significantly, resulting in a substantial rise in the volume of electronic evidence generated during investigations. Emails, digital documents, CCTV footage, mobile device data, social media interactions, and cloud-based records frequently serve as critical sources of evidence in modern legal proceedings.

The reliability of digital evidence depends heavily on its authenticity and integrity. Any alteration, deletion, or unauthorized modification of evidence can lead to serious legal consequences and may weaken the credibility of investigative findings. Therefore, maintaining an accurate and verifiable chain of custody is essential throughout the lifecycle of digital evidence. Traditional evidence management systems commonly

rely on centralized databases or cloud-based storage solutions. While these approaches provide accessibility and ease of management, they introduce several challenges, including vulnerability to cyberattacks, unauthorized access, accidental data loss, and limited transparency. Since evidence records are maintained under the control of a central authority, stakeholders must place complete trust in that authority to preserve the integrity of stored information.

Blockchain technology offers a promising alternative to conventional evidence management architectures. As a distributed ledger technology, blockchain provides immutability, transparency, and decentralization. Every transaction recorded on the blockchain is cryptographically linked to previous records, making unauthorized modifications practically infeasible. These characteristics make blockchain particularly suitable for applications requiring strong integrity guarantees and verifiable audit trails.

However, storing large evidence files directly on a blockchain network is inefficient due to storage limitations and transaction costs. To address this challenge, the InterPlanetary File System (IPFS) can be integrated with blockchain infrastructure. IPFS provides decentralized content-addressable storage, allowing large files to be stored efficiently while maintaining cryptographic references on the blockchain.

The proposed framework combines the strengths of blockchain and IPFS to establish a secure digital evidence preservation environment. Metadata associated with evidence records is stored on the Ethereum blockchain through smart contracts, while the actual evidence files are maintained within IPFS. Through this hybrid architecture, the system ensures integrity, transparency, and scalability while minimizing storage overhead.

The primary contributions of this work are

summarized as follows:

- Development of a decentralized framework for digital evidence preservation.
- Integration of Ethereum smart contracts for immutable metadata management.
- Utilization of IPFS for secure and scalable evidence storage.
- Implementation of role-based access mechanisms for authorized stakeholders.
- Establishment of a transparent and verifiable chain of custody.
- Performance evaluation of the framework in terms of security and operational efficiency.

The remainder of this paper is organized as follows. Section 2 presents the literature review and discusses related research. Section 3 describes the problem statement and system objectives. Subsequent sections explain the proposed architecture, implementation methodology, experimental observations, and future research directions.

2. LITERATURE REVIEW

The application of blockchain technology in digital forensics and evidence management has gained considerable attention in recent years. Researchers have explored various approaches to improve evidence integrity, transparency, and traceability through decentralized technologies.

Several studies have investigated the use of blockchain for preserving forensic evidence records. These approaches leverage blockchain's immutable ledger structure to create tamper-resistant audit trails that can be used during judicial proceedings. The recorded transactions provide chronological documentation of evidence-related activities, thereby strengthening the chain of custody.

Researchers have also examined the integration of cryptographic techniques with blockchain networks to enhance evidence security. Encryption-based solutions

ensure confidentiality while blockchain mechanisms preserve integrity. Although such systems provide strong protection against unauthorized access, many implementations focus primarily on security without addressing scalability concerns associated with large evidence files.

The emergence of decentralized storage technologies has further expanded research opportunities in this domain. The InterPlanetary File System (IPFS) has been widely adopted as a complementary technology for blockchain-based systems. IPFS allows large multimedia evidence files to be stored outside the blockchain while maintaining content authenticity through cryptographic hashes. This significantly reduces blockchain storage requirements and improves overall system efficiency.

Another area of investigation involves chain-of-custody management. Maintaining a verifiable record of evidence ownership and handling activities is essential in forensic investigations. Blockchain-based chain-of-custody frameworks provide transparent documentation of evidence transfers, minimizing the possibility of record manipulation and enhancing legal reliability.

Despite the progress achieved by existing solutions, several limitations remain. Many proposed systems focus exclusively on evidence storage without providing practical user interfaces for law enforcement agencies. Some frameworks offer decentralized storage but lack effective access control mechanisms. Others provide secure record management but fail to address scalability and usability requirements necessary for real-world deployment.

The framework proposed in this research attempts to bridge these gaps by combining blockchain-based metadata preservation, decentralized IPFS storage, smart-contract-driven management, and controlled evidence access within a unified architecture. The objective is to create a practical and secure platform capable of supporting modern digital forensic

investigations while preserving evidence integrity throughout its lifecycle.

3. SYSTEM OVERVIEW

3.1 Problem Statement

The increasing use of digital devices and online communication platforms has resulted in a significant growth in the volume of electronic evidence collected during criminal investigations and judicial proceedings. Such evidence includes emails, digital documents, surveillance footage, multimedia files, mobile device records, and network logs. Preserving the authenticity and integrity of these records is essential for ensuring their admissibility in courts of law.

Existing evidence management solutions primarily rely on centralized databases and cloud-based infrastructures. Although these systems provide convenience and accessibility, they remain vulnerable to unauthorized modifications, insider threats, accidental deletion, and single-point failures. Furthermore, maintaining a trustworthy chain of custody often requires extensive manual documentation, increasing the likelihood of human errors and record inconsistencies.

Another major challenge is ensuring transparency in evidence handling. In centralized environments, stakeholders must depend on a trusted authority to maintain records accurately. Any compromise of the central repository can raise doubts regarding the authenticity of evidence and may negatively impact legal proceedings.

Therefore, there is a need for a secure, decentralized, and tamper-resistant framework capable of preserving digital evidence while providing transparent verification and accountability mechanisms. The proposed blockchain-based framework addresses these challenges through immutable record keeping, decentralized storage, and cryptographic verification.

3.2 Motivation

Digital evidence has become a critical component of modern forensic investigations. As cybercrime incidents continue to rise, law enforcement agencies and judicial organizations require reliable mechanisms to preserve evidence throughout its lifecycle.

The motivation behind this work originates from the limitations observed in conventional evidence management systems. Existing approaches often struggle to guarantee long-term integrity, transparency, and resistance against unauthorized modifications. In addition, the growing size of multimedia evidence presents challenges related to storage efficiency and scalability.

Blockchain technology offers a unique opportunity to establish trust without relying on centralized authorities. By combining blockchain with decentralized storage technologies such as IPFS, evidence can be preserved in a secure and verifiable manner. This research aims to leverage these technologies to create a practical framework capable of improving digital evidence management practices.

3.3 Objectives

The primary objective of the proposed framework is to design and implement a secure platform for preserving and verifying digital evidence using blockchain and decentralized storage technologies.

Specific objectives include:

1. To develop a decentralized evidence management framework that eliminates dependence on centralized repositories.
2. To utilize Ethereum smart contracts for maintaining immutable evidence records and transaction histories.
3. To integrate IPFS for efficient storage and retrieval of large digital evidence files.
4. To establish a secure chain of custody through blockchain-based transaction logging.

5. To implement role-based access mechanisms for authorized users.

6. To provide cryptographic verification for detecting evidence tampering.

7. To evaluate the framework in terms of security, transparency, and operational efficiency.

3.4 Proposed System

The proposed framework combines Ethereum blockchain technology and the InterPlanetary File System (IPFS) to create a decentralized environment for evidence preservation and verification.

Whenever an evidence file is submitted to the system, it is first uploaded to IPFS. The storage process generates a unique content identifier (CID), which acts as a cryptographic reference for the file. A hash value is subsequently generated and stored on the Ethereum blockchain along with associated metadata such as evidence ID, timestamp, uploader information, and case details.

Smart contracts manage evidence registration, access control, and verification operations. Every action performed within the system is recorded as a blockchain transaction, ensuring transparency and immutability.

During evidence verification, the stored blockchain hash is compared with the hash generated from the retrieved file. If both values match, the integrity of the evidence is confirmed. Any modification to the file results in a mismatch, immediately indicating possible tampering.

The proposed framework provides the following advantages:

- Decentralized evidence preservation
- Tamper-resistant record management
- Transparent chain of custody
- Secure verification mechanisms
- Improved scalability through off-chain storage
- Enhanced accountability and auditability

3.5 System Architecture

The architecture of the proposed framework consists of four major layers:

A. Presentation Layer

The presentation layer provides a web-based interface through which authorized users interact with the system. Functions available within this layer include evidence upload, retrieval, verification, and report generation.

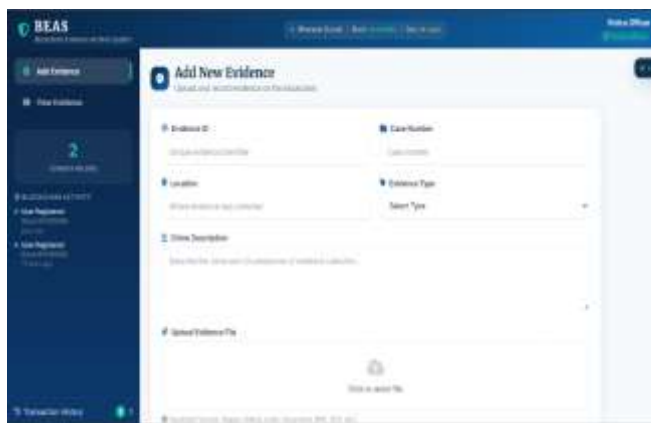


Fig 1: Project Dashboard Police

The dashboard provides centralized access to all evidence-related operations and allows users to monitor evidence records efficiently.

B. Application Layer

The application layer contains the business logic responsible for processing user requests and coordinating interactions between blockchain and storage components.

Major functions include:

- Evidence registration
- Metadata management
- Access validation
- Verification processing
- Transaction monitoring

C. Blockchain Layer

The blockchain layer consists of Ethereum smart contracts responsible for maintaining immutable records of evidence transactions.

Key responsibilities include:

- Evidence metadata storage

- Hash preservation
- Transaction recording
- Chain of custody management
- Access control enforcement

Every transaction performed within the system is permanently recorded on the blockchain, creating an auditable trail of evidence activities.

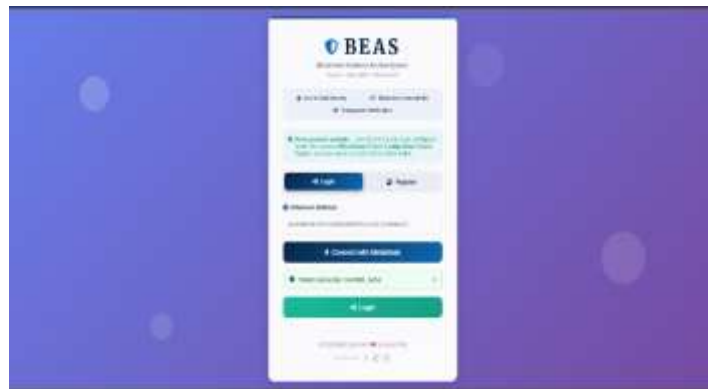


Fig 2: MetaMask Authentication Screen

D. Storage Layer

The storage layer utilizes IPFS to store digital evidence files in a decentralized manner.

Instead of storing large files directly on the blockchain, the framework stores evidence within IPFS and records only cryptographic references on-chain.

Benefits include:

- Reduced blockchain storage requirements
- Improved scalability
- Faster file retrieval
- Decentralized file availability



Fig 3: Evidence Upload Interface

3.6 Workflow of the Proposed Framework

The operational workflow of the framework is illustrated through the following sequence:

Step 1: User Authentication

Authorized personnel access the platform through blockchain wallet authentication using MetaMask.

Step 2: Evidence Submission

The user uploads digital evidence through the web application interface.

Step 3: IPFS Storage

The uploaded evidence is stored within IPFS, generating a unique content identifier.

Step 4: Blockchain Registration

The generated IPFS hash along with evidence metadata is stored on the Ethereum blockchain using smart contracts.

Step 5: Evidence Retrieval

Authorized users can retrieve evidence using the associated content identifier and blockchain record.

Step 6: Integrity Verification

The system compares current and stored cryptographic hashes to verify evidence authenticity.

Step 7: Audit Trail Generation

All activities are logged on the blockchain, providing a transparent and immutable chain of custody.



Fig 4: Evidence Verification Screen

3.7 Technology Stack

The implementation utilizes a combination of modern web, blockchain, and decentralized storage technologies.

Frontend Technologies:

- HTML5
- CSS3
- JavaScript

Backend Technologies:

- Node.js
- Express.js

Blockchain Technologies:

- Ethereum
- Solidity
- Web3.js
- Ganache

Storage Technologies:

- IPFS
- Pinata Gateway

Authentication:

- MetaMask Wallet

Development Tools:

- Visual Studio Code
- GitHub

The selected technology stack provides flexibility, scalability, and compatibility with modern blockchain ecosystems while supporting efficient evidence preservation and verification operations.

4. APPLICATIONS OF THE PROPOSED FRAMEWORK

The proposed Blockchain-Based Evidence Preservation Framework can be applied across multiple sectors where data authenticity, traceability, and integrity are critical requirements. By combining blockchain technology with decentralized storage, the framework provides a reliable mechanism for preserving digital records and ensuring accountability.

4.1 Law Enforcement and Criminal Investigations

One of the primary applications of the framework is within law enforcement agencies. Digital evidence such as CCTV recordings, mobile device extractions, email communications, call logs, and forensic reports

can be securely preserved within the system. Since every transaction is recorded on the blockchain, investigators can maintain a transparent and verifiable chain of custody throughout the investigation process.

4.2 Digital Forensics Laboratories

Forensic laboratories frequently handle large volumes of digital evidence collected from multiple cases. The proposed framework allows forensic analysts to securely archive evidence while preserving its integrity. Cryptographic verification mechanisms help ensure that evidence remains unchanged from acquisition to courtroom presentation.

4.3 Judicial and Legal Systems

Courts require reliable methods to verify the authenticity of digital evidence submitted during trials. The proposed framework provides immutable evidence records and complete audit trails, enabling judges and legal professionals to verify evidence history and ownership with confidence.

4.4 Cybercrime Investigation Units

Cybercrime divisions can utilize the framework to preserve network logs, malware samples, digital communications, and other electronic artifacts. The decentralized architecture minimizes the risk of unauthorized modifications and improves trust in investigative findings.

4.5 Academic Certificate Verification

Educational institutions can adapt the framework for secure certificate management. Academic records, degree certificates, and transcripts can be stored and verified through blockchain-based mechanisms, reducing the possibility of forgery and unauthorized modifications.

4.6 Intellectual Property Protection

Organizations and content creators can use the framework to preserve ownership records for patents,

copyrights, trademarks, and creative works. Blockchain-based timestamping provides proof of ownership and creation dates, strengthening intellectual property protection.

4.7 Healthcare Record Management

Hospitals and healthcare providers can utilize similar mechanisms to preserve sensitive patient records. The framework can ensure secure storage, controlled access, and complete auditability of medical information while maintaining data integrity.

4.8 Corporate Compliance and Auditing

Businesses can employ the framework for preserving compliance documents, audit records, contracts, and financial reports. The immutable nature of blockchain records increases transparency and simplifies auditing procedures.

5. CONCLUSION

The increasing dependence on digital evidence within investigative and judicial processes necessitates robust mechanisms for preserving authenticity, integrity, and accountability. Traditional centralized evidence management systems often face challenges related to unauthorized access, data manipulation, limited transparency, and single-point failures. These limitations can compromise the credibility and admissibility of digital evidence.

This research presented a Blockchain-Based Evidence Preservation Framework that integrates Ethereum blockchain technology with the InterPlanetary File System (IPFS) to establish a secure and decentralized evidence management environment. The proposed framework records evidence metadata and transaction histories on the blockchain while storing actual evidence files within IPFS. Through the use of cryptographic hashing and smart contracts, the system

provides tamper-resistant storage, transparent audit trails, and verifiable chain-of-custody records.

The implementation demonstrates that combining blockchain and decentralized storage technologies can significantly enhance the security and reliability of digital evidence preservation. The framework successfully eliminates dependence on centralized repositories while ensuring evidence integrity throughout its lifecycle. Furthermore, role-based access mechanisms and transaction transparency strengthen accountability among stakeholders involved in evidence handling.

The obtained results indicate that the proposed approach offers a practical and scalable solution for modern forensic environments. The framework can support law enforcement agencies, forensic laboratories, judicial institutions, and other organizations requiring secure digital record preservation.

Overall, the research validates the effectiveness of blockchain-enabled evidence management and highlights its potential for transforming digital forensic practices in future investigative ecosystems.

6. FUTURE SCOPE

Although the proposed framework successfully addresses many challenges associated with digital evidence preservation, several opportunities exist for further enhancement and expansion.

6.1 Integration with Public Blockchain Networks

Future implementations may migrate from local blockchain environments to public or consortium blockchain networks. Such deployments can provide stronger decentralization, wider accessibility, and enhanced trust among participating organizations.

6.2 Biometric-Based Authentication

The incorporation of biometric authentication methods such as fingerprint recognition, facial recognition, or iris verification can strengthen user authentication and

reduce the risk of unauthorized access.

6.3 Artificial Intelligence for Evidence Classification

Machine learning and artificial intelligence techniques can be integrated to automatically categorize evidence files based on content type, case relevance, and risk levels. This would improve evidence organization and retrieval efficiency.

6.4 Decentralized Identity (DID) Integration

Future versions of the framework may leverage decentralized identity solutions to provide more secure and privacy-preserving authentication mechanisms for investigators, forensic experts, and judicial authorities.

6.5 Mobile Platform Support

Developing dedicated mobile applications would enable authorized users to upload, verify, and monitor evidence records directly from smartphones and tablets while maintaining blockchain security standards.

6.6 Advanced Encryption Techniques

Additional cryptographic mechanisms such as attribute-based encryption and zero-knowledge proofs can be integrated to further enhance confidentiality and privacy.

6.7 Cross-Agency Collaboration

The framework can be expanded into a nationwide or multi-agency platform that enables secure evidence sharing among police departments, forensic laboratories, and judicial organizations while preserving ownership and accountability.

6.8 Real-Time Monitoring and Analytics

Future research may incorporate advanced analytics dashboards capable of monitoring evidence activity, detecting suspicious access attempts, and generating real-time audit reports.

REFERENCES

- [1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
- [2] Juan Benet, "IPFS: Content Addressed, Versioned, Peer-to-Peer File System," Protocol Labs White Paper, 2014.
- [3] Gavin Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Yellow Paper, 2014.
- [4] Melanie Swan, Blockchain: Blueprint for a New Economy, O'Reilly Media, 2015.
- [5] M. Crosby, P. Pattanayak, S. Verma and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," Applied Innovation Review, vol. 2, pp. 6–19, 2016.
- [6] A. Dorri, S. S. Kanhere and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 451–476, 2020.
- [7] M. Conti, E. S. Kumar, C. Lal and S. Ruj, "A Survey on Security and Privacy Issues of Blockchain Technology," IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 3416–3452, 2020.
- [8] "Blockchain-Based Digital Evidence Management Framework Using IPFS," International Journal of Computer Science and Information Security, vol. 20, no. 9, pp. 101–108, 2022.
- [9] "A Study on Blockchain-Enabled Judicial Evidence Preservation Systems," IEEE Access, vol. 12, pp. 45390–45401, 2024.
- [10] "Management of Digital Evidence Chain of Custody Using Blockchain Technology," International Journal of Advanced Computer Science and Applications, vol. 16, no. 2, pp. 112–120, 2025.
- [11] T. Sadanshiv, A. Patil, S. Trimbake, S. Naladkar, and S. H. Thengil, "Decentralized Digital Evidence Archival System with Blockchain and IPFS," International Journal of Scientific Research in Engineering and Management (IJSREM), vol. 09, no. 11, Nov. 2025, DOI: 10.55041/IJSREM53558.