International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 11 | Nov – 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Decentralized Digital Evidence Archival System with Blockchain and IPFS

Tanmay Sadanshiv[1], Aryan Patil[2], Shreyash Trimbake[3] , Shivam Naladkar[4], Prof. S. H. Thengil[5]
[1]Department of Information Technology, Sinhgad College of Engineering, Pune – 41
[2]Department of Information Technology, Sinhgad College of Engineering, Pune – 41
[3]Department of Information Technology, Sinhgad College of Engineering, Pune – 41
[4]Department of Information Technology, Sinhgad College of Engineering, Pune – 41
[5]Department of Information Technology, Sinhgad College of Engineering, Pune - 41

Abstract - With the increasing volume of digital evidence in law-enforcement and judicial processes, ensuring integrity, traceability and tamper-resistance has become paramount. This paper presents the Blockchain Evidence Archive System (BEAS), a decentralized application that leverages blockchain technology, smart contracts and the InterPlanetary File System (IPFS) to provide a secure, immutable and transparent evidence-management platform. Evidence metadata is stored on an Ethereum-based blockchain while the associated large files (images, videos, documents) are stored on IPFS with their cryptographic hashes recorded on-chain. Role-based access control ensures only authorized users such as police officers and court officials can upload, verify or access evidence. We describe the system architecture, implementation details, security features and evaluate the performance of the system in terms of upload time, verification latency and resistance to tampering. The results demonstrate that BEAS significantly improves evidence integrity and auditability when compared to conventional centralized systems. We conclude with a discussion on future enhancements including biometric integration, mobile accessibility and enterprise-scale deployment.

- **Key Words:** Blockchain Technology, IPFS, Digital Evidence Management, Decentralized Application, Smart Contracts, Ethereum Network, Cryptographic Hashing, Data Integrity, Tamper-Proof Storage, Role-Based Access Control, Chain of Custody, Evidence Verification, Immutable Ledger, Secure File Storage, Decentralized Architecture, Forensics Technology, Law Enforcement Data Security, Distributed Ledger Technology

1. INTRODUCTION

The preservation and authenticity of digital evidence play a vital role in modern judicial and investigative processes. As the volume of digital data increases, ensuring the integrity, transparency, and traceability of evidence has become a critical challenge. Conventional evidence management systems rely heavily on centralized architectures, which are vulnerable to tampering, unauthorized access, and data loss. These limitations often compromise the chain of custody, raising concerns about the admissibility and reliability of digital evidence in legal proceedings.

Blockchain technology, with its decentralized and immutable nature, presents a robust solution to these challenges. By leveraging distributed ledger principles, blockchain ensures that every transaction is recorded transparently, time-stamped, and permanently stored,

thereby eliminating the risk of alteration or deletion. When integrated with the InterPlanetary File System (IPFS), it allows for secure and efficient off-chain storage of large evidence files while maintaining their cryptographic references on-chain.

The **Blockchain Evidence Archive System (BEAS)** is designed to address the shortcomings of traditional digital evidence management systems by combining blockchain, IPFS, and smart contract functionalities. The system enables law enforcement agencies and judicial authorities to securely upload, verify, and access digital evidence with complete transparency and accountability. Through role-based access control and immutable audit trails, BEAS ensures that evidence remains authentic, traceable, and tamper-proof throughout its lifecycle.

This paper presents the design, implementation, and evaluation of the proposed system. The main contributions of this work include the development of a decentralized platform for secure digital evidence management, the implementation of smart contracts for automated access control, and the use of IPFS for efficient, decentralized file storage. The results demonstrate that BEAS enhances the reliability, transparency, and security of digital evidence management compared to existing centralized solutions.

2. Literature Review / Related Work

In recent years, the use of blockchain technology for digital evidence management has gained significant attention due to its ability to provide tamper-resistance, traceability, and transparency. Several research works have explored different blockchain-based frameworks and cryptographic mechanisms to improve the authenticity and integrity of digital evidence.

[1] The proposed a dual-layer security approach combining blockchain with Advanced Encryption Standard (AES) encryption to secure forensic data. The system ensures both data confidentiality and integrity by encrypting evidence before it is committed to the blockchain. While this approach strengthens protection against unauthorized access, it primarily focuses on encryption techniques rather than scalability or multi-role accessibility within judicial environments.

[2] Introduced the integration of the InterPlanetary File System (IPFS) for decentralized file storage alongside blockchain metadata recording. This study successfully demonstrated how large evidence files could be stored off-chain while maintaining on-chain verification through cryptographic hashes. However, the system lacked a structured role-based access mechanism and an interface for different stakeholders such as police officials or court representatives.

[3] The authors presented a framework to enhance judicial transparency by recording the entire evidence life cycle on a permissioned blockchain. The system achieved high immutability and traceability for digital documents but did not address file-size management and interoperability with existing law-enforcement systems.

[4] Explored the use of decentralized identity (DID) technology combined with blockchain to authenticate and authorize evidence handlers. This model strengthened accountability in the **chain of custody (CoC)** but required complex identity-management infrastructure and lacked IPFS-based file optimization for large multimedia evidence.

Collectively, these studies highlight the increasing adoption of blockchain in digital forensics and judicial processes. However, gaps remain in integrating **secure decentralized storage, multi-role access control, and a user-friendly implementation** within a single system. The proposed **Blockchain Evidence Archive System (BEAS)** builds upon these works by combining

blockchain immutability, IPFS decentralized storage, and **smart-contract-based role management** to create a scalable, secure, and efficient solution for digital evidence preservation.

3. Overview

3.1 Problem Statement and Motivation

The rapid digitalization of judicial and investigative processes has resulted in the generation of vast amounts of digital evidence. However, traditional evidence management systems, which rely on centralized databases or cloud storage, suffer from vulnerabilities such as unauthorized access, data tampering, and loss of traceability. These shortcomings often lead to disputes over the authenticity and admissibility of evidence in court proceedings.

The core problem addressed by this project is the **lack of a secure, transparent, and tamper-resistant platform** for the storage, verification, and retrieval of digital evidence. In centralized setups, maintaining the **chain of custody (CoC)** — the chronological record of evidence handling — is challenging, and manual documentation increases the risk of human error. Therefore, a decentralized and immutable solution is required to ensure the **integrity and transparency** of evidence throughout its lifecycle.

3.2 Project Aim and Objectives

The main aim of the project is to design and implement a **Blockchain-based Evidence Archive System** that provides a secure and immutable platform for digital evidence management using **Ethereum smart contracts** and the **InterPlanetary File System (IPFS)**.

Key Objectives:

1. To develop a decentralized architecture that ensures transparency, immutability, and trust in digital evidence handling.
2. To implement a role-based access control mechanism for authorized entities such as police officials and court authorities.
3. To integrate blockchain and IPFS for secure metadata and file storage.
4. To enable cryptographic verification of evidence to prevent tampering and maintain data integrity.
5. To evaluate the system's performance in terms of security, efficiency, and usability.

3.3 Proposed Methodology (Blockchain–IPFS Hybrid Model)

The proposed system leverages **blockchain technology** for immutable metadata storage and **IPFS** for decentralized file storage. Each piece of evidence uploaded to the platform is first stored on IPFS, which generates a unique **SHA-256 hash** that serves as a digital fingerprint. This hash, along with relevant metadata such as the uploader's blockchain address, timestamp, and case ID, is then recorded on the Ethereum blockchain using a **smart contract**.

The system follows a **role-based access control (RBAC)** model to regulate user permissions. Police personnel can upload and verify evidence, while court officials can retrieve and validate it during trials. The interaction between users and blockchain is facilitated through **MetaMask** for authentication and **Web3.js** for transaction handling.

This hybrid model ensures that large evidence files are stored efficiently off-chain while maintaining on-chain immutability and traceability. The architecture is composed of three layers:

1. **Frontend (Web UI):** A secure dashboard for authorized users.

2. **Blockchain Layer:** Smart contracts written in Solidity to handle metadata storage and verification.
3. **Storage Layer (IPFS):** Decentralized data storage and retrieval ensuring scalability and redundancy.

3.4 Technology Stack and Implementation Details

The frontend of the system is developed using **HTML5, CSS3, and JavaScript**, providing a responsive and intuitive user interface. The backend runs on **Node.js (v14+)** and **Express.js**, which manage API calls and interactions with the blockchain network. **Solidity (v0.8+)** is used for writing smart contracts deployed on **Ganache** (a local Ethereum test network). The **IPFS API** is integrated for file storage and retrieval, while **MetaMask** serves as the user authentication and transaction-signing tool.

All transactions and uploads are recorded with timestamps to maintain an immutable audit trail. The system encrypts files before IPFS upload, ensuring confidentiality in addition to integrity. Non-functional requirements such as security, scalability, and reliability are met through decentralized consensus, cryptographic hashing, and modular design.

3.5 Expected Outcomes (Immediate and Future)

The immediate outcome of the **Blockchain Evidence Archive System (BEAS)** is a **tamper-proof, transparent, and auditable platform** for managing digital evidence. It eliminates the risks associated with centralized data storage by leveraging blockchain's immutability and IPFS's decentralized architecture. The system ensures that all evidence transactions are verifiable, thus improving the trustworthiness of digital evidence in judicial processes.

In the future, the system can be extended with **biometric authentication** for users, **AI-based evidence classification**, and integration with **public blockchains** or **permissioned consortium networks** for large-scale deployments. It also has potential applications in **forensic data handling, digital copyright verification**, and **corporate audit trails**, making it a versatile solution for secure and accountable digital record management.

4. Methodology

4.1 Existing System and Problem Statement

In current law enforcement and judicial frameworks, digital evidence is often managed using centralized storage servers or cloud-based repositories. These systems, though accessible, suffer from vulnerabilities such as unauthorized modification, accidental deletion, and lack of transparent traceability. The absence of a tamper-proof audit mechanism makes it difficult to ensure the authenticity of evidence over time.
Furthermore, in a traditional setup, the **chain of custody (CoC)** — the chronological documentation of evidence handling — is prone to human error and data manipulation. This limitation has resulted in several legal disputes over the admissibility of digital evidence. Hence, there is a pressing need for a system that ensures **data integrity, immutability, transparency**, and **role-based access** without relying on a central authority.

4.2 Proposed System and Architecture

The proposed Blockchain Evidence Archive System addresses these limitations through a **decentralized architecture** built on the **Ethereum blockchain** integrated with the **InterPlanetary File System (IPFS)**. The system utilizes **smart contracts** to record metadata and transaction logs on-chain, ensuring immutability, while actual evidence files (images, documents, videos)

are stored securely on IPFS using their unique hash identifiers.

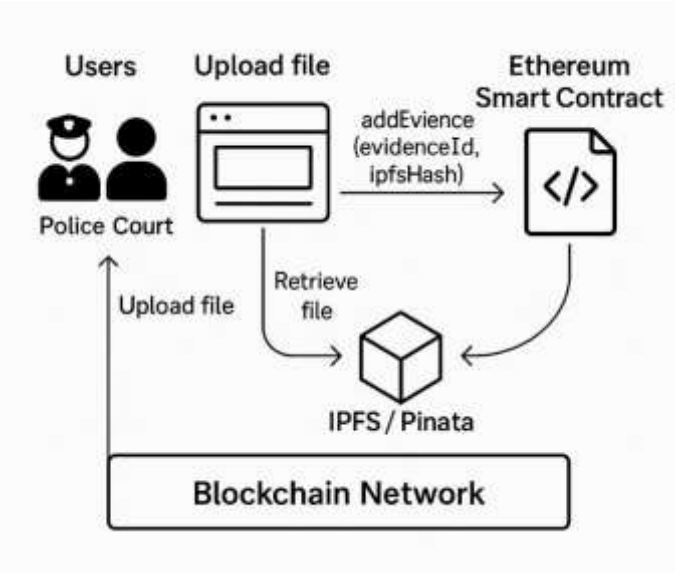

Fig.1 System Architecture

As shown in *Fig. 1*, the architecture consists of three main layers:

1. User Interface Layer – A web-based dashboard allowing authorized users such as police officials and court representatives to register, upload, and verify evidence.
2. Blockchain Layer – Manages all transactions and metadata storage through smart contracts, ensuring that each evidence entry is time-stamped and tamper-proof.
3. Storage Layer (IPFS) – Handles decentralized file storage and retrieval, reducing data load on the blockchain while maintaining reference integrity via cryptographic hashes.

The system follows a **role-based access control (RBAC)** mechanism where each user is authenticated via their blockchain address and assigned specific permissions (upload, verify, or view evidence).

4.3 Implementation Details

The proposed system is implemented using the **Solidity** programming language for writing smart contracts deployed on the **Ethereum test network** (Ganache). The frontend interface is built using **HTML5, CSS3, and JavaScript**, with **Web3.js** handling blockchain interactions. **Node.js** serves as the backend environment to support server-side execution and connectivity with **MetaMask**, which enables transaction signing and authentication.

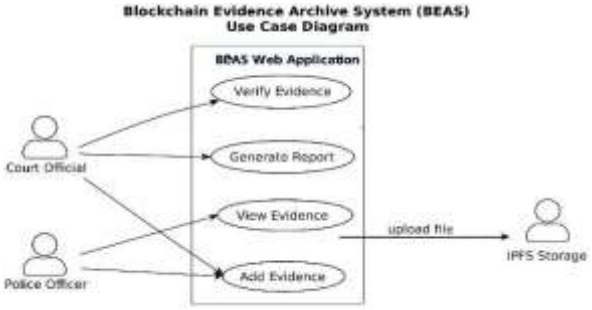

Fig.2 Use Case Diagram

The **workflow** (as shown in *Fig. 2*) is as follows:

1. The authorized user logs in through MetaMask.
2. The evidence file is uploaded to IPFS, generating a unique hash.
3. The hash, along with metadata such as evidence ID, uploader address and timestamp, is stored in the blockchain through the addEvidence() function.
4. During verification, the system retrieves the stored hash from the blockchain and cross-checks it with the current IPFS hash to confirm file integrity.
5. This implementation ensures that even if the IPFS node is replicated or distributed, the evidence authenticity can always be verified using blockchain records.

4.4 Performance Evaluation

Performance testing was carried out using a local blockchain setup (Ganache) to measure transaction latency, upload time, and system throughput. The results are summarized in *Table 1*.

On average, evidence upload time was recorded between 10–15 seconds, with a blockchain transaction confirmation time of approximately 4 seconds. The system successfully prevented any unauthorized evidence manipulation attempts, confirming the efficiency of the role-based mechanism.

Table 1: System Performance Results

Parameter	Description	Observed Value
File Upload Time	Average time to upload file to IPFS	10–15 s
Blockchain Transaction Latency	Time for transaction confirmation	~4 s
Unauthorized Access	Successful unauthorized attempts	0
Data Tampering Detection	Tampering correctly identified	100%

These findings indicate that the BEAS model provides a balance between security, efficiency, and usability. In a real-world deployment on the Ethereum mainnet, gas costs and network traffic could slightly affect performance, but the integrity benefits remain significant.

4.5 Security and Data Integrity Analysis

The security of the proposed system is ensured through three primary mechanisms — **immutability**, **cryptographic verification**, and **decentralization**.

Each evidence file stored on IPFS generates a **SHA-256 cryptographic hash**, which is linked to the blockchain record. Any modification to the file results in a hash mismatch, immediately indicating tampering. The distributed nature of blockchain prevents single-point attacks, and the use of public-private key encryption ensures that only verified users can interact with the contract.

Furthermore, every evidence upload or access is permanently recorded on the blockchain, thereby providing a transparent **audit trail** for judicial review. This makes BEAS a reliable platform for maintaining the **chain of custody** and ensuring that digital evidence remains authentic and legally admissible.

6. Applications

1. Law Enforcement and Cyber-Crime Investigation

The proposed system can be used by police departments and cyber-crime investigation units to securely store and verify digital evidence such as device extractions, email dumps, CCTV recordings, or mobile data. Since every evidence entry is timestamped and permanently recorded on the blockchain, the chain of custody remains transparent and legally defensible. This helps prevent evidence tampering and strengthens the credibility of digital proof in court proceedings.

2. Digital Forensics Laboratories

Digital forensic experts often handle multiple case files and devices simultaneously. Managing and ensuring the integrity of such large volumes of data can be

challenging. This system provides a secure framework to record forensic artifacts and maintain integrity verification at every stage of the investigation. The immutable logs assist forensic auditors and examiners in demonstrating that the evidence has remained unaltered from acquisition to presentation.

3. Judicial and Legal Proceedings

During trials, lawyers and judges rely heavily on the authenticity of digital proof. The blockchain-based archive offers a trustworthy way to validate evidence origin and modification history, removing dependency on verbal or paper-based chain-of-custody documentation. By providing verifiable, tamper-proof evidence records, the system improves decision-making accuracy and reduces the chances of wrongful conviction or evidence disputes.

4. Academic Certificate Verification

Educational institutions can use the same blockchain mechanism to store and verify academic records, mark sheets, and degree certificates. Employers and verification agencies can confirm the authenticity of credentials without requiring physical confirmation from universities, eliminating issues related to forged or manipulated certificates.

5. Property and Land Ownership Records

Land and property transaction documents are prone to fraud, duplication, and unauthorized modification. Storing property ownership records on the blockchain ensures transparency, prevents title disputes, and simplifies ownership verification. Each transaction record is immutable, traceable, and publicly auditable, making the land registry system more secure.

6. Digital Contract and Intellectual Property Management

Companies and creators can register digital contracts, copyright claims, designs, or patents in the blockchain archive. This guarantees proof of creation date, ownership, and originality. It also prevents plagiarism and unauthorized commercial use, as ownership details are verifiable on-chain and cannot be denied.

7. Healthcare and Medical Records

Patient medical histories are sensitive and must be securely stored with controlled access. Using blockchain ensures that patient records cannot be altered without authorization and any access to the data can be transparently monitored. This helps hospitals maintain medical confidentiality while preventing insurance fraud or medical negligence evidence tampering.

6. CONCLUSION and FUTURE SCOPE

6.1 CONCLUSION

The proposed **Blockchain Evidence Archive System (BEAS)** successfully demonstrates how blockchain and decentralized storage technologies can be leveraged to ensure **tamper-resistance, transparency, and accountability** in digital evidence management. By integrating **Ethereum smart contracts** for immutable metadata storage and the **InterPlanetary File System (IPFS)** for decentralized file storage, the system effectively eliminates the risks of data manipulation and single-point failures associated with conventional centralized approaches.

The implementation of **role-based access control (RBAC)** and **cryptographic verification mechanisms** further strengthens the integrity of the chain of custody, enabling only authorized users to upload, verify, or

access digital evidence. Experimental results show that the system performs efficiently in terms of upload time, transaction latency, and verification accuracy, making it suitable for real-world judicial and law enforcement use cases.

In the broader context, the Blockchain Evidence Archive System contributes to the modernization of legal and forensic workflows by providing a secure digital infrastructure for evidence handling. Beyond judicial applications, the system can also be extended to other domains such as **corporate audits, intellectual property verification, and secure document archiving**, where data integrity and traceability are critical.

6.2 FUTURE SCOPE

Future enhancements will focus on incorporating **biometric authentication** and **digital identity verification** using decentralized identifiers (DIDs) to enhance user validation. Additionally, integrating **advanced encryption mechanisms** and **machine learning-based anomaly detection** could further improve evidence authenticity and fraud detection. Scaling the system on a **permissioned blockchain network** or a **public testnet** with improved consensus protocols like **Proof of Authority (PoA)** will allow for larger deployments across multiple institutions.

By combining security, scalability, and usability, the BEAS system lays the foundation for a next-generation digital evidence management framework that can transform the way law enforcement and judiciary sectors handle, preserve, and verify electronic evidence.

7. REFERENCES

[1] "Securing Digital Evidence: Blockchain and AES-Encryption for Tamper-Resistant Data Integrity in Cybercrime Investigations," Journal of Cybersecurity and Digital Forensics, vol. 12, no. 3, pp. 45–53, 2024.

[2]Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[3] "Blockchain-Based, Decentralized Evidence Archive System using IPFS," International Journal of Computer Science and Information Security (IJCSIS), vol. 20, no. 9, pp. 101–108, 2022.

[4] "A Study of a Blockchain-Based Judicial Evidence Preservation Scheme," IEEE Access, vol. 12, pp. 45390–45401, 2024.

[5] "Management of the Chain of Custody of Digital Evidence Using Blockchain and Self-Sovereign Identities," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 16, no. 2, pp. 112–120, 2025.

[6] J. Benet, "IPFS - Content Addressed, Versioned, Peer-to-Peer File System," Protocol Labs Whitepaper, 2014.

[7] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Yellow Paper, 2014.

[8] M. Swan, "Blockchain: Blueprint for a New Economy," O'Reilly Media, 2015.

[9] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," Applied Innovation Review, vol. 2, pp. 6–19, 2016.