

Evidence Management System Using Blockchain

Rajlaskhmi ¹k, Sakshi Gaikwad², Abhishek Ponde³, Vivek Bhogade⁴, Vikram Chavan⁵

^{1, 2, 3, 4} Dept of Computer Engineering

⁵ Assistant professor, Dept of Computer Engineering

^{1, 2, 3, 4, 5} Sinhgad Institute of Technology, Lonavala, India.

Abstract- *The study suggests a Decentralised Evidence Management System that uses distributed storage and blockchain technology to protect, authenticate, and expedite the lifetime of digital forensic evidence. This solution fixes flaws that can jeopardise court proceedings, such as tampering, illegal access, and ineffective evidence tracking. It combines the InterPlanetary File System (IPFS) for off-chain storage and employs a two-tier blockchain topology that divides static data from dynamic data. By automating access control, smart contracts strengthen auditability and the chain of custody. The design is tamper-proof and fault-tolerant, and it has secure interfaces for judicial and law enforcement stakeholders. The method is a transparent, safe, and effective way to address contemporary digital forensic issues since it increases trust, accountability, and transparency in the processing of digital evidence.*

Keywords- IPFS, evidence, system, blockchain, digital, data.

I. INTRODUCTION

The growing prevalence of cybercrime and digital evidence in modern investigations necessitates robust and tamper-proof evidence management solutions. Traditional centralized evidence handling systems face several challenges, including limited transparency, vulnerability to tampering, inefficient access control, and difficulties in maintaining an unbroken chain of custody [1]. As forensic data increasingly forms the cornerstone of legal proceedings, ensuring its integrity, accessibility, and authenticity has become critical. Blockchain technology, with its inherent properties of immutability, decentralization, and transparency, offers a promising alternative for digital evidence management. A blockchain-based system can securely record every interaction with a piece of evidence, ensuring that each transaction is time-stamped and cryptographically linked, thereby preventing any unauthorized modifications [2]. Additionally, smart contracts can be employed to automate permissions and evidence handling workflows, reducing human error and administrative overhead [3]. To address the issue of blockchain scalability and storage efficiency, many recent systems integrate distributed file systems such as the InterPlanetary File System (IPFS) to store large evidence files off-chain. Only the content hashes are maintained on the blockchain,

ensuring integrity without compromising performance [4]. Furthermore, a layered blockchain design—such as separating cold (archived) and hot (active) data—has shown significant improvements in system responsiveness and scalability [2]. Several recent implementations have demonstrated the feasibility and effectiveness of decentralized systems in digital forensics. These frameworks not only ensure secure storage and sharing of evidence but also enhance traceability and legal admissibility by maintaining a verifiable audit trail [5]. Building upon these advancements, this research proposes a comprehensive decentralized evidence management system that integrates blockchain, IPFS, and smart contracts to offer a secure, scalable, and transparent solution for forensic data handling.

II. RELATED WORKS

Recent years have seen a significant increase in the use of blockchain technology in digital evidence management, with researchers investigating a variety of strategies to improve security, accountability, and transparency. The drawbacks of conventional centralised evidence warehouses have been addressed by a number of methods. To reduce tampering concerns and provide a secure chain-of-custody, Sharma et al. [1] presented a blockchain-based platform. With time-stamped records that provide an unchangeable audit trail, their system makes it possible to track evidence. The authors contend that a decentralised ledger provides an efficient means of guaranteeing data integrity, pointing out that traditional systems are vulnerable to data manipulation, particularly during handovers. Kim et al. [2] suggested a two-level blockchain design especially for managing digital criminal evidence, building on the difficulties noted in earlier research. Their methodology makes a distinction between long-term, unchangeable evidence records (stored in a "cold" blockchain) and regularly updated metadata (stored in a "hot" blockchain). Data integrity is maintained while performance is improved by this separation. Legal chain-of-custody requirements are strengthened when role-based smart contracts are used for controlled access, which guarantees that only authorised individuals can access or alter documents. The potential of IPFS (InterPlanetary File System) to overcome blockchain's intrinsic limitations in storing huge multimedia evidence files was investigated by Kumar et al.

[3]. Digital files are stored off-chain in their decentralised archive system, but their hashes are kept on-chain for validation.

its execution and presence on the system. A postmortem digital forensics analysis of the system will never reveal any information that may be referable to either the deleted data set or automation process.

This hybrid method greatly lessens the storage load on blockchain nodes without sacrificing the evidence's immutability or verifiability. As the amount of digital evidence in cyber investigations increases, the authors show that this model can scale well.

The application of blockchain technology for forensic evidence screening and authentication was the main emphasis of Ashitha et al. [4]. To guarantee that the evidence is kept intact, their method uses digital signatures and smart contract-driven authentication checks. The framework places a strong emphasis on secure access policies, in which each modification or request is recorded and linked to an authorised user. This provides a crucial level of accountability, particularly when delicate or high-stakes legal actions are involved.

A blockchain-enabled chain-of-custody concept designed especially for legal and law enforcement organisations is presented by Tesma [5]. Every action concerning a piece of evidence, from acquisition to storage to presentation in court, is recorded by their system. The architecture allows for real-time verification by courts, attorneys, and forensic specialists while guaranteeing regulated access through the use of a permissioned blockchain. The study provides insights that are immediately applicable to real-world applications by highlighting realistic deployment problems such regulatory compliance and interoperability with existing systems.

These pieces collectively provide a solid basis for decentralised digital evidence systems. However, an integrated system that fully addresses scalability and legal admissibility while integrating distributed storage, blockchain, and automated access control is still required. By combining best practices from earlier research into a coherent, useful framework for safe and effective digital evidence handling, this study seeks to close that gap.

III. PROPOSED SYSTEM

The suggested method addresses the crucial problems of trust, transparency, and data security in conventional

centralised models by managing and storing digital forensic evidence via a decentralised network of blockchain nodes. The system guarantees redundancy, fault tolerance, and the removal of single points of failure—common weaknesses in traditional evidence storage frameworks—by distributing data among several trustworthy nodes [1].

Every action involving digital evidence is cryptographically signed and documented on the blockchain ledger, including acquisition, alteration, transmission, and analysis. Since these records cannot be removed or changed once they are added, the legitimacy and integrity of the evidence lifecycle are guaranteed. The foundation for admissibility in court proceedings is the clear and legally verifiable chain of custody formed by this unchangeable audit trail [2]. Smart contracts are incorporated into the system to manage and safeguard access to private data. Only authorised persons, including law enforcement officials, forensic analysts, and legal professionals, are allowed to access or modify particular evidence components thanks to these programmable scripts that automatically enforce established access control restrictions. This guarantees non-repudiation, role-based access, and confidentiality—all of which are essential when working with sensitive forensic data [3]. Furthermore, the system architecture offers timestamped actions, traceability across the evidence lifecycle, and tamper-proof logs to improve adherence to legal and regulatory requirements. It is simpler to prove adherence to legal processes, cybersecurity standards, and digital evidence handling techniques because to the blockchain's decentralised and transparent nature [4][5].

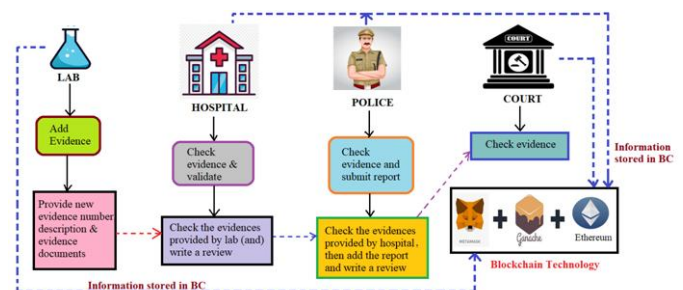


Fig. 1. Architecture of proposed system

IV. MODULES

A. Lab

Lab Incharge Registration: In this module, the lab incharge registers by providing the necessary personal and professional details, along with login credentials, to securely access the system.

Lab Incharge Login: Once registered, the lab incharge logs into the system using their secure credentials, gaining access to system functionalities designated for laboratory personnel.

Add Evidence: After logging in, the lab incharge can add new evidence by entering the evidence number, providing a detailed description, and uploading relevant files. This information is securely stored in the central blockchain-enabled database.

B.Hospital

Hospital Registration: In order to participate, hospitals must first register on the platform and provide the necessary institutional information needed for access authorisation and authentication.

Hospital Login: To access hospital-specific system features and case-related data, authorised hospital staff must check in with their registered login credentials.

Verify and Check Evidence: In this module, hospital employees examine and verify digital evidence pertaining to forensic or medical elements of ongoing cases. Their observations help to verify the data's veracity and accuracy.

provide Review: By providing reviews that are connected to particular pieces of evidence, hospitals can provide more context or insights, enhancing the case files with professional medical or clinical viewpoints.

C. Police

Police Registration: In order to verify their identity and position inside the system, police officers must register by presenting official identification and other necessary information.

Police Login: After successfully registering, police officers can use their login information to access features and resources specific to their investigative duties.

Verify Evidence and Submit Report: This module allows police officers to access, examine, and evaluate the digital evidence that is relevant to their investigations. Additionally, they have the option to file official reports, which are permanently recorded in the system.

D.Court

Court Registration: In order to gain secure and limited access to judicial functions, court officials must register for the system by providing pertinent authentication information.

Court Login: To view evidence and other legal documents pertaining to ongoing cases, authorised court employees must check in with their credentials.

Check Evidence: The court can examine and validate digital evidence in this module, using the data to support legal proceedings and guarantee impartial and well-informed decision-making

To access the features of the platform, the court is required to enter a valid username and password during login and logout sessions.

Once authenticated, the court can perform various tasks such as requesting court registration and viewing evidences related to a case. However, without valid login credentials, the court will not be able to access these features.

V. SOFTWARE ENVIRONMENT

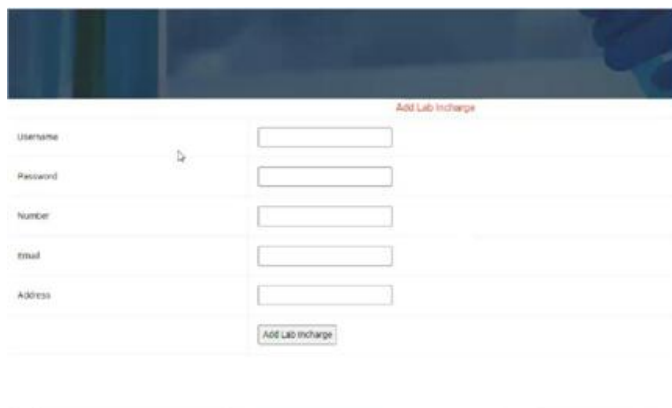
GANACHE: Ganache is an easy-to-use interface for tracking activity on the Ethereum blockchain. It makes tracking accounts, transactions, and smart contracts easier, so even people without extensive blockchain knowledge can utilise it. Ganache helps with debugging and guarantees transaction accuracy by providing comprehensive transaction information, including as sender, receiver, amounts, gas usage, and success status. Additionally, it monitors smart contract deployments to ensure proper deployment and operation. Processes for monitoring and verification are made simpler by this transparency. We can examine every block on the Ethereum blockchain in detail thanks to Ganache. We can determine when a specific block was added, the transactions that occurred within it, and the amount of gas (processing power) that was consumed. Additionally, ganache makes it possible to retrieve data from blocks that have been saved, giving developers access to and analysis of particular block information.

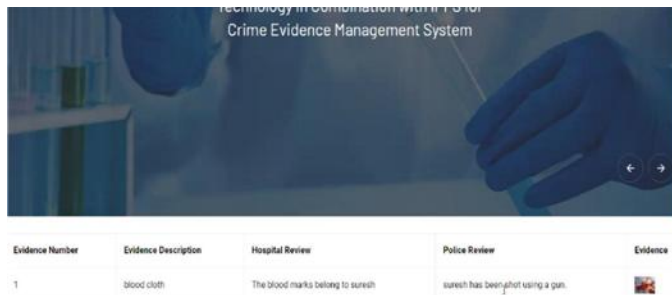
METAMASK: Metamask is both an Ethereum wallet and a browser extension. It simplifies cryptocurrency management and provides direct access to DApps, making interactions with blockchain applications easier. In the project, Metamask ensures secure Ethereum transactions, promoting transparency by showing the deduction of ETH as fees. This transparency maintains accuracy and ensures confident, reliable financial interactions within the system.


PYTHON LANGUAGE: High-level, object-oriented, interpreted Python is a computer language with dynamic semantics. It is highly appealing for Rapid Application Development and for usage as a scripting or glue language to

join pre-existing components because of its high-level built-in data structures, dynamic typing, and dynamic binding. Python's easy-to-learn syntax prioritises readability, which lowers software maintenance costs. Python promotes code reuse and software modularity by supporting modules and packages. For all major platforms, the Python interpreter and the large standard library are freely distributable and available in source or binary form. Python's greater productivity is often the reason why programmers fall in love with it. The edit-test-debug cycle is extremely quick because there is no compilation stage. Python programs are straightforward to debug because a segmentation failure is never caused by a bug or incorrect input. Rather, the interpreter raises an exception when it finds a mistake. The interpreter prints a stack trace if the application fails to catch the exception. Setting breakpoints, evaluating arbitrary expressions, inspecting local and global variables, stepping through the code line by line, and more are all made possible by a source level debugger. The debugger's introspective nature is demonstrated by the fact that it was written in Python. However, adding a few print statements to the source code is frequently the fastest way to debug a program; this straightforward method works very well due to the short edit-test-debug cycle.

VI. SCREENSHOTS





Evidence Number	Evidence Description	Hospital Review	Police Review	Evidence
1	blood cloth	The blood marks belong to sunesh	sunesh has been shot using a gun	

VII. FUTURE SCOPE

The proposed decentralised evidence management system offers a secure, transparent, and scalable framework for handling digital forensic data. However, there is need for improvement in the way Artificial Intelligence (AI) and Machine Learning (ML) algorithms are integrated for automated evidence classification, relevance detection, and anomaly spotting. AI-powered analytics can improve the efficacy and accuracy of investigations by emphasising significant pieces of evidence based on predetermined criteria. Cross-jurisdictional interoperability standards, which facilitate seamless collaboration between domestic and international companies, represent another area in need of development. Future versions of the system might have standardised APIs and interchain communication protocols to allow for the secure and approved sharing of evidence across different blockchain networks and legal jurisdictions.

The scalability of blockchain networks remains an important consideration, particularly given the increasing volume of high-resolution digital evidence, such as logs, videos, and sensor data. Future studies may look into layer-2 solutions like state channels or sidechains to increase transaction throughput and reduce latency without compromising security or data integrity [3]. With the addition of intuitive forensic dashboards and mobile interfaces, the system will be more beneficial to non-technical stakeholders such as jurors, field officers, and legal teams. Features like audit visualisations, real-time evidence monitoring, and automated report generation can enhance usability and operational transparency [1]. Furthermore, future research may focus on ensuring regulatory compatibility by utilising smart contracts that dynamically adapt to evolving judicial admissibility standards and data protection laws (like GDPR and HIPAA). The automatic adherence of evidence processing methods to evolving legal standards can be ensured by programmable logic-driven legal compliance engines [5]. Implementing biometric authentication and multi-factor identification verification can help improve access control, especially when handling highly sensitive or classified evidence.

VIII. CONCLUSION

The issues of authenticity, integrity, and traceability in digital evidence in criminal and legal investigations are intended to be addressed by the suggested decentralised evidence management system. The system builds a transparent, safe, and impenetrable foundation for digital evidence using distributed storage, smart contracts, and blockchain technology. By using a decentralised network of

blockchain nodes, the system eliminates single points of failure and ensures redundancy and fault tolerance. A transparent chain of custody is maintained by cryptographically recording transactions on an unchangeable ledger. By enforcing role-based access restriction, smart contracts improve stakeholder collaboration and confidentiality. For off-chain storage, the system incorporates IPFS, guaranteeing verifiability via hash integrity. This hybrid architecture solves storage issues without sacrificing evidentiary value by striking a balance between security and efficiency. The system improves operational transparency, legal dependability, and regulatory compliance. Advanced identity verification methods, cross-jurisdictional interoperability, and AI-driven evidence processing are examples of future advancements. This decentralised strategy guarantees that evidence is safe, verifiable, and unaltered throughout its lifecycle, strengthening the digital forensic process and fostering institutional and public trust.

REFERENCES

- [1] Sharma, A., et al. (2020). Blockchain-Based Digital Evidence Management System. *Forensic Science International: Reports*. [ScienceDirect](#)
- [2] Kim, D., Ihm, S.-Y., & Son, Y. (2021). Two-Level Blockchain System for Digital Crime Evidence Management. *Sensors*, 21(9), 3051. [MDPI](#)
- [3] Kumar, A., et al. (2021). Blockchain-based, Decentralized Evidence Archive System using IPFS. *ResearchGate*. [Link](#)
- [4] Ashitha, C. A., et al. (2023). Screening Forensic Evidence Employing Blockchain. *International Journal of Scientific Development and Research (IJS DR)*. [PDF](#)
- [5] Tesma, G. (2023). Blockchain-based Chain of Custody for Digital Evidence. *International Journal of Engineering and Advanced Scientific Technology (IJEAST)*. [PDF](#)