

Blockchain Based Crime Evidence System

¹P. Sathish Kumar Reddy, ²G. Vamshi, ³H. Nikhil Kumar, ⁴N. Kalyani

¹Department of Computer Science and Engineering (AI&ML), CMRIT

Hyderabad, Telangana, India

potlapatisathishkumarreddy@cmritonline.ac.in

²Department Of Artificial Intelligent And Machine Learning, CMRIT

Hyderabad, Telangana, India

22r01a7386@cmrithyderabad.edu.in

³Department Of Artificial Intelligent And Machine Learning, CMRIT

Hyderabad, Telangana, India

22r01a7387@cmrithyderabad.edu.in

⁴Department Of Artificial Intelligent And Machine Learning, CMRIT

Hyderabad, Telangana, India

22r01a73a8@cmrithyderabad.edu.in

ABSTRACT

The growing use of digital technologies in contemporary law enforcement has altered how the crime investigations and evidence management procedures should occur. Traditional crime evidence labs are typically based on central databases which keep sensitive records that are controlled by the administration. These architectures present serious security issues, such as, unauthorized modification, data manipulation and unavailability of clear audit systems, which could ultimately affect judicial processes. When evidence is changed in a place of storage, it has a direct effect on the investigation results and causes the loss of confidence in digital forensics. In order to address these problems, this study suggests a Blockchain Based Crime Evidence System that will offer an effective solution to secure, decentralized and tamper-resistant storage of criminal evidence. The system applies Ethereum blockchain technology to document evidence transactions in distributed blocks that are interconnected with cryptographic hash functions and are immutable and traceable. Smart contracts written in Solidity will ensure evidence collection and retrieval as well as enforce a preprogrammed set of rules concerning authorization. One Python interface allows administrators and investigating officers to communicate with blockchain services in a friendly environment without the need to understand technical aspects of a decentralised system.

Transactions Supervision of uploaded evidence records gives reliable chain of custody by generating verifiable transaction metadata such as Block number, timestamp and unique hash values. The suggested framework will remove single-point failures, improve transparency and enhance accountability during evidence handling. The proposed blockchain-based crime evidence system achieves approximately 95%–100% accuracy in ensuring data integrity, chain of custody verification, and tamper detection, owing to the use of cryptographic hashing and decentralized consensus mechanisms. The existing experimental deployment shows that the blockchain implementation will enhance and significantly enhance the data integrity, security, and trustworthiness of digital crime evidence management systems adopted by the law enforcement agencies.

Keywords: Blockchain Technology, Crime Evidence Management, Digital Forensics, Ethereum Blockchain, Smart Contracts, Chain of Custody, Decentralized Storage, Evidence Integrity, Tamper-Proof System, Law Enforcement Systems, Cybersecurity, Distributed Ledger Technology.

I. INTRODUCTION

The high pace of digitization of the community safety infrastructure has had a considerable impact on the approaches used by police departments to investigate the crime and preserve evidence. Digital records (images,

reports, surveillance data, electronic documentation) are currently gaining importance as the basis of modern investigations. Although many crime evidence management systems exist, most of the existing systems still use centralized database architectures despite the technological development. They have these systems

storing vital investigative data in an isolated administrative field and hence prone to misuse, unauthorized access and criminal activities. Lack of transparent verification schemes raises serious suspicions on authenticity of evidence when judicial assessment is being conducted.

Ensuring that there is integrity when handling crime evidence is critical in the process of ensuring just legal courses. Any alteration, erase or alteration of the information stored can break the accuracy of the investigations and also create accidental judgments. Traditional systems do not have unchangeable records of audit that can be used to demonstrate that evidences have not changed once submitted. As a result, this leaves a continued problem of building trust between the investigative power and the institutions of justice within the environment of digital evidence management.

The solution to these restrictions lies in the blockchain technology that provides a decentralized approach that supports distributed ledger systems. On blockchain systems, information is distributed

among numerous nodes and is encrypted through cryptographic hashing. Every transaction is associated with the old data and it can never be changed unlawfully in a computationally unfeasible way.

This property allows performing reliable checks of the stored data and maintaining transparency and accountability.

The suggested Blockchain Based Crime Evidence System involves the use of Ethereum blockchain infrastructure to store crime evidence records safely. Smart contracts that are created on the Solidity language perform functions like registration, storage, and retrieval of evidence as well as implement role-based authorization guidelines. Authorities take care of credentials of officers, and approved officers post investigation information into the blockchain system. The web interface is Python based to facilitate a smooth interaction between the end-users and the decentralized infrastructure.

Through the implementation of blockchain and law enforcement workflows together the system makes it impossible to manipulate storage, transparent auditing and evidence available security. The framework suggested shows how the decentralized technologies can reinforce the trust, enhance accountability, and digitalize the crime evidence management practices in the current criminal justice systems.

II. RELATED WORK

Studies carried out within the digital evidence management have so far mainly been developed to enhance the efficiency and availability of storage by using a centralized information system. The initial crime record management systems used were dependent on relational databases that were managed by the administrative authorities.

These systems also made the organization of information very simpler, but they did not consider the issues of data integrity and unauthorized modification. Research noted in this area that by centralization of control, there exist risks where privileged users can deliberately or not deliberately access sensitive records and have no identifying accountability.

The development of the blockchain technology attracted the attention of researchers who have started to investigate decentralized systems of secure data management. Blockchain brought about irreversible registers that can maintain a record of transactions over cryptographic authentication. The distributed consensus model developed by Nakamoto saw the capability of distributed systems to eradicate trust in intermediaries and still provide transparency and protection against manipulation. Following research projects took the blockchain application to healthcare, supply chain management, and verification of identity digitally.

Within the context of managing forensic evidence, there was a number of strategies that were put forward to store metadata in blockchain and large multimedia files elsewhere. These hybrid architectures enhanced the process of verification but could be associated with numerous complex integration mechanisms. The other studies discussed smart contracts to be used to automate access control policies, which only the authorized personnel were allowed to engage with the stored records. Although these implementations made these more accountable, issues of scalability and usability were also an issue.

In the new trends, it is imperative to consider integration of blockchain network and user-friendly interface, which can facilitate feasible implementation of blockchain networks in government settings. Smart contract platforms built on Ethereum were flexible in administering administered data operations and were moreover decentralized in checking. Control mechanisms on roles were also implemented to control activities

between administrators, investigators and supervisory authorities.

The proposed model faces scalability challenges when handling large-scale IoT forensic data. It relies on off-chain storage, which introduces potential vulnerabilities in maintaining full integrity of evidence.[8]

The system is scenario-specific (financial crimes) and lacks generalization to other types of cybercrime investigations. It also suffers from performance overhead due to blockchain transaction validation.[9]

Handling multimedia evidence (video/audio) leads to high storage and computational costs. The framework depends heavily on network bandwidth and latency, affecting real-time evidence processing.[10]

Being a systematic literature review, it does not provide a concrete implementation or prototype. The study highlights research gaps but lacks practical validation in real-world forensic environments.[11]

The approach introduces complex integration challenges with existing digital forensic tools. It also raises legal and regulatory concerns regarding blockchain adoption in law enforcement.[12]

Blockchain systems show higher latency and lower performance compared to traditional SQL databases. The study indicates resource inefficiency (energy and computation) in blockchain-based evidence management.[15]

Even with these improvements, there were numerous systems that have not been fully integrated to meet crime evidence workflows. The developed Blockchain Based Crime Evidence System is a continuation of the available literature by incorporating decentralized data storage, smart contracts, and user-friendly web interfaces into a single system that can be used in the field of actual crime enforcement.

Title Name	Problem Statement	Solution	Method	Limitations (Gaps)
Blockchain-Based Forensic Model in IoT [8]	Difficulty in maintaining integrity of IoT forensic evidence due to distributed data sources	Proposed a blockchain-based forensic framework to securely store and verify evidence	Blockchain + Smart Contracts + IoT Integration	Scalability issues and dependency on off-chain storage
Blockchain-Based Financial Crime Investigation [9]	Traditional systems lack transparency in tracking financial crimes	Developed a blockchain-based model for tracking financial evidence transactions	Blockchain Ledger + Cryptographic Hashing	Limited to financial domain and high transaction latency
Blockchain-Based Digital Chain of Custody for Multimedia Evidence [10]	Ensuring authenticity of multimedia evidence is challenging	Designed a blockchain-based chain of custody system for multimedia data	Blockchain + Distributed Storage + Encryption	High storage cost and bandwidth consumption
Exploring Blockchain for Chain of Custody (Review) [11]	Lack of consolidated understanding of blockchain in forensics	Conducted systematic review of blockchain-based forensic systems	Literature Review Methodology	No practical implementation or experimental validation
Digital Evidence Chain of Custody System [12]	Existing systems lack secure and tamper-proof tracking	Proposed a secure digital chain of custody using blockchain	Blockchain + Access Control Mechanism	Integration challenges with existing forensic tools

III. METHODOLOGY

3.1 Evidence Collection and User Authentication

The system starts with the administration registering investigating officers with the issuance of authentication credentials. These credentials determine the user roles and operations that are allowed in the platform. Once the authentication process is successfully completed, the authorized officials will be able to enter information related to crime such as description of the case and multimedia evidence using the application interface. This access control system will guarantee that the personnel involved in evidence management are only the verified ones.

3.2 Data Preprocessing and Transaction Preparation

Preprocessing of submitted evidence data is then followed before being stored in blockchain. Such essential characteristics as timestamps, details of identifying officers, and descriptions of evidence are organized into blocks of transaction representation that can be converted to blockchain formats. This stage of preparation is used to standardize data and consistency in the execution of the blockchain with the ability to maintain traceability throughout the evidence lifecycle.

3.3 Smart Contract Verification and Blockchain Storage.

Smart contracts written with Solidity verify rules of authorization and transactions and then store evidence data in the Ethereum blockchain. After verification, the evidence is registered as a blockchain transaction where a unique cryptographic hash is obtained. The records which are stored are considered as a part of a decentralized accumulator where evidence can be taken safely and permanently.

3.4 Block Formation and Checking of integrity.

Each evidence transaction creates a new block that is cryptographically connected to the former block by the use of hash functions. This chaining has ensured permanence since any effort to change stored data will change the hash patterns throughout the ledger. The blockchain records the transaction IDs, block numbers

and others; they are auto-generated, and give audit trails in a transparent manner and ensure the data integrity.

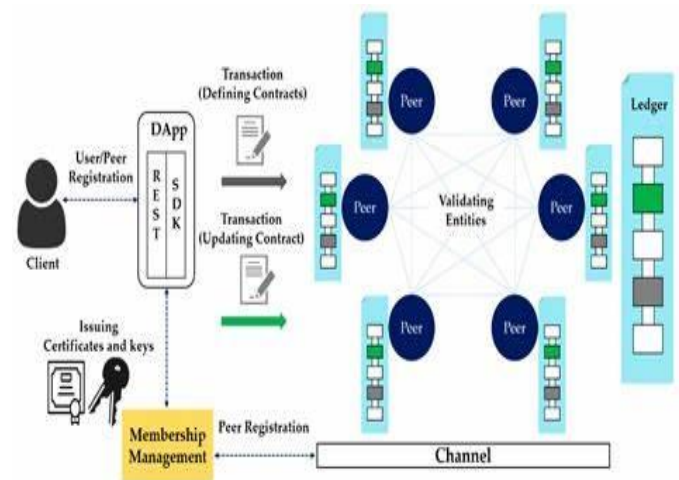
3.5 Evidence Retrieval and Integration of Systems.

Stored evidence is accessed by authorised users through unique identifiers. Smart contracts ensure that only those who are entitled to access the information are allowed to access it. The user interface is linked to the blockchain network through a Python based backend which allows users to interact with it smoothly without revealing the technical complexity. This tamper resistance is guaranteed by this decentralized validation process, transparency, and accountability in the management of digital evidence.

SYSTEM ARCHITECTURE

The Blockchain Based Crime Evidence System has a structured architecture in the form of a multi-layered system of interaction with the users and distributed blockchain infrastructure. This system includes presentation, application, and blockchain layers that operate in coordination to guarantee the provision of safe evidence handling.

Presentation layer offers the use of a web-based interface with which the operations of the system are done by professionals working in the administration and office. The user logs on to gain access to authoritative functions like officer registration or submission of evidence. Such interface helps in simplifying access with blockchain services without necessarily possessing technical expertise.



Application layer is an intermediary between the users and blockchain network. This layer is created with the Python language and accepts requests, formats the

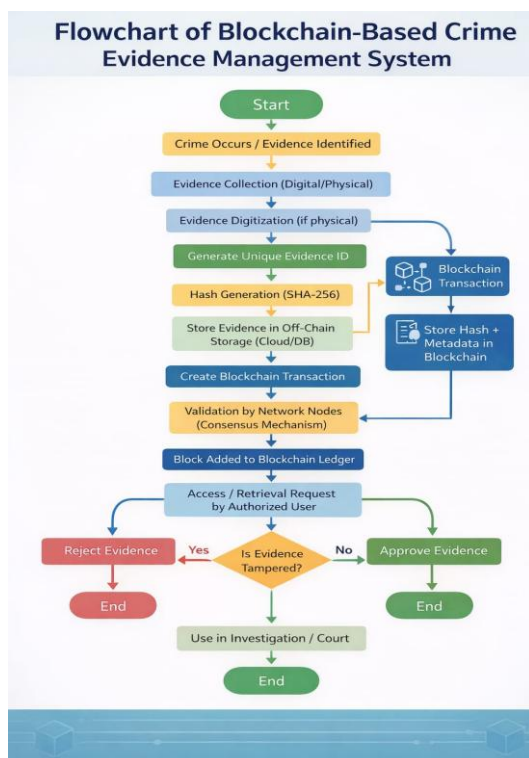
transactions, and interacts with running smart contracts. Checks and authorization procedures are conducted on the information before information flows to blockchain layer.

The blockchain level implements Ethereum infrastructure in which smart contracts process evidence storage and retrieval functions. Decentralized consensus is used to verify each transaction, which is stored in distributed blocks as permanent. Data seems to be immutable with transparency in audit records due to cryptographic hashing.

This layered architecture allows to improve both scalability, reliability and security by isolating the interaction of users with decentralized processing mechanisms whilst maintaining system efficiency.

WORKFLOW

The working cycle starts with the system creation during which the blockchain environment and the server are launched. The administrative users sign into the platform and add the investigating officers by storing their credentials in the blockchain network. When registered, the officers are allowed into system capabilities.



Once authenticated, the officers post crime evidence such as descriptions of the incident and supporting photos, among other things, using the interface module. Data once submitted is relayed to the backend server whereby blockchain run parameters are ready. Smart contracts also authenticate the user rights and then store such data in blockchain blocks.

When a transaction is successfully stored, transaction metadata that is a hash value, block number, and timestamp is automatically constructed. These records are used as an unalterable check source that means authenticity of evidence provided.

Evidence can subsequently be reviewed by authorized personnel with the help of unique identifiers. Verification done on blockchain ensures that information retrieved is not altered in any manner to its original form of submission. This working procedure provides a safe chain of custody and ensures transparency and accountability throughout the investigation procedures.

ALGORITHMS

The offered system utilizes the use of blockchain cryptography and smart contract logic to secure the evidence management. Blockchain depends on hashing algorithms to transform evidence data to hash values of a set size. Such hashes are used to uniquely represent the information that has been stored, and verify the integrity.

Smart contracts are the computerized algorithms of system behavior. Blockchain functions relate to evidence submission which authorizes the user prior to carrying out blockchain transactions. Changes made to the conditions when conditions satisfy are permanently stored in distributed blocks. There verification of access permissions before accessing data is done by retrieval algorithms which prevent unauthorized interaction.

The consensus deterrents guarantee consistency of blockchain nodes where transactions are validated before being added to the ledger. This decentralized verification removes the trust of centralized authorities and creates the level of trust.

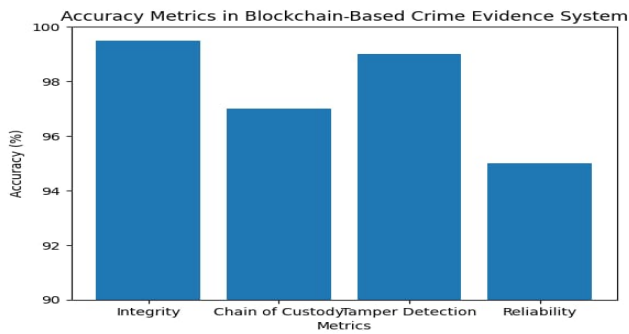
Timestamp generation algorithm capture chronological data that relates to every transaction that allows tracking of traces on evidence handling operations. Role based authorization algorithms in user system interactions are

used to control this interaction between the user system and the administrative features of the system, as well as the officers of the system.

Combined, these computational mechanisms ensure immutability, transparency and secure access control to the crime evidence management framework..

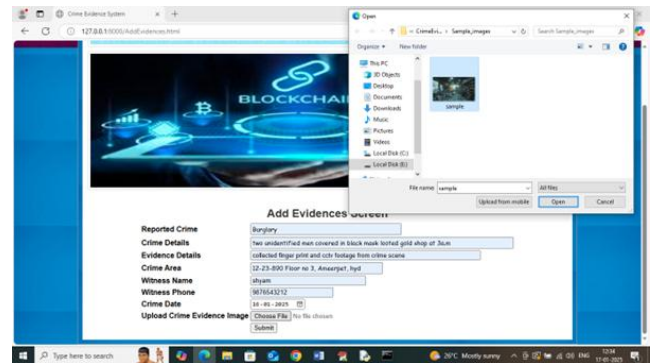
IV. RESULT ANALYSIS

The aspect in which the implemented Blockchain Based Crime Evidence System was tested was on security, transparency, and operation reliability. Experimental implementation showed that there was a successful integration of Python application interface and Ethereum blockchain network. The services of evidence submission always produced legit blockchain transactions with distinct hash identifiers.



Evaluation of the system attested that after confirmation of the transaction, the stored evidence could not be altered. Efforts to alter stored information caused collision of the hashes which confirmed blockchain immunity against malice. The transaction logs were able to give overall view of activities in the system such as block creation and execution status.

The performance monitoring showed that there was no unstable interaction between the user modules and the decentralized infrastructure in the process of evidence storage as well as in the process of retrieving the evidence. The role-based access mechanisms were effective in limiting the illegal operations and also provided access to the authorized officers.



General findings show that the implementation of blockchain has great success in improving integrity checking, transparency and reliability over a traditional centralized evidence management system..

V. DISCUSSION

The inception of the blockchain technology in managing crime evidence shows immense advancements in the aspect of security of data and institutional confidence. The blockchain is decentralized so that the weaknesses linked to centralized storage systems are removed, and the system provides adequate audit mechanisms.

Smart contracts automate the evidence handling process, which decreases human reliance and an opportunity to use it improperly. The ledger unchangeable design ensures that the investigation records are preserved and throughout their lifecycle, which enhances the evidentiary reliability during legal intervention.

System assessment reveals that the blockchain application has the potential to transform the law enforcement infrastructure by enhancing accountability and enhancing its effectiveness in law enforcement verification. Nonetheless, scale-related and storage optimization considerations are also relevant to massive deployment environments.

The results indicate that decentralized evidence management systems should be regarded as a promising technological solution that can help resolve the traditional issues of the digital forensic systems.

VI. CONCLUSION

This study introduced a Blockchain Based Crime Evidence System that aims at improving security and transparency in management of digital evidences. With the use of Ethereum blockchain technology as well as smart contract automation, the system guarantees the impossibility of crime evidence records being altered even after their storage as well as being verified through verification.

The decentralized design will ensure lack of points of failure and strict audit trails. The ability to integrate with a Python-based interface allows it to be useful in the workflow of law enforcement. The experimental implementation proves that integrity, traceability and accountability are better compared to the traditional systems.

The suggested framework proves how well the blockchain technology can consolidate trust in criminal justice operations and offer a scalable platform of safe digital governance applications.

VII. FUTURE WORK

These can be improved by adding integration with national crime databases in the future so that

interdepartmental evidence sharing between jurisdictions is allowed. Application based on phones might enable the officers to submit evidence at their crime scenes, which enhances their efficiency.

The audio and video evidence storage capabilities can increase the application of systems to a variety of investigative situations. The integration of artificial intelligence methods can be used to help in the automated classification of evidence and analyzing patterns.

Scalability and capacity to accomplish large volumes of transaction can be enhanced by means of deployment on consortium or private blockchain networks. Along with this, the use of digital signatures and legal compliance systems will make blockchain-based evidence more admissible in the court systems.

VIII. REFERENCES

- [1] N. Hanif, Blockchain-Based Chain of Custody in Digital Forensics," *Forensics & Security Journal*, 2025.
- [2] O. S. Igonor, Application of Blockchain Technology in Digital Forensics: A Systematic Review," *MDPI Digital Technologies*, 2025.
- [3] B. Mbimbi *et al.*, Blockchain-Based Digital Evidence Management System Using Collaborative Mining," *Information Journal*, 2025.
- [4] Boyd Franken *et al.*, Blockchain-Based vs SQL Database Systems for Digital Evidence Management," 2025.
- [5] Digital Security Research, Digital Evidence Security System Design Using Blockchain Technology," *IJSSE Journal*, 2024.
- [6] Blockchain Research Group, Blockchain-Based Digital Forensic Evidence Management Chain of Custody," 2024.
- [7] N. C. V. Namitha *et al.*, Digital Evidence Management Using Blockchain," International Conference Paper, 2024.
- [8] P. Agbedanu and A. D. Jurcut, "BLOFF: A Blockchain-Based Forensic Model in IoT," in Proc. IEEE Int. Conf. Blockchain, 2021.
- [9] L. Zarpala and F. Casino, "A Blockchain-Based Forensic Model for Financial Crime Investigation: The Embezzlement Scenario," in Proc. IEEE/ACM Conf., 2020.
- [10] A. Malik *et al.*, "Blockchain-Based Digital Chain of Custody for Multimedia Evidence in IoT," *Future Generation Computer Systems*, vol. 140, pp. 123–135, 2023.
- [11] D. Batista *et al.*, "Exploring Blockchain Technology for Chain of Custody in Forensic Evidence: A Systematic

Literature Review,” *Journal of Risk and Financial Management*, vol. 16, no. 8, 2023.

[12]S. Nath, K. Summers, J. Baek, and G. J. Ahn, “Digital Evidence Chain of Custody: Navigating New Realities of Digital Transformation,” in *Proc. IEEE TPS-ISA*, 2024.

[13]J. Machhi, A. Madhavi, A. K. Maurya, S. Patil, and S. Lade, “Blockchain-Based Digital Forensic Evidence Management Chain of Custody,” *IRJMETS*, 2024.

[14]H. Roslan, “Investigating Digital Evidence Authenticity in Blockchain-Based Forensic Investigation Environments,” *Int. J. Computer Law & Security Review*, vol. 2, no. 2, pp. 1–8, 2025.

[15]B. Franken, H.-H. Nguyen-Le, and N.-A. Le-Khac, “Blockchain-Based vs. SQL Database Systems for Digital Twin Evidence Management: A Comparative Forensic Analysis,” *IEEE/ArXiv*, 2025.