International Journal of Science, Strategic Management and Technology
Volume **02** Issue **04** April-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Criminal Evidences Management System using Blockchain

A. Sai Sankeerth Goud
UG Student, Dept of CSE(Data Science),
CMR Technical Campus
Hyderabad, Telangana, India
237r1a67d0@cmrtc.ac.in

A.Vignesh Reddy
UG Student, Dept of CSE(Data Science),
CMR Technical Campus
Hyderabad, Telangana, India
237r1a67d1@cmrtc.ac.in

K.Jaswanth Sai Kumar
UG Student, Dept of CSE(Data Science),
CMR Technical Campus
Hyderabad, Telangana, India
237r1a67f7@cmrtc.ac.in

N.Aishvarya Reddy
UG Student, Dept of CSE(Data Science),
CMR Technical Campus
Hyderabad, Telangana, India
237r1a67h3@cmrtc.ac.in

Mr.A.V.H.Sai prasad
Associate Professor, Dept of CSE(data Science)
CMR Technical Campus
Hyderabad, Telangana, India

https://doi.org/10.55041/ijsmt.v2i4.319

Cite this Article: Goud, A. S. S., Reddy, A., Kumar, K. S. & Reddy, N. (2026). Criminal Evidences Management System using Blockchain. International Journal of Science, Strategic Management and Technology, *02*(04). https://doi.org/10.55041/ijsmt.v2i4.319

Abstract:
Criminal Evidence Management System through Blockchain technology seeks to create an effective, unbreakable and decentralized mechanism where one can store and retrieve evidence related to crimes. Centralized systems have weaknesses such that unauthorized manipulations of vital data may be done. However, with this technology, one takes advantage of the decentralized aspect of Blockchain technology through which evidence is stored in immutable blocks characterized by unique hash codes. Smart Contracts programmed in Solidity language are applied to manage evidence transactions on the Ethereum Blockchain network while the Python programming language provides the front-end interface for admin and officers' users.

I. INTRODUCTION

The advent of modern technology has seen revolutionary changes in the method of storing, managing, and securing of data. Within the field of law enforcement, the security of criminal evidence becomes paramount. Most current evidence management systems operate in centralized platforms and hence prone to data alterations, hacking, and single points of vulnerability. This poses a significant risk to the integrity of the evidence.

A more efficient and secure method would involve the use of blockchain technology. The technology offers a platform for storing data, which is immutable. Here, data is stored in blocks that are interlinked using hashing algorithms. After a datum is entered in the blockchain, it cannot be deleted without altering all other blocks in the chain. This ensures the integrity of the evidence.The system will use smart contracts for the automation of processes within the system, including the uploading, accessing, and authentication of the records. By doing so, there will be enhanced transparency, trust, and

traceability within the system. Besides, an intuitive interface will be designed to facilitate easy interaction between users and the system.

II. LITERATURE REVIEW

"Blockchain-Based Digital Evidence Management System"

Z. Zheng, S. Xie, H. Dai, X. Chen (2018)

This paper investigates the ways blockchain can be employed to manage digital evidence safely. The researchers focus on the intrinsic drawbacks associated with centralization of forensic processes, such as the possibility of evidence tampering and its untraceable character. Due to the immutable nature of blockchains, the method offered by the researchers allows ensuring security and traceability of evidence storage and handling operations.

"A Secure Framework for Forensic Evidence Preservation Using Blockchain"

K. K. R. Choo, A. Dehghantanha (2017)

In this research, a framework for forensic evidence management is suggested. Problems related to the use of traditional approaches to forensic evidence management are analyzed. These include problems associated with violating chain of custody and modifying the evidence without authorization. The framework proposed by the authors employs the principles of cryptography and distributed ledgers to record the handling of forensic evidence.

III. PROPOSED SYSTEM

The suggested system implements the Blockchain based Criminal Evidence Management System that addresses the drawbacks associated with centralized databases. In this regard, all information related to crimes and evidence will be stored in a decentralization, immutable, and tamper-proof database known as the Ethereum Blockchain. Every transaction of the criminal evidence is logged in a block, while each of those blocks is chained to the preceding one through a unique hash function.

This way, in case someone tries to manipulate the data, there will be a mismatch between the hash values of the blocks. For management purposes, the proposed system uses Solidity written smart contracts. This smart contract code defines the rules according to which crime and evidence data can be retrieved from or updated in the blockchain. These smart contracts are deployed to the blockchain and can be accessed via the Python-based interface..

IV. METHODOLOGY

This proposed system is structured through the use of Blockchain technology, smart contracts, and an interface for the management of criminal evidence.

1. Architecture Design: This system is developed to be a decentralized application where the evidence records would be stored in the Ethereum Blockchain rather than in a centralized database. There would be a specified role for both users and data flow, access mechanisms, and blockchain interaction layers.

2. Smart Contracts: Smart contracts are developed in Solidity programming language, which handles all activities related to evidence. The smart contracts have functions to add officers, evidence metadata, record retrieval, and access control. They are uploaded to the Ethereum Blockchain to ensure automation and immutability.

3. Evidence Data Handling and Hashing: In the process of uploading new evidence, information about the cases and files are handled. Hashing cryptographic algorithms are used to create unique hashes from the evidence stored on the Blockchain.

4. Integration with Blockchain: The Smart Contracts are integrated into the Python application through blockchain interaction libraries, ensuring that transactions can be carried out within the Ethereum network.

5. User Authentication and Permissions: Administrator and Officer logins are provided. User authentication allows limited actions such as recording and retrieving evidence information.

6. Evidence Information Storage and Retrieval: An Officer logs onto the interface and uploads information about the evidence. This leads to the execution of Smart Contracts for storing evidence information. Users can retrieve the information from the Blockchain using evidence identification numbers.

7. Testing and Validation: The system is tested for correct execution of transactions, immutability, restricted access, and tamper detection. Functionality test checks ensure that the system performs well under different scenarios.

8. Execution and Deployment: The system will be executed and deployed in an environment where interactions occur through the Python application interface. Decentralization ensures that evidence information cannot be manipulated.

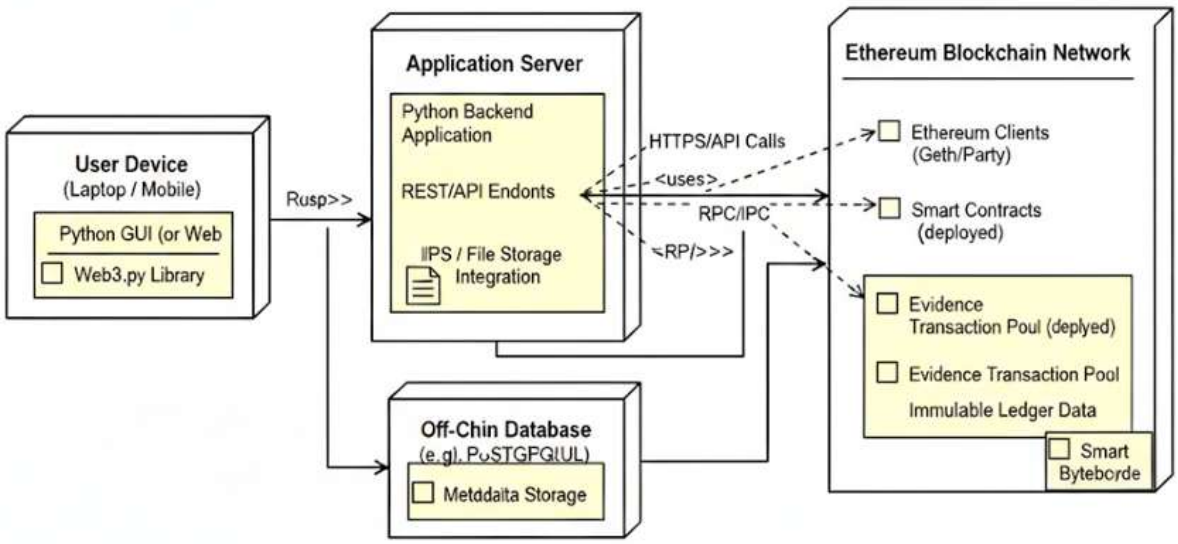

Fig 1: Criminal Evidences Management System using Blockchain

V. RESULTS AND FUTURE WORK

The Criminal Evidence Management System based on the Blockchain Technology has many advantages that help avoid possible issues associated with traditional approaches. Firstly, it ensures complete transparency, does not allow any unauthorized parties to access data, and eliminates possible manipulations with information. Secondly, the introduction of a convenient web interface enables Admins and Officers to handle evidence records easily and efficiently.

The backend of the system performs an important function by integrating such features as authentication, transactions with smart contracts, and managing records. These functions help to perform many actions automatically, eliminate any mistakes that might occur during the process, and ensure the consistency of handling evidence data. All data is stored in the Ethereum blockchain, which makes it impossible to change records or delete any information.

Finally, the proposed project demonstrates the high efficiency of the application of blockchain technology in enhancing evidence management systems' reliability and integrity. It not only ensures effective protection of information from any manipulation but also promotes accountability and transparency of the entire process.

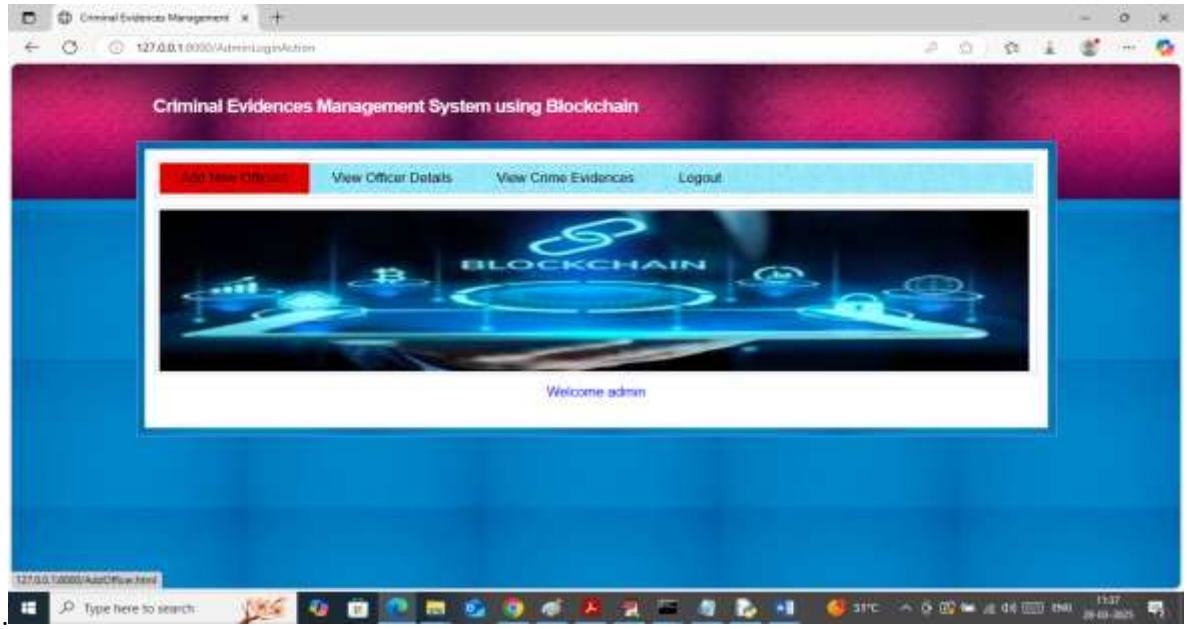

Fig 2: Home page of Criminal Evidence Management System

Fig 3: Output After Criminal Evidence Storage in Blockchain

Future Work: The proposed Criminal Evidence Management System based on Blockchain technology may also be improved by integrating state-of-the-art technologies like Artificial Intelligence and Machine Learning for analyzing and classifying evidence. It could be of assistance in accelerating investigation process by detecting abnormalities, revealing certain patterns, and supporting decisions of law enforcement bodies.

The suggested system might also become more flexible by implementing cloud technologies and Internet of Things (IoT) solutions that would help in collecting and monitoring evidence in real time via surveillance cameras and other means. Besides, enhancing scalability and performance of the underlying Ethereum network as well as adopting hybrid blockchain architecture might make the system better in processing cases of high complexity.

Moreover, future development of the proposed system may also entail better access control mechanisms, biometric authentication capabilities, and integration with mobile applications, which would allow for greater flexibility and usability of the platform. Thus, the presented system would not only become more intelligent but also more viable in terms of its practical application in criminal investigations.

VI. CONCLUSION

The proposed Criminal Evidence Management System with Blockchain Technology is a contemporary way of dealing with sensitive data. This system does not suffer from drawbacks typical of conventional systems since it ensures transparency, minimizes unauthorized access, and eliminates chances of data manipulation. The web interface that has been integrated into the system makes it easier for Admins and Officers to manage evidence records.

It should be noted that the backend of the system is critical for the operation of the application. The backend has been designed to include the process of authentication, interaction with smart contracts, and evidence management logic. This enables automation, minimization of human error, and consistent record management. Since all data will be stored on the Ethereum blockchain, there will be a high level of security and traceability.

In conclusion, the development of the project proves the efficiency of blockchain technology in the field of criminal investigation and forensic science. Moreover, blockchain has made it possible to ensure the security and reliability of evidence management. The application can be scaled up and used in practice.

VII. REFERENCES

1. Satoshi Nakamoto,“Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
2. Zibin Zheng, Shaoan Xie, Hongning Dai, Xi Chen, and Huaimin Wang, “Blockchain Challenges and Opportunities: A Survey,” *International Journal of Web and Grid Services*, 2018.
3. Michael Crosby, Pradan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman, “Blockchain Technology: Beyond Bitcoin,” *Applied Innovation Review*, 2016.
4. Kim-Kwang Raymond Choo and Ali Dehghantanha,“Contemporary Digital Forensic Investigations of Cloud and Blockchain Technologies,” *IEEE Cloud Computing*, 2017.
5. Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor, “Making Smart Contracts Smarter,” *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2016.
6. A. Elakaş, H. Sözer, İ. Şafak, and K. Kalkan,“A Systematic Mapping on Software Testing for Blockchains,” *Cluster Computing*, 2024.
7. H. Rameder, M. di Angelo, and G. Salzer,“Review of Automated Vulnerability Analysis of Smart Contracts on Ethereum,” *Frontiers in Blockchain*, 2022.
8. P. Honkanen, M. Nylund, and M. Westerlund,“Organizational Building Blocks for Blockchain Governance: A Survey of 241 Blockchain White Papers,” *Frontiers in Blockchain*, 2021.
9. H. Huang, W. Kong, S. Zhou, Z. Zheng, and S. Guo,“A Survey of State-of-the-Art on Blockchains: Theories, Modelings, and Tools,” *arXiv preprint arXiv:2007.03520*, 2020.
10.R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia,“A Survey on Blockchain Interoperability: Past, Present, and Future Trends,” *arXiv preprint arXiv:2005.14282*, 2020.
11.N. Deepa, Q.-V. Pham, D. C. Nguyen, et al.,“A Survey on Blockchain for Big Data: Approaches, Opportunities, and Future Directions,” *arXiv preprint arXiv:2009.00858*, 2020.

12.H. Ahmad, M. A. Ahsan, and A. N. Mian,"Trends in Publishing Blockchain Surveys: A Bibliometric Perspective," *arXiv preprint*, 2021.
13.M. Rahmaty,"Evaluating Blockchain-Based Supply Chain Challenges (A Survey)," *International Journal of Innovation in Engineering*, 2023.
14.X. Lu and A. Taghipour,"A Review of Supply Chain Digitalization and Emerging Research Paradigms," *Logistics*, 2025. [1] P. H. S. Kalmet, S. Sanduleanu, S. Primakov, G. Wu, A. Jochems, T. Refaee, A. Ibrahim, L. V. Hulst, P. Lambin, and M. Poeze, "Deep learning in fracture detection: A narrative review," Acta Orthopaedica, vol. 91, pp. 215–220, 2020.