ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 1(1), 2026

Peer Reviewed, Referred & Indexed Journal

Research Paper

ForensiChain: A Decentralized Evidence Management System Using Blockchain Technology

Zoya Tabassum[1], *Syeda Zeba Qureshi*[2] *Mohammad Samiullah Khan*[3], Mohammed Rizwan Ali[4], *Mohammed Nasir Hussain*[5]

[1,2]Assistant Professor, Department of CSE (Data Science), Lords Institute of Engineering and Technology, Hyderabad, Telangana, India.
[3,4,5]UG Students, Department of CSE (Data Science), Lords Institute of Engineering and Technology, Hyderabad, Telangana, India.

***Abstract*— This project presents a secure and decentralized approach for managing forensic evidence using blockchain technology. Traditional evidence management systems, whether manual or centralized, are vulnerable to tampering, data loss, and unauthorized access. To address these issues, the proposed system utilizes blockchain to store forensic data in a tamper-resistant and encrypted format. Each piece of evidence is recorded as a block and linked with previous records through cryptographic hash values, ensuring data integrity and transparency. The system employs Ethereum-based blockchain along with smart contracts to securely store and retrieve evidence details. Additionally, a Python-based interface is integrated to interact with the blockchain, enabling authorized users to add and access records efficiently. This approach enhances trust, reliability, and accountability in forensic investigations and legal proceedings.**

***Keywords*—Blockchain, Forensic Evidence, Ethereum, Smart Contracts, Data Security, Decentralization**

I. INTRODUCTION

Forensic evidence management is a crucial aspect of criminal investigations, as it directly influences the outcome of legal proceedings. Proper handling, storage, and tracking of evidence are necessary to maintain its authenticity and reliability. However, traditional methods such as paper-based documentation and centralized digital systems often face challenges including human error, data manipulation, and security vulnerabilities. These issues can lead to loss or alteration of critical evidence, ultimately affecting justice delivery. Therefore, there is a strong need for a secure and transparent system that ensures evidence remains intact throughout its lifecycle. Blockchain technology offers an effective solution by providing a decentralized and tamper-resistant environment [7]. With its ability to record data in immutable blocks linked through cryptographic hashes, blockchain enhances trust and accountability [5]. This project focuses on applying blockchain technology to improve the security and efficiency of forensic evidence management systems [1].

In recent years, the growth of digital technologies has increased the importance of secure data management in various sectors, including law enforcement. Forensic evidence, whether physical or digital, must be preserved in a way that prevents unauthorized modifications and ensures accurate tracking. Existing centralized systems are often vulnerable to cyberattacks and insider threats, making them unreliable for handling sensitive information. Blockchain technology addresses these concerns by distributing data across multiple nodes, eliminating the need for a single controlling authority [9]. Each transaction recorded on the blockchain is verified and linked to previous records, creating a transparent and traceable history. This feature is particularly beneficial in maintaining the chain of custody for forensic evidence [1]. By implementing blockchain, the system ensures that every action related to evidence is recorded securely, thereby increasing confidence among investigators, legal professionals, and judicial authorities [2].

The concept of decentralization in blockchain technology plays a significant role in enhancing data security and reliability. Unlike traditional databases, where a single point of failure can compromise the entire system, blockchain operates on a distributed network where data is replicated across multiple nodes [6]. This structure makes it extremely difficult for attackers to alter or delete information. In the context of forensic evidence management, such security is essential to prevent tampering and ensure that evidence remains credible. Additionally, blockchain uses cryptographic techniques to protect data, ensuring that only authorized users can access or update records [4]. The use of smart contracts further automates processes such as data entry and verification, reducing the chances of human error. This project utilizes these features to create a robust system for managing forensic evidence, ensuring transparency, security, and efficiency in handling sensitive information [10].

II. RELATED WORK

Bonomi et al., (2018) [1] Bonomi and colleagues proposed a blockchain-based system called BCoC to manage the chain of custody in digital forensics. Their work highlights how blockchain can ensure integrity and traceability of evidence. The system records every action performed on evidence, making it transparent and verifiable. By using cryptographic hashing, it prevents unauthorized modifications. The authors emphasized that traditional systems lack proper tracking mechanisms. Their approach improves trust among investigators and legal authorities. It also reduces the chances of evidence tampering. The study demonstrates how blockchain can strengthen forensic processes.

Bou Abdo et al., (2020) [3] Bou Abdo and co-authors introduced a hybrid consensus mechanism based on reputation for blockchain networks. Their work aims to improve trust and efficiency in permissionless blockchains. The proposed model evaluates node behaviour to maintain network reliability. It reduces the risk of malicious activities within the system. The study shows how consensus mechanisms play a key role in blockchain security. It also enhances performance compared to traditional methods. This approach is useful in applications requiring high data integrity. The research contributes to improving blockchain reliability.

Gopalan et al., (2019) [2] Gopalan and team explored the application of blockchain in digital forensic investigations. They focused on improving security and reliability in handling forensic data. The study explains how decentralized storage eliminates single points of failure. Blockchain ensures that once data is recorded, it cannot be altered. The authors also discussed challenges in existing forensic systems. Their proposed model enhances transparency and accountability. It supports secure evidence sharing among multiple parties. The research highlights blockchain as a promising solution for forensic data management.

Varshney et al., (2019) [4] Varshney and colleagues discussed the importance of authentication and encryption in blockchain security. Their work focuses on protecting data from unauthorized access. The authors explained how cryptographic techniques secure transactions in blockchain networks. They highlighted the role of encryption in maintaining confidentiality. The study also addresses common security threats in digital systems. Their approach strengthens data protection mechanisms. It ensures secure communication between users. The research supports the use of blockchain for secure applications.

Androulaki et al., (2018) [10] Androulaki and team presented Hyperledger Fabric as a platform for permissioned blockchain systems. Their work focuses on enterprise-level applications requiring privacy and control. The platform allows only authorized participants to access data. It provides modular architecture for flexibility and scalability. The authors highlighted its suitability for secure data sharing. The system supports smart contracts for automation. It improves performance compared to public blockchains. The study shows how permissioned blockchains can be used in real-world applications like forensic systems.

III. DATASET DETAILS

The dataset used in this project consists of forensic evidence records collected and managed through the application interface. It includes various attributes such as case identification number, type of crime, date and time of occurrence, location details, description of the incident, and information related to the collected evidence. Additional fields may include officer details, evidence status, and remarks for further investigation. Each record entered into the system is treated as a unique transaction and is securely stored on the blockchain. The dataset is not preloaded but is dynamically generated as users input data through the application. This ensures that the data remains up-to-date and relevant to real-time investigations. All entries are structured in a consistent format, enabling easy storage, retrieval, and verification.

The use of blockchain ensures that once the dataset is recorded, it cannot be modified or deleted, maintaining its integrity.

The dataset is managed in a decentralized manner using blockchain technology, where each record is stored as a block linked with previous records through cryptographic hashes. This structure ensures transparency and traceability of all evidence-related information. The data is encrypted and associated with unique account addresses, providing secure access only to authorized users. Retrieval of dataset information is performed through smart contract functions, which allow users to fetch stored evidence details without altering the original data. The system supports continuous addition of new records, making the dataset scalable and adaptable to different cases. Unlike traditional databases, this dataset does not rely on a single server, reducing the risk of data loss or unauthorized manipulation. Overall, the dataset plays a vital role in maintaining a secure, reliable, and verifiable record of forensic evidence for investigation and legal purposes.

IV. PROPOSED METHODOLOGY

The proposed system uses blockchain technology to securely manage forensic evidence data. Initially, a smart contract is designed using Ethereum to define functions for storing and retrieving evidence details. The blockchain network is set up using tools like Truffle, which helps in deploying and testing the contract. A Python-based application, developed using Django, provides a user interface for authorized users such as administrators or police personnel. When evidence data is entered through the interface, it is processed and sent to the blockchain network. Each entry is converted into a transaction and stored as a block, ensuring data integrity and security.

Once the data is stored on the blockchain, it becomes immutable and can only be accessed through predefined smart contract functions. The system verifies each new transaction by linking it with the previous block using cryptographic hashing. This process maintains a continuous and secure chain of custody for all records. Users can retrieve stored evidence details through the application, which interacts with the blockchain using the contract address. The decentralized nature of the system ensures that data is not dependent on a single server, reducing risks of data loss or tampering while improving transparency and reliability.

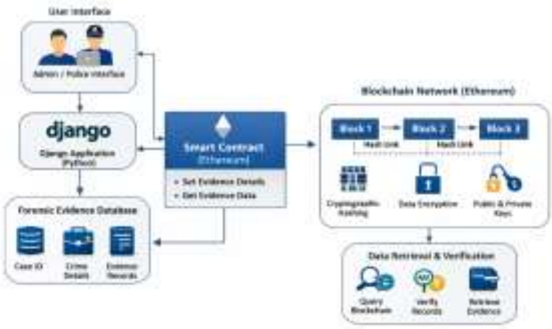

Figure [1] : System Architecture of Blockchain-Based Forensic Evidence Management System

Figure[1] The system allows admin or police users to enter and manage forensic evidence through a user interface. The Django application processes the data and connects it with the blockchain using smart contracts. Evidence details are securely stored in the Ethereum blockchain as linked blocks using cryptographic hashing. The system also enables retrieval and verification of stored data, ensuring transparency and tamper-proof records.

V.RESULT AND DISCUSSION

The implementation of the blockchain-based forensic evidence management system produced reliable and secure results in storing and retrieving evidence data. The system successfully allowed authorized users, such as administrators, to add crime-related information through the web interface. Each submitted record was converted into a blockchain transaction and stored as a block linked with previous entries using hash values. The results showed that once the data was recorded, it could not be modified or deleted, ensuring complete data integrity. The retrieval process was efficient, as users could fetch all stored evidence details through the application without any data loss. The integration of Django with Ethereum worked smoothly, enabling seamless communication between the user interface and blockchain network. The system also demonstrated proper generation of account addresses and secure handling of keys for encryption. Overall, the results confirm that the proposed system effectively maintains a tamper-proof record of forensic evidence and provides a transparent method for accessing stored information when required for investigation or legal use.

Figure [2] : Administrator Login Interface for Forensic Evidence Management System

Figure [2] This screen allows the administrator to securely log into the system using valid credentials. It contains fields for entering a username and password along with a login option. Only authorized users can access the system to manage forensic evidence data. This step ensures controlled access and protects sensitive information from unauthorized use.

Figure [3] : Forensic Evidence Data Entry Screen

Figure [3] This screen allows users to enter detailed information related to a crime case. It includes fields such as record ID, crime type, description, and collected evidence details. Additional inputs like crime location and witness information are also captured. After entering the details, the data is submitted and securely stored in the system.

Figure [4] : Stored Forensic Evidence Records Display Screen

Figure [4] This screen shows the list of evidence records stored in the system. It displays details such as record ID, crime type, description, and collected evidence. Additional information like crime area, witnesses, and date is also presented. Users can view all stored data, which is securely retrieved from the blockchain.

DISCUSSION

The developed system highlights the advantages of using blockchain technology in forensic evidence management. One of the key observations is the improvement in data security compared to traditional methods. Since the data is stored in a decentralized manner, it eliminates the risk associated with a single point of failure. The use of cryptographic hashing ensures that any attempt to alter stored records can be easily detected. Additionally, the system provides transparency by maintaining a clear history of all transactions, which is important in legal scenarios. However, the implementation also brings certain challenges. The complexity of setting up the blockchain environment and integrating it with existing applications requires technical expertise. There may also be concerns regarding scalability and transaction processing time as the number of records increases. Despite these limitations, the system proves to be a strong solution for maintaining the authenticity of forensic evidence. It enhances trust among investigators and supports accurate decision-making in the judicial process by ensuring that the data remains secure and verifiable.

VI. CONCLUSION

The proposed system demonstrates an effective approach for managing forensic evidence using blockchain technology. By replacing traditional storage methods with a decentralized structure, the system ensures that all records remain secure, transparent, and protected from unauthorized changes. Each piece of evidence is stored as a block linked through cryptographic techniques, which helps in maintaining data integrity and a clear chain of custody. The integration of Ethereum and a Python-based application provides a practical solution for storing and retrieving information in a reliable manner. The system also improves trust among investigators and legal authorities by ensuring that evidence cannot be altered once recorded. Although there are challenges such as system complexity and scalability, the overall benefits outweigh the limitations. This approach can be further enhanced with advanced features and wider adoption in real-world applications, making it a strong solution for modern forensic evidence management.

REFERENCES

1. Bonomi, S., Casini, M., & Ciccotelli, C. (2018). BCoC: Blockchain-based chain of custody for evidence management in digital forensics. arXiv preprint arXiv:1807.10359.

2. Gopalan, S. H., Suba, S. A., Ashmithashree, C., Gayathri, A., & Andrews, V. J. (2019). Application of blockchain in digital forensic systems. International Journal of Recent Technology and Engineering, 8(2S11), 182-184.

3. Bou Abdo, J., El Sibai, R., & Demerjian, J. (2020). A hybrid reputation-based consensus model for permissionless blockchain systems. Transactions on Emerging Telecommunications Technologies, 32(1).

4. Varshney, T., Sharma, N., Kaushik, I., & Bhushan, B. (2019). Security services in blockchain using authentication and encryption techniques. In Proceedings of the International Conference on Computing, Communication, and Intelligent Systems (pp. 63-68).

5. Kahate, A. (2003). Cryptography and network security. McGraw-Hill Education.

6. Guegan, D. (2017). Comparison of public and private blockchain systems.

7. National Institute of Standards and Technology (NIST). (2018). Blockchain technology overview.

8. Castor, A. (2017). Overview of blockchain consensus mechanisms. Coindesk.

9. Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Blockchain applications and future directions. IEEE Xplore.

10. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., et al. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. Proceedings of the Thirteenth EuroSys Conference, 1-15.

11. Goodell, G., & Aste, T. (2019). Decentralized digital identity systems using blockchain technology. Frontiers in Blockchain, 2.

12. Krstić, M., & Krstić, L. (2020). Overview of Hyperledger frameworks with emphasis on Hyperledger Fabric. Vojnotehnicki Glasnik, 68(3), 639-663.
13. Babburi, S. Privacy-Preserving Collaborative Framework with Auditable Federated Learning.
14. Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
15. Immadi, S. K. (2025). Optimizing ERP for Human Capital Management. Applied Research for Growth, Innovation and Sustainable Impact, 377–384. https://doi.org/10.1201/9781003684657-63
16. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
17. Poojari, R. INTELLIGENT SYSTEMS+B108 AND APPLICATIONS IN ENGINEERING.
18. Mahimalur, R. K., Vasgam, M., & Manoharan, D. Devops Lifecycle Management And Cloud Migration Assessments: A Security-Driven CICD Perspective.
19. Viswanathan, V. (2023). AI-Augmented Decision Intelligence for Enterprise Systems: Integrating Cognitive Analytics for Resource and Talent Optimization.
20. Agrawal, A. M., Gajula, S., Shinde, R. P., Shah, H., & Ghosh, H. (2025, July). Machine Translation for Long Sequences with Enhanced Attention Mechanisms. In 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1-6). IEEE.
21. Maturi, S. Y. (2021). Blockbond hardening: Securing pooled-hash protocols against

traffic tampering, MITM hash-rate hijacking, and template coercion. International Journal of Communication Networks and Information Security, 13(3), 718–728.

22. Adabala, P. K. (2024). Utilizing predictive analytics to improve efficiency and decision-making in ERP-connected supply chains. International Journal of Intelligent Systems and Applications in Engineering, 12(22s), 2465
23. Kavuri, S. (2026). An Explainable Machine Learning Framework for Predicting Software Defects in Large-Scale Software Systems. 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC), 1–6. https://doi.org/10.1109/icaic67076.2026.11395777
24. Gajula, S. (2025). Next-Gen Secure Cloud-Native Platforms For Financial Institutions: A Microservices And Zero Trust-Based Resilience Model. Journal of International Crisis and Risk Communication Research, 280–287. https://doi.org/10.63278/jicrcr.vi.3355
25. Shashank, A. (2025). Self-Healing Data Pipelines for Enhanced Reliability: A Paradigm Shift in Enterprise Data Management. Journal of Computer Science and Technology Studies, 7(8), 1097-1104.
26. Susarla, R. S., Boyapati, P. K., & Kandula, S. T. R. (2025, July). Cloud-Based Secure Data Storage in Smart Cities Using Central-Smoothing Hypergraph Neural Networks. In 2025 IEEE 4th World Conference on Applied Intelligence and Computing (AIC) (pp. 279-284). IEEE.
27. Boyapati, P. K. Building a centralized data operations hub for healthcare enterprise integration. IJSAT-Int. J. Sci. Technol. 16 (2). https://doi.org/10.71097/IJSAT.v16.i2.3219