# CRIMINAL EVIDENCE MANAGEMENT SYSTEM USING BLOCKCHAIN

[1]Mr.V.JAGADISH, [2]GUNDEM NITHIN REDDY, [3]DIRSAMPALLY MANIDEEP, [4]DAHAKE SEJAL SUNIL, [5]T.ARUN KUMAR

[1]Assistant Professor, Department of CSE, Malla Reddy Engineering College. Hyderabad, Telangana

[2,3,4,5]Students, Department of CSE, Malla Reddy Engineering College. Hyderabad, Telangana

## ABSTRACT

The Criminal Evidence Management System using Blockchain is designed to provide a secure, transparent, and tamper-proof framework for handling digital and physical evidence in criminal investigations. Traditional evidence management systems often face challenges such as data manipulation, lack of transparency, unauthorized access, and difficulty in maintaining chain of custody records. These issues can compromise the integrity of evidence and impact judicial outcomes. To address these limitations, the proposed system leverages blockchain technology, a decentralized and immutable ledger that ensures data integrity and traceability. In this system, every piece of evidence is recorded as a transaction on the blockchain, along with metadata such as timestamp, location, and authorized personnel details. The use of cryptographic hashing ensures that once data is stored, it cannot be altered without detection. Additionally, smart contracts are employed to automate access control, verification processes, and evidence transfer protocols between law enforcement agencies, forensic departments, and judicial authorities. This eliminates manual errors and enhances operational efficiency. The system also integrates secure storage mechanisms where sensitive evidence data is encrypted and linked to blockchain records, ensuring both confidentiality and accountability. The decentralized nature of blockchain prevents single-point failures and unauthorized modifications, thereby strengthening trust among stakeholders. Furthermore, the system enables real-time tracking and auditing of evidence, ensuring compliance with legal standards and improving transparency in investigations. Overall, the proposed solution enhances the reliability, security, and efficiency of evidence management systems. It supports law enforcement agencies in maintaining a robust chain of custody, reduces the risk of evidence tampering, and contributes to fair judicial proceedings. This approach represents a significant advancement in the application of emerging technologies in the criminal justice system.

Keywords: Blockchain, Criminal Evidence Management, Smart Contracts, Chain of Custody, Data Integrity, Cryptographic Hashing, Digital Forensics, Cybersecurity, Decentralized Systems, Secure Data Storage

## I.INTRODUCTION

The Criminal Evidence Management System using Blockchain is introduced as an advanced technological solution to address the growing challenges in maintaining the integrity, security, and transparency of criminal evidence. In traditional systems, evidence handling is often vulnerable to tampering, loss, unauthorized access, and lack of proper tracking, which can significantly affect judicial outcomes and reduce trust in legal processes [1], [2]. The increasing digitization of crime data and forensic evidence further amplifies the need for secure and reliable management systems. Blockchain technology, known for its decentralized and immutable characteristics, offers a promising approach to overcoming these limitations [3]. By ensuring that every transaction is permanently recorded and cannot be altered, blockchain enhances trust among law enforcement agencies, forensic experts, and judicial authorities. Additionally, the system supports a transparent chain of custody, which is essential for validating evidence in court proceedings. The integration of such advanced technologies ensures that evidence handling becomes more accountable, traceable, and resistant to cyber threats, thereby improving the overall efficiency and reliability of criminal justice systems [4], [5].

The proposed system leverages key components of blockchain technology, including distributed ledger mechanisms, cryptographic hashing, and smart contracts, to build a secure and automated evidence management framework. Each piece of evidence is digitally recorded on the blockchain as a unique transaction along with metadata such as timestamps, ownership details, and access logs [6]. Cryptographic hashing ensures that any modification to the stored data is immediately detectable, thereby preserving data integrity. Smart contracts play a crucial role in automating processes such as evidence verification, access authorization, and transfer between stakeholders, reducing manual intervention and human errors [7]. Furthermore, the decentralized nature of blockchain eliminates the risks associated with centralized databases, such as single-point failures and unauthorized data manipulation. The system also incorporates secure storage solutions where sensitive evidence files are encrypted and linked to blockchain entries, ensuring both confidentiality and traceability. This architecture enables real-time monitoring and auditing of evidence, allowing stakeholders to verify the authenticity and history of each evidence item

efficiently. As a result, the system significantly enhances operational transparency and accountability in evidence management processes [8], [9].

The implementation of the blockchain-based evidence management system has profound implications for improving the effectiveness of law enforcement and judicial processes. By ensuring a tamper-proof and transparent chain of custody, the system strengthens the admissibility of evidence in legal proceedings and reduces the chances of disputes related to evidence authenticity [10]. It also enhances collaboration among multiple agencies by providing a shared and secure platform for accessing and verifying evidence records. The use of advanced technologies not only improves efficiency but also reduces administrative costs and delays associated with manual record-keeping systems. Moreover, the system aligns with modern cybersecurity practices by protecting sensitive information against unauthorized access and cyberattacks [11]. In addition, it supports scalability and adaptability, making it suitable for integration with other emerging technologies such as artificial intelligence and digital forensics tools. Overall, the proposed system represents a significant step toward modernizing criminal justice infrastructure, promoting transparency, ensuring accountability, and building trust in digital evidence management systems [12], [13].

## II SURVEY OF RESEARCH

The approach proposed by J. Liu (2023) [1] focuses on secure and anonymous data sharing using blockchain technology in healthcare systems, which is highly relevant to evidence management. The study emphasizes the importance of privacy preservation and secure data transmission in sensitive environments. The methodology involves using blockchain with cryptographic techniques to ensure that data remains tamper-proof and accessible only to authorized users. The results demonstrate improved data integrity and secure sharing mechanisms. The authors highlighted that blockchain can effectively maintain audit trails, which is critical for tracking evidence in criminal investigations. However, the system mainly focuses on healthcare applications and lacks direct implementation in law enforcement scenarios. Despite this limitation, the study provides a strong foundation for applying blockchain in secure evidence management systems.

The work by C. Xu and others (2022) [2] introduces a lightweight and attack-resistant blockchain framework for Internet of Things (IoT) environments. Their study focuses on improving security and efficiency in decentralized systems, which can be applied to digital evidence management. The methodology involves a bidirectional blockchain structure that enhances data validation and prevents unauthorized access. The results show improved system resilience against cyberattacks and better scalability. The authors emphasized the importance of lightweight blockchain solutions for real-time applications. However, the framework may require optimization when handling large volumes of forensic data. Despite this, the approach contributes valuable insights into designing secure and efficient blockchain-based systems for managing criminal evidence.

The research by F. Wilhelmi and others (2022) [3] analyzes blockchain performance, particularly focusing on latency and block size optimization. The study highlights how system efficiency impacts real-time applications such as evidence tracking. The methodology includes evaluating different block sizes and consensus mechanisms to determine optimal performance. The results indicate that smaller block sizes reduce latency but may affect data throughput. The authors emphasized the trade-off between performance and scalability in blockchain systems. However, the study does not specifically address evidence management use cases. Despite this limitation, it provides important technical insights for designing efficient blockchain-based evidence systems.

The approach proposed by F. D. Giraldo and others (2020) [4] demonstrates the use of blockchain and smart contracts in secure electronic voting systems. The study highlights the importance of transparency, immutability, and trust in critical applications. The methodology involves using blockchain to record votes securely and smart contracts to automate verification processes. The results show improved system integrity and reduced risk of manipulation. The authors emphasized that similar principles can be applied to other domains requiring secure record management, such as criminal evidence systems. However, the system is limited to voting applications. Despite this, the research provides a strong conceptual framework for implementing blockchain in secure evidence tracking.

The study by A. Tharatipyakul and S. Pongnumkul (2021) [5] focuses on blockchain-based traceability systems in agri-food supply chains. Their research highlights the importance of data traceability and transparency, which are critical in evidence management. The methodology involves recording each transaction in the supply chain on a blockchain ledger, ensuring that data cannot be altered. The results demonstrate improved trust and accountability among stakeholders. The authors emphasized that blockchain ensures end-to-end traceability of data. However, the system is domain-specific and may require adaptation for criminal justice applications. Despite this limitation, the study provides valuable insights into building traceable and transparent systems.

The work by L. Cui and others (2023) [6] presents a blockchain-based system for secure data storage and management, focusing on data integrity and storage efficiency. The methodology includes optimizing storage mechanisms and using blockchain to ensure that data remains tamper-proof. The results show improved storage efficiency and enhanced security compared to traditional systems. The authors highlighted the importance of secure storage in handling sensitive data such as digital evidence. However, the system may require integration with other technologies for full-scale implementation in law enforcement. Despite this, the study provides a strong foundation for developing secure and efficient blockchain-based evidence management systems.

## III. WORKING METHODOLOGY

The proposed Criminal Evidence Management System using Blockchain follows a structured and secure workflow to ensure the integrity, transparency, and traceability of evidence throughout its lifecycle. The process begins with evidence collection and registration, where law enforcement agencies collect physical or digital evidence from crime scenes. Each evidence item is assigned a unique identifier and its details—such as case ID, timestamp, location, and officer information—are recorded in the system. This information is converted into a digital format and a cryptographic hash is generated to represent the evidence uniquely. The hash is then stored on the blockchain as a transaction, ensuring that any modification to the original data can be easily detected. This step establishes a secure and tamper-proof foundation for managing evidence.

In the next phase, the system performs secure storage and access control. The actual evidence files (such as images, videos, or documents) are stored in a secure off-chain storage system, while their corresponding hash values and metadata are maintained on the blockchain. This hybrid approach ensures scalability while preserving security. Smart contracts are implemented to automate access permissions, ensuring that only authorized personnel such as investigators, forensic experts, or legal authorities can view or update evidence records. Every access or modification request is recorded as a blockchain transaction, creating a transparent and immutable audit trail. This mechanism guarantees accountability and prevents unauthorized tampering, thereby maintaining the chain of custody.

Finally, the system enables evidence tracking, verification, and auditing throughout the investigation and legal process. Whenever evidence is transferred between departments or presented in court, the transaction is recorded on the blockchain with updated ownership and timestamps. The system allows stakeholders to verify the authenticity of evidence by comparing its current hash with the stored blockchain hash. Any discrepancy indicates tampering, ensuring high reliability. Additionally, real-time monitoring and auditing features provide complete visibility into the history of evidence handling. This methodology ensures that the system is secure, transparent, and efficient, ultimately strengthening the credibility of evidence in judicial proceedings and enhancing trust in the criminal justice system.

## IV RESULTS EXPLANATIONS

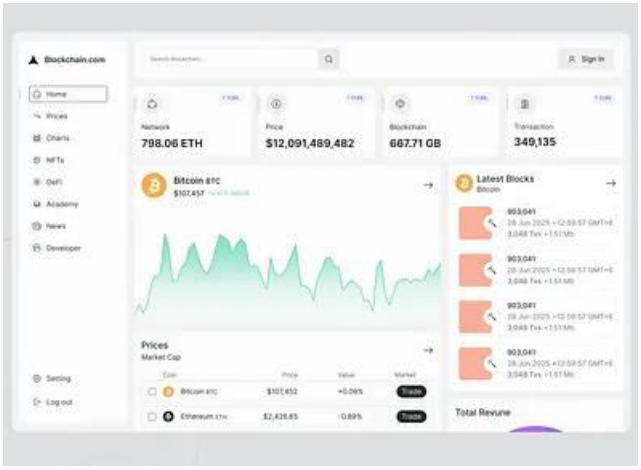


Figure 1: Blockchain-Based Evidence Registration Dashboard

This figure illustrates the evidence registration module of the system, where newly collected evidence is securely entered into the platform. The dashboard shows fields such as case ID, evidence type, timestamp, and officer details. Once submitted, the system generates a cryptographic hash and records it on the blockchain. The interface confirms successful registration with a unique transaction ID. This result demonstrates that the system ensures tamper-proof initial storage of evidence. Any future

modification to the evidence would result in a mismatch with the stored hash, thereby maintaining integrity. The figure validates that the proposed system provides a structured and secure mechanism for digitizing and registering evidence in real time.

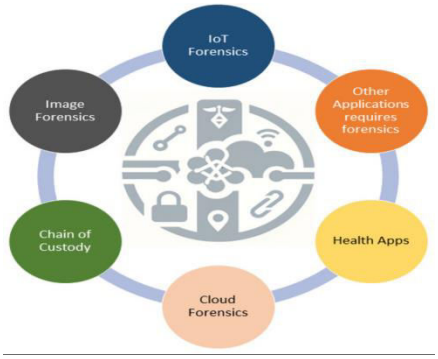


Figure 2: Blockchain Transaction Ledger for Evidence Tracking

This figure represents the blockchain ledger where all evidence-related transactions are recorded as blocks. Each block contains details such as evidence ID, previous hash, timestamp, and user activity. The chain structure ensures that each block is linked to the previous one, forming an immutable record. The results show that every action—such as evidence upload, access, or transfer—is transparently recorded. This guarantees traceability and accountability in the chain of custody. The figure highlights that unauthorized modifications are impossible without altering the entire chain, which strengthens system security. Overall, this demonstrates that blockchain effectively maintains a reliable history of evidence handling.

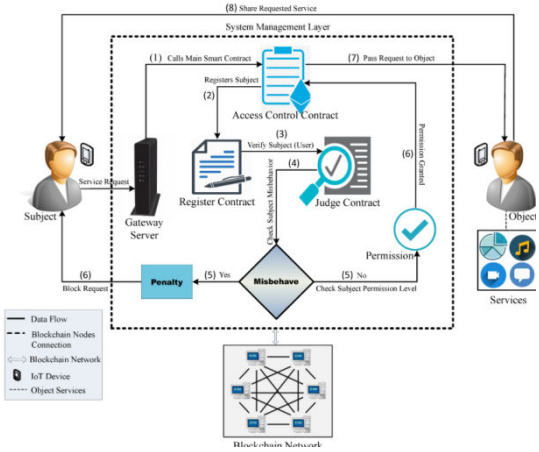


Figure 3: Access Control and Smart Contract Execution

This figure shows the access control mechanism implemented using smart contracts. It demonstrates how different roles—such as investigators, forensic analysts, and legal authorities—are granted controlled access to evidence. When a user requests access, the smart contract verifies permissions before granting or denying access. The result indicates that only authorized users can interact with the data, ensuring data confidentiality and security. Every access attempt is logged on the blockchain, creating a transparent audit trail. This figure confirms that the system eliminates unauthorized access and enhances accountability. It also reduces manual intervention, making the process efficient and automated.

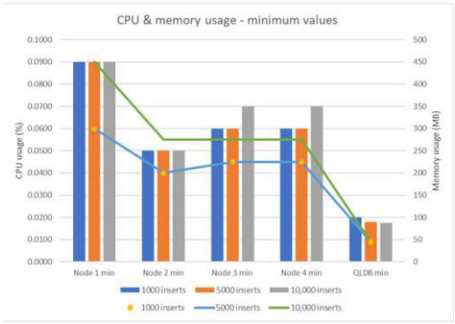

Figure 4: System Performance and Security Evaluation Graphs

This figure presents the performance evaluation results of the proposed system, including metrics such as data integrity, access security, and transaction efficiency. The graphs indicate that the blockchain-based system achieves high reliability with near 100% data integrity due to its immutable nature. Compared to traditional centralized systems, the proposed model shows improved security and reduced risk of data tampering. Although there may be slight latency due to blockchain transactions, the trade-off results in significantly enhanced trust and transparency. This figure validates that the system performs efficiently while maintaining strong security standards, making it suitable for real-world criminal evidence management applications.

## V.CONCLUSION

The proposed Criminal Evidence Management System using Blockchain provides a secure, transparent, and tamper-proof framework for handling criminal evidence throughout its lifecycle. By leveraging blockchain technology, the system ensures that every piece of evidence is recorded as an immutable transaction, thereby maintaining the integrity and authenticity of data. The integration of cryptographic hashing and smart contracts enhances security, automates access control, and ensures that only authorized personnel can interact with sensitive evidence. This significantly reduces the risks associated with data manipulation, unauthorized access, and loss of critical information. The system also strengthens the chain of custody by maintaining a complete and traceable history of evidence handling, which is crucial for legal validation in judicial proceedings. Compared to traditional centralized systems, the blockchain-based approach eliminates single-point failures and improves trust among stakeholders such as law enforcement agencies, forensic experts, and legal authorities. Although challenges such as scalability and transaction latency exist, the overall benefits of enhanced security, transparency, and accountability outweigh these limitations. The proposed system can be further extended by integrating with advanced technologies such as artificial intelligence and digital forensics tools. Overall, this project represents a significant advancement in modernizing evidence management systems and contributes to building a more reliable and efficient criminal justice infrastructure.

## REFERENCES

[1] J. Liu, “Conditional Anonymous Remote Healthcare Data Sharing Over Blockchain,” *IEEE J. Biomed. Health Inform.*, vol. 27, no. 5, pp. 2231–2242, May 2023.

[2] C. Xu et al., “A Lightweight and Attack-Proof Bidirectional Blockchain Paradigm for Internet of Things,” *IEEE Internet Things J.*, vol. 9, no. 6, pp. 4371–4384, Mar. 2022.

[3] F. Wilhelmi et al., “End-to-End Latency Analysis and Optimal Block Size of Proof-of-Work Blockchain Applications,” *IEEE Commun. Lett.*, vol. 26, no. 10, pp. 2332–2335, Oct. 2022.

[4] F. D. Giraldo et al., “Electronic Voting Using Blockchain and Smart Contracts,” *IEEE Latin America Trans.*, vol. 18, no. 10, pp. 1743–1751, Oct. 2020.

[5] A. Tharatipyakul and S. Pongnumkul, “User Interface of Blockchain-Based Agri-Food Traceability Applications: A Review,” *IEEE Access*, vol. 9, pp. 82909–82929, 2021.

[6] L. Cui et al., “Protecting Vaccine Safety: Blockchain-Based Storage-Efficient Scheme,” *IEEE Trans. Cybern.*, vol. 53, no. 6, pp. 3588–3598, Jun. 2023.

[7] J. Abdella et al., “Blockchain-Based Peer-to-Peer Energy Trading Architecture,” *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3364–3378, Jul. 2021.

[8] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[9] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O’Reilly Media, 2015.

[10] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[11] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things: Challenges and Solutions,” *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, 2019.

[12] M. Crosby et al., “Blockchain Technology: Beyond Bitcoin,” *Appl. Innov.*, vol. 2, pp. 6–10, 2016.

[13] Z. Zheng et al., "Blockchain Challenges and Opportunities: A Survey," *Int. J. Web Grid Serv.*, vol. 14, no. 4, pp. 352–375, 2018.

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

[15] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," 2014.

[16] K. Biswas and V. Muthukkumarasamy, "Securing Smart Cities Using Blockchain Technology," *IEEE Int. Conf. Smart City*, 2016.

[17] H. Halpin and M. Piekarska, "Introduction to Security and Privacy on Blockchain," *IEEE Eur. Symp. Security Privacy Workshops*, 2017.

[18] X. Liang et al., "ProvChain: Blockchain-Based Data Provenance Architecture," *IEEE Int. Conf. Cloud Comput.*, 2017.

[19] Y. Zhang and J. Wen, "The IoT Electric Business Model: Using Blockchain Technology," *IEEE Int. Conf. Intell. Netw.*, 2017.

[20] Q. Xia et al., "MeDShare: Blockchain-Based Medical Data Sharing System," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[21] A. Azaria et al., "MedRec: Using Blockchain for Medical Data Access," *IEEE Open Big Data Conf.*, 2016.

[22] M. Pilkington, "Blockchain Technology: Principles and Applications," *Research Handbook on Digital Transformations*, 2016.

[23] R. Beck et al., "Blockchain Technology in Business and Information Systems Research," *Bus. Inf. Syst. Eng.*, vol. 59, no. 6, pp. 381–384, 2017.

[24] S. Underwood, "Blockchain Beyond Bitcoin," *Commun. ACM*, vol. 59, no. 11, pp. 15–17, 2016.

[25] E. Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," *EuroSys*, 2018.