International Journal of Advanced Trends in Engineering and Management
(ISSN 2583-7052)

pp. 40-43, May

Securing Forensic Evidence using Blockchain

Suguna A[1*], Pavitra C[2], Aishwaryaa R[3], Vegash P[4], Sriram V[5]

[1]Assistant Professor, Department of Computer Science and Engineering, Sri Sairam College of Engineering, Bangalore, 560126.

[2,3,4,5] Department of Computer Science and Engineering, Sri Sairam College of Engineering, Bangalore, 560126.

ABSTRACT: In today's digital era, the protection and management of data have become essential across all fields. With the increasing risks of tampering and cyberattacks, ensuring the security and authenticity of sensitive information is critical, especially for forensic evidence. Cybercriminals often attempt to alter crucial data, threatening the reliability needed for legal investigations. To address these challenges, it is vital to maintain the integrity and traceability of forensic evidence as it moves through various stakeholders, including pathology labs, hospitals, and law enforcement agencies. Blockchain technology provides an ideal solution by offering a decentralized, transparent, and immutable system for managing forensic evidence. This paper proposes a blockchain-based framework for securely handling forensic reports, implemented on the Ethereum platform. By leveraging smart contracts and cryptographic methods, the system ensures evidence integrity, making tampering easily detectable at any stage in the chain of custody.

Keywords: Blockchain, Forensic Evidence, Digital Signature, Smart Contracts, Chain of Custody, Data Integrity, Decentralization.

1. Introduction

Blockchain technology has emerged as a powerful distributed and decentralized platform, replacing traditional centralized systems. It organizes data into blocks that are cryptographically linked, ensuring transparency, security, and trust among participants. Blockchain employs consensus mechanisms to validate transactions, eliminating the need for intermediaries and significantly reducing costs and fraud risks. This structure guarantees data immutability, meaning records, once added, cannot be altered without detection. The distributed ledger technology is being adopted across several domains, including the Internet of Things, legal and public sectors, supply chain management, media, and healthcare. Blockchain enhances the traceability of digital assets and ensures the authenticity of transactional data, making it highly suitable for digital transformation efforts. Despite being in a developmental phase, blockchain continues to show promise through various proofs of concept and real-world implementations.

2. Recent Works

Multiple studies have explored how blockchain can enhance the security and traceability of digital forensic evidence. Adarsh Mandadi et al. (2022) examined diverse blockchain applications aimed at preserving the integrity of forensic data, emphasizing the necessity of robust consensus algorithms. Edward Wijaya et al. (2023) introduced a hybrid system combining Ethereum and Hyperledger Sawtooth to overcome scalability challenges while securing forensic records. Ammar Odeh et al. (2021) reviewed blockchain-based solutions that incorporate encryption and smart contracts to bolster evidence authenticity. V. Dharani et al. (2023) highlighted the significance of maintaining chain-of-custody logs with timestamping and strict access controls. Additionally, Kerin Pithawala et al. (2021) investigated the role of blockchain in integrating

IoT devices for tamper-resistant forensic storage. While these works contributed valuable perspectives, many depended on static datasets or conventional models. In contrast, our approach introduces the PHISHNET system, integrating smart contracts and digital signatures to deliver real-time traceability, enhanced security, and privacy without relying solely on static storage methods.

3. Proposed Work Explanation

3.1 Introduction to Blockchain and Evidence Management

The proposed project focuses on applying blockchain technology to forensic evidence management, aiming to improve transparency, security, and data integrity. From evidence collection to courtroom presentation, blockchain's core properties—decentralization, immutability, and traceability—safeguard the chain of custody. As reliance on digital evidence grows, particularly in cybercrime investigations, the demand for a trustworthy and auditable management system becomes critical. This work addresses that need by creating a decentralized and verifiable platform for forensic evidence tracking.

3.2 Project Objectives

- **Blockchain-Based Evidence Management**: Develop an immutable ledger to log forensic evidence transactions for full traceability.
- **Maintaining Chain of Custody**: Ensure transparent and auditable custody records across the evidence lifecycle.
- **Enhanced Security**: Apply cryptographic methods, including digital signatures and hashing, to prevent evidence tampering.
- **Automated Processes**: Use smart contracts to automate critical steps like evidence transfer and validation, minimizing human errors.
- **System Compatibility**: Design the solution to integrate seamlessly with existing forensic and legal frameworks to facilitate widespread adoption.

3.3 Project Significance

- **Enhanced Evidence Credibility**: Blockchain's tamper-proof nature increases the reliability and admissibility of forensic evidence in court.
- **Reduced Tampering Risks**: Decentralized validation processes prevent centralized manipulation of records.
- **Efficient Evidence Handling**: Automated workflows improve operational efficiency and reduce processing delays.
- **Streamlined Authentication**: Blockchain's transparent and secure ledger simplifies the process of verifying evidence authenticity.

3.4 The System Architecture Involves Four Major Nodes

Pathology Lab, Hospital, Police Department, and Final Report Administrator, each playing a role in maintaining evidence integrity across the blockchain network.

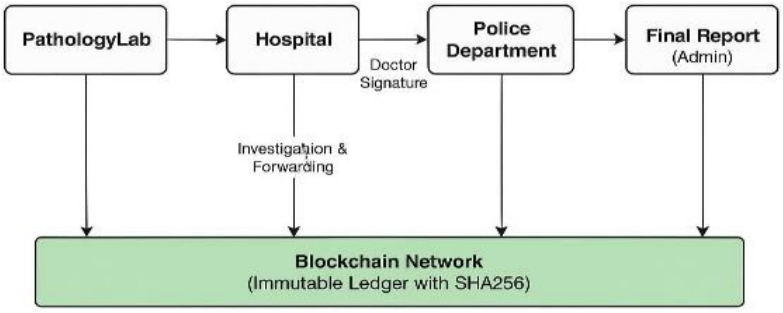

Figure 1: *Blockchain-Based Forensic System*

3.4.1 Pathology Lab

The Pathology Lab is responsible for generating the initial forensic report. In conventional systems, reports are sent via email or hard copy, which leaves room for tampering. In the proposed blockchain-based system, the report is uploaded to a distributed ledger, ensuring immutability and resistance to unauthorized alterations. Even in the event of a node failure, the data can be retrieved from other nodes on the network.

3.4.2 Hospital

The Hospital node receives the forensic report from the Pathology Lab and assigns a doctor to verify it. After verification, the doctor appends a digital signature to the report. Since the report is protected by a cryptographic hash generated at the time of upload, any unauthorized modifications result in a detectable change in the hash. The Hospital also maintains a record of the report in its local ledger.

3.4.3 Police Department

The Police Department node receives the digitally signed report for further investigation. Because the report has already been authenticated by the previous nodes, the police officercan rely on its integrity. Any attempts to alter the report are evident due to changes in the hash values, which are traceable through the blockchain's immutable history.

3.4.4 Final Report (Admin)

The Final Report node, managed by the administrator of the blockchain network, allows for the comprehensive review of the transaction history associated with the forensic report. This module ensures end-to-end traceability and confirms that the original data has not been tampered with by comparing hash values across the blockchain. Any discrepancies can be traced back to the specific node where tampering occurred.

4. Results and Discussion

The blockchain-based forensic evidence management system achieved its primary goals: ensuring immutability, traceability, transparency, and security. Real-time simulations were conducted where forensic reports traveled across multiple network nodes—Pathology Lab, Hospital, Police Department, and Admin. At every transition, cryptographic signatures and SHA-256 hashing were used to verify report integrity. No unauthorized changes went unnoticed, demonstrating the effectiveness of the system's security mechanisms. Unlike traditional systems that often depended on physical or unsecured digital exchanges, the proposed blockchain model flagged any alteration attempts through immediate hash mismatches. Furthermore, every action—such as uploading, signing, or transferring reports— was permanently recorded on the Ethereum blockchain, enabling comprehensive audit trails and greater trust.

5. Conclusions

Integrating blockchain technology into forensic evidence management significantly strengthens the security, transparency, and integrity of digital evidence throughout its lifecycle. By utilizing blockchain's decentralized and immutable ledger, the system ensures that evidence remains tamper-resistant and verifiable, thereby enhancing its credibility in legal proceedings. The project effectively addresses critical challenges such as maintaining chain of custody, automating evidence processing through smart contracts, and improving transparency within the judicial system. Although blockchain offers substantial benefits, challenges like scalability and integration with legacy systems must still be addressed. Future enhancements could involve incorporating machine learning for advanced evidence analysis, extending cross-border evidence management capabilities, and improving blockchain scalability to support broader adoption. Overall, the system lays a strong foundation for revolutionizing global forensic evidence handling practices.

References

1. Satoshi Nakamoto, Year: 2008, “Bitcoin: A peer-to-peer electronic cash system”.

2. Zibin Zheng; Shaoan Xie; Hongning Dai; Xiangping Chen; Huaimin Wang, Year: 2017, “An overview of blockchain technology: Architecture, consensus, and future trends”, In 2017 IEEE international congress on big data (BigData congress), pp. 557 – 564.

3. Vitalik Buterin, Year: 2014, “A next-generation smart contract and decentralized application platform”, white paper, Vol: 3, No: 37, pp. 2 – 1.

4. Wenbo Wang; Dinh Thai Hoang, Year: 2016, “A survey on consensus mechanisms and mining strategy management in blockchain networks”, IEEE Access, Vol: 4, pp. 556 – 564.

5. M. Macdonald; L. Liu-Thorrold; R. Julien, Year: 2016, “The blockchain: A comparison of platforms and their users beyond Bitcoin,” COMS4507: Adv. Computer and Network Security, pp. 1 – 18.

6. Amitai Porat; Avneesh Pratap; Parth Shah; Vinit Adkar, Year: 2017, “Blockchain Consensus: An analysis of Proof-of-Work and its applications”.

7. Kaspars Zile; Renate Strazdina, Year: 2018, “Blockchain and use cases and their feasibility,” Appl. Computer Syst., Vol: 23, pp. 45 – 54.

8. Stephen O’shaughnessy; Anthony Keane, Year: 2013, “Impact of cloud computing on digital forensic investigations”, In Advances in Digital Forensics IX: 9th IFIP WG 11.9 International Conference on Digital Forensics, Orlando, FL, USA, January 28 – 30, 2013, Revised Selected Papers, Vol: 9, pp. 291 – 303.

9. Shijie Chen; Chengqiang Zhao; Lingling Huang; Jing Yuan; Mingzhe Liu, Year: 2020, “Study and implementation on the application of blockchain in electronic evidence generation”, Forensic Science International: Digital Investigation, Vol: 35, p. 301001.

10. Zibin Zheng; Shaoan Xie; Hongning Dai; Xiangping Chen; Huaimin Wang, Year; 2017, “An overview of blockchain technology: Architecture, consensus, and future trends”, In 2017 IEEE international congress on big data (BigData congress), pp. 557 – 564.

11. Giuliano Giova, Year: 2011, “Improving chain of custody in forensic investigation of electronic digital systems”, Int. J. Computer Sci. and Network Security, Vol: 11, No: 1, pp. 1 – 9.

12. Lamprini Zarpala; Fran Casino, Year: 2021, “A blockchain-based forensic model for financial crime investigation: the embezzlement scenario”, Digital Finance, Vol: 3, pp. 301– 332.

13. Auqib Hamid Lone; Roohie Naaz Mir, Year: 2018, “Forensic-chain: Ethereum blockchain based digital forensics chain of custody”, Sci. Pract. Cyber Secur. pp. 21 – 27.

14. Hyperledger Project. [Online]. Available: https://www.hyperledger.org