BLOCKCHAIN BASED CRIME EVIDENCE SYSTEM

SMD Shafiulla*[a], Dr.A.Balaram[b], Dr.G.Anil Kumar[c], K.Nagalatha[d]

M.Jyothi[e]

[a,d,e]*Assistant Professor, Department of CSE, Scient Institute of Technology, India*

[b,c]*Professor, Department of CSE, Scient Institute of Technology, India*

ABSTRACT: In recent years, the integrity and security of digital evidence have become critical challenges in criminal investigations. Traditional evidence management systems are often centralized and vulnerable to tampering, unauthorized access, and data loss, which can compromise the credibility of evidence in legal proceedings. This project proposes a Blockchain-Based Crime Evidence System that leverages the decentralized and immutable nature of blockchain technology to securely store and manage digital evidence. The system ensures that once evidence is recorded on the blockchain, it cannot be altered or deleted, thereby maintaining its authenticity and integrity.

The proposed system allows authorized users such as law enforcement agencies, forensic experts, and judicial authorities to upload, verify, and access evidence through a secure platform. Each piece of evidence is encrypted and stored along with a unique hash value, which acts as a digital fingerprint. Blockchain ensures that any attempt to modify the data can be easily detected due to changes in the hash values. Smart contracts are used to automate processes such as evidence verification, access control, and chain-of-custody tracking, ensuring transparency and accountability throughout the investigation process.

Additionally, the system enhances trust among stakeholders by providing a tamper-proof audit trail of all activities related to the evidence. It reduces dependency on centralized authorities and minimizes the risk of data manipulation. The integration of blockchain with secure storage and encryption techniques makes the system robust and reliable for modern digital forensics. Overall, the proposed solution improves the efficiency, transparency, and security of crime evidence management, making it suitable for real-world law enforcement applications.

Keywords: Blockchain, Digital Evidence, Cybersecurity, Smart Contracts, Data Integrity, Chain of Custody, Cryptographic Hash, Decentralized System, Forensic Analysis, Secure Storage

I. INTRODUCTION

The increasing reliance on digital technologies in modern society has led to a significant rise in cybercrime and digital offenses. As a result, digital evidence has become a crucial component in criminal investigations and legal proceedings. Digital evidence includes data such as emails, documents, images, videos, and system logs that can be used to establish facts in a case. However, managing and preserving the integrity of such evidence is a major challenge. Traditional evidence management systems are often centralized, making them vulnerable to unauthorized access, tampering, and data loss. These vulnerabilities can compromise the authenticity of evidence and weaken its admissibility in court.

Ensuring the integrity and authenticity of evidence is essential for maintaining trust in the judicial system. One of the key challenges in evidence management is maintaining a proper chain of custody, which records every action taken on the evidence from collection to presentation in court. In traditional systems, maintaining this chain is often manual and prone to errors or manipulation. Any break or inconsistency in the chain of custody can raise doubts about the validity of the evidence. Therefore, there is a need for a secure and transparent system that can track and verify all interactions with digital evidence in a reliable manner.

Blockchain technology has emerged as a promising solution to address these challenges. Blockchain is a decentralized and distributed ledger system that records transactions in a secure and immutable manner. Each block in the blockchain contains a set of records and is linked to the previous block using cryptographic hash functions. Once data is added to the blockchain, it cannot be altered without affecting all subsequent blocks, making it highly resistant to tampering. This immutability property makes blockchain an ideal technology for managing sensitive data such as crime evidence.

The use of blockchain in evidence management allows for secure storage, transparent access control, and reliable tracking of all activities related to the evidence. Each piece of evidence can be assigned a unique hash value, which serves as its digital identity. Any modification to the evidence will result in a change in the hash, making tampering easily detectable. Additionally, smart contracts can be used to automate processes such as evidence submission, verification, and access permissions. This reduces human intervention and ensures that all operations are carried out according to predefined rules.

This project focuses on the development of a Blockchain-Based Crime Evidence System that enhances the security, transparency, and reliability of evidence management. The system aims to provide a tamper-proof platform for storing and accessing digital evidence while maintaining a complete and verifiable chain of custody. By integrating blockchain technology with cryptographic techniques and secure storage mechanisms, the proposed solution offers a modern approach to handling digital evidence. It has the potential to improve the efficiency of law enforcement agencies and strengthen the credibility of evidence in legal proceedings.

II. SURVEY OF RESEARCH

Early research in crime evidence management systems primarily relied on centralized databases and manual record-keeping methods. These systems were designed to store and manage digital evidence collected during investigations. However, centralized systems posed significant challenges, including vulnerability to unauthorized access, data tampering, and single points of failure. Researchers identified that maintaining data integrity and ensuring a secure chain of custody were major concerns in traditional systems. Any alteration or loss of evidence could compromise investigations and reduce the reliability of evidence in legal proceedings.

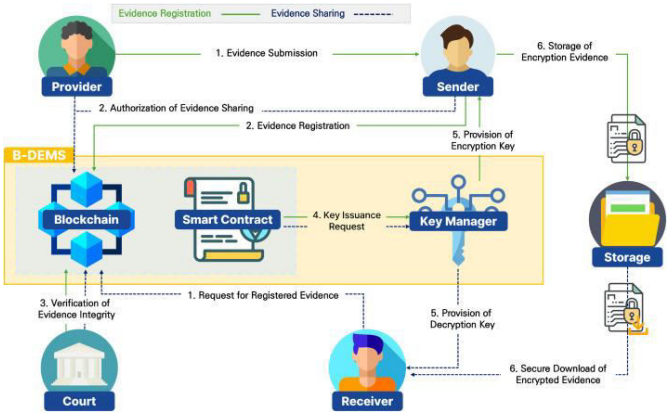
With the advancement of digital forensics, researchers began exploring secure methods for storing and verifying digital evidence. Techniques such as cryptographic hashing and digital signatures were introduced to ensure data integrity. Hash functions were used to generate unique fingerprints for evidence, allowing verification of whether the data had been altered. Digital signatures provided authentication by verifying the identity of the person handling the evidence. While these methods improved security, they still relied on centralized systems, which remained susceptible to internal threats and data manipulation.

The emergence of blockchain technology introduced a new paradigm for secure data management. Researchers started investigating the use of blockchain in digital forensics and evidence management due to its decentralized and immutable nature. Studies demonstrated that blockchain could provide a tamper-proof ledger where every transaction is recorded and verified by multiple nodes. This eliminates the need for a central authority and reduces the risk of data manipulation. Blockchain-based systems also ensure transparency, as all transactions are recorded and can be audited at any time.

Recent research has focused on integrating blockchain with smart contracts to automate evidence handling processes. Smart contracts are self-executing programs that enforce predefined rules and conditions. In the context of crime evidence systems, they can be used to automate tasks such as evidence submission, access control, and verification. This reduces human intervention and minimizes the chances of errors or unauthorized actions. Researchers have also explored combining blockchain with cloud storage to handle large volumes of data, as storing large files directly on the blockchain can be inefficient.

Furthermore, modern studies are exploring hybrid systems that combine blockchain with advanced technologies such as artificial intelligence and Internet of Things (IoT). AI can be used to analyze evidence and detect patterns, while IoT devices can collect real-time data from crime scenes. These technologies, when integrated with blockchain, enhance the overall efficiency and intelligence of evidence management systems. Despite these advancements, challenges such as scalability, storage limitations, and regulatory concerns remain active areas of research. Overall, the evolution of research in this field highlights the growing importance of blockchain technology in ensuring secure and reliable crime evidence management.

IV. IMPLEMENTATION



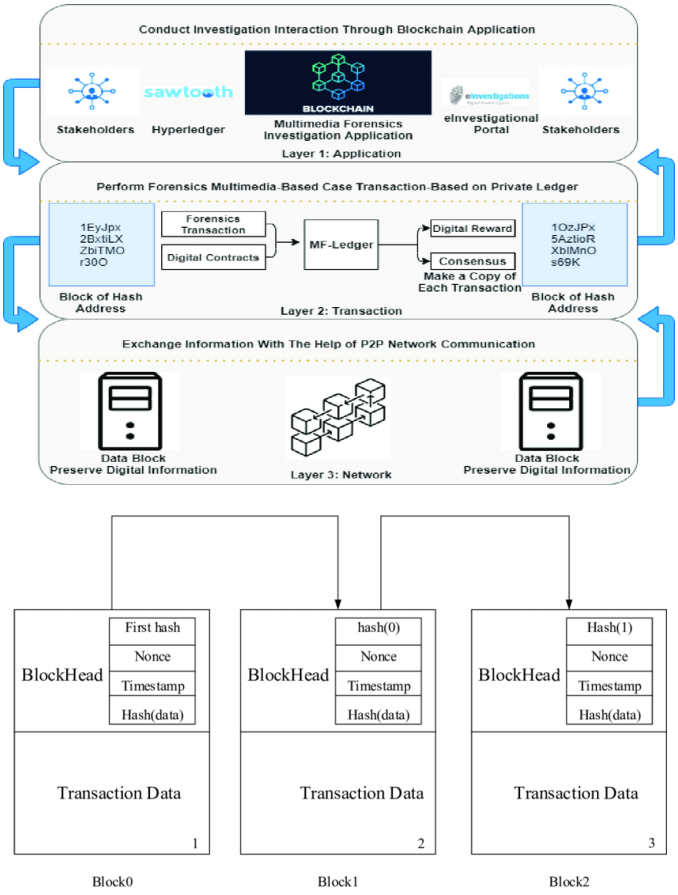


Fig.2. Implementation of Blockchain-Based Evidence System

The implementation of the Blockchain-Based Crime Evidence System involves integrating blockchain technology with secure storage and application interfaces. The system is developed using a combination of web technologies, blockchain platforms such as Ethereum, and programming languages like Solidity, Python, or JavaScript. The implementation is divided into modules including evidence upload, hash generation, blockchain storage, and access control.

In the first stage, the user interface is designed to allow authorized users such as law enforcement officers to upload digital evidence. When evidence is uploaded, the system generates a cryptographic hash using algorithms such as SHA-256. This hash uniquely represents the evidence and ensures that any modification can be detected. The original file is stored in a secure database or cloud storage, while the hash and related metadata are prepared for blockchain storage.

Smart contracts are developed using Solidity to manage the logic of the system. These contracts define rules for uploading evidence, verifying ownership, and controlling access permissions. When a user uploads evidence, a transaction is created and sent to the blockchain network. The smart contract verifies the transaction and records the hash, timestamp, and user details on the blockchain. This ensures that all records are immutable and traceable.

The blockchain network, such as Ethereum, processes the transactions through consensus mechanisms, ensuring that all nodes agree on the validity of the data. Once confirmed, the data becomes part of the blockchain and cannot be altered. The system also provides functionality

for retrieving and verifying evidence. When a user requests access, the system compares the stored hash with the current hash of the file to confirm its integrity.

Overall, the implementation demonstrates a secure and transparent system for managing digital evidence. The use of blockchain ensures immutability, while smart contracts automate processes and reduce human intervention. The system can be deployed as a web or cloud-based application, making it accessible and scalable for real-world use.

V. RESULTS EXPLANATION

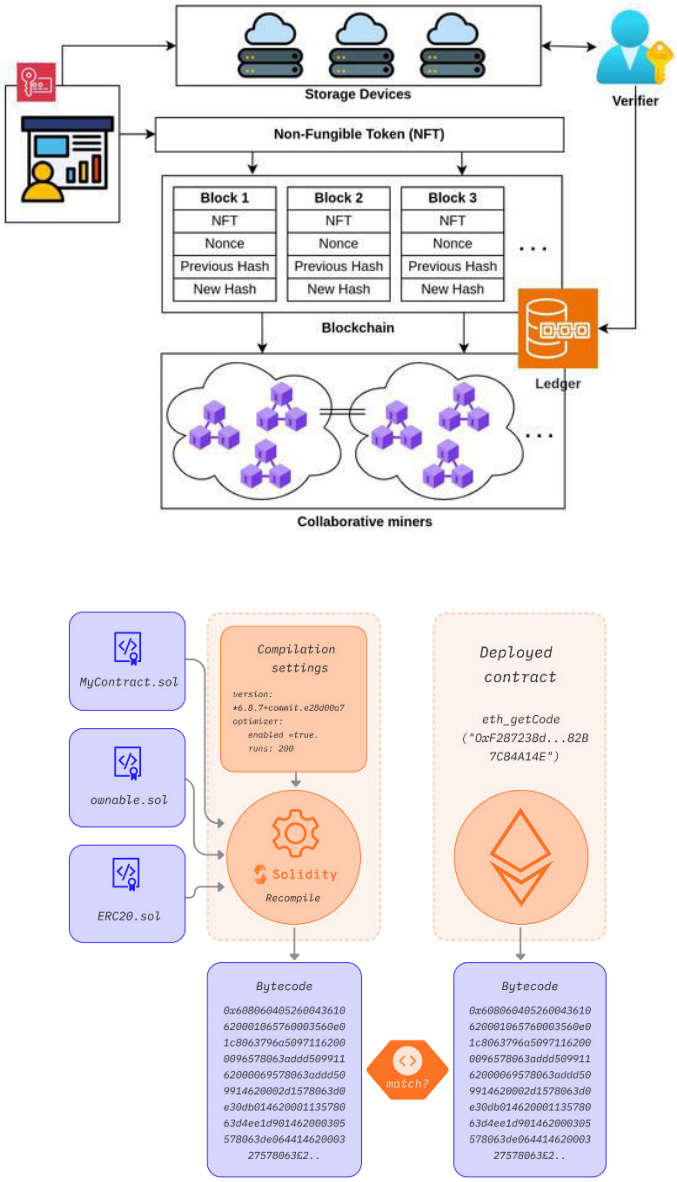


Fig.3. Output of Evidence Upload and Verification

The results of the Blockchain-Based Crime Evidence System demonstrate its effectiveness in ensuring secure and tamper-proof evidence management. The system successfully allows authorized users to upload digital evidence and generate unique hash values. These hash values

are stored on the blockchain, ensuring that the integrity of the evidence is maintained throughout its lifecycle.

The comparison between the original evidence and the stored hash confirms that any modification to the data can be easily detected. When the evidence is verified, the system recalculates the hash and compares it with the blockchain record. If both values match, the evidence is considered authentic and untampered. This verification process ensures reliability and strengthens the credibility of the evidence in legal proceedings.

The system also provides a transparent record of all activities related to the evidence. Every transaction, including uploads, access requests, and verification actions, is recorded on the blockchain with timestamps. This creates a complete and traceable chain of custody, eliminating the possibility of unauthorized modifications. The transparency of the system builds trust among stakeholders such as law enforcement agencies and judicial authorities.

Another important result is the improved security of the system compared to traditional centralized approaches. Since the blockchain is decentralized, there is no single point of failure, reducing the risk of data breaches or loss. The use of smart contracts ensures that access control policies are strictly enforced, preventing unauthorized users from accessing sensitive data.

Overall, the results confirm that the proposed system is efficient, secure, and reliable. It enhances the integrity, transparency, and accountability of crime evidence management, making it a suitable solution for modern digital forensic applications.

VI. CONCLUSION

The Blockchain-Based Crime Evidence System provides a secure, transparent, and reliable solution for managing digital evidence in modern forensic investigations. Traditional systems face significant challenges such as data tampering, lack of transparency, and weak chain-of-custody management. By leveraging blockchain technology, the proposed system overcomes these limitations by ensuring immutability and decentralization, which are essential for maintaining the authenticity of evidence.

The integration of cryptographic hashing techniques ensures that every piece of evidence has a unique digital identity, making any unauthorized modification easily detectable. The use of smart contracts automates critical processes such as evidence submission, verification, and access control, reducing human intervention and minimizing the chances of errors or manipulation. This enhances both efficiency and reliability in evidence handling.

The system also improves transparency by maintaining a complete and traceable record of all activities related to the evidence. Every action, including uploads and access requests, is recorded on the blockchain with timestamps, ensuring a strong and verifiable chain of custody. This feature is particularly important in legal proceedings, where the credibility of evidence plays a crucial role.

Furthermore, the decentralized nature of blockchain eliminates the risks associated with centralized systems, such as single points of failure and data breaches. The system is scalable and can be integrated with cloud storage and other advanced technologies to handle large volumes of data. It can be effectively used in law enforcement agencies, judicial systems, and digital forensic applications.

In conclusion, the proposed system offers a modern and robust approach to crime evidence management. It enhances security, transparency, and efficiency while ensuring the integrity and

authenticity of digital evidence. This makes it a valuable contribution to the field of cybersecurity and digital forensics.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Applied Innovation Review*, no. 2, pp. 6–19, 2016.

[3] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[4] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *NIST Special Publication*, 2018.

[5] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and solutions," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1916–1928, 2019.

[6] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[7] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," 2014.

[8] V. Buterin, "A next-generation smart contract and decentralized application platform," 2014.

[9] H. Tian, J. He, and Y. Ding, "Medical data management on blockchain," *Journal of Healthcare Engineering*, 2019.

[10] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.

[11] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT," *Future Generation Computer Systems*, vol. 88, pp. 173–190, 2018.

[12] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 983–994, 2017.

[13] S. Underwood, "Blockchain beyond bitcoin," *Communications of the ACM*, vol. 59, no. 11, pp. 15–17, 2016.

[14] M. Swan, *Blockchain: Blueprint for a New Economy*. O'Reilly Media, 2015.

[15] X. Xu et al., "A taxonomy of blockchain-based systems," *IEEE International Conference on Software Architecture*, 2017.

[16] J. Benet, "IPFS - Content addressed, versioned, P2P file system," 2014.

[17] E. Androulaki et al., "Hyperledger Fabric: A distributed operating system for permissioned blockchains," *EuroSys*, 2018.

[18] R. Kshetri, "Blockchain's roles in strengthening cybersecurity," *IT Professional*, vol. 19, no. 4, pp. 68–72, 2017.

[19] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for IoT," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[20] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access," *IEEE Open & Big Data Conference*, 2016.

[21] M. Alharby and A. van Moorsel, "Blockchain-based smart contracts: A systematic mapping study," *Computer Science Review*, vol. 36, 2020.

[22] S. Rouhani and R. Deters, "Security, performance, and applications of smart contracts," *IEEE Conference on Blockchain*, 2019.

[23] Q. Lin, H. Wang, X. Pei, and J. Wang, "Food safety traceability system using blockchain," *IEEE Access*, vol. 7, pp. 20698–20707, 2019.

[24] J. Xie, H. Tang, T. Huang, F. Yu, R. Xie, and J. Liu, "A survey of blockchain technology applied to smart cities," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2794–2830, 2019.

[25] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020.

[26] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain," *International Journal of Production Research*, vol. 57, no. 7, pp. 2117–2135, 2019.

[27] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain," *IEEE International Conference on Smart City*, 2016.

[28] H. Halpin and M. Piekarska, "Introduction to security and privacy on the blockchain," *IEEE European Symposium on Security and Privacy*, 2017.

[29] S. Gupta, M. Jain, and P. Mishra, "Blockchain-based secure data sharing," *International Journal of Computer Applications*, vol. 182, no. 12, pp. 1–5, 2018.

[30] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Computing Surveys*, vol. 52, no. 3, pp. 1–34, 2019.