International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

CRIMINAL EVIDENCES MANAGEMENT SYSTEM USING BLOCK CHAIN

[1]MALLIPUDI DEEPIKA SAI PRASANNA, [2]Y SRINIVAS RAJU

[1]Students, Department of MCA, B V Raju College, Bhimavaram Ap

[2]Assistant Professor**,** Department of MCA, B V Raju College, Bhimavaram Ap

ABSTRACT

In traditional crime evidence management systems, all data is stored in a centralized database, making it vulnerable to tampering, unauthorized access, and manipulation by administrators. Such vulnerabilities can compromise the integrity of criminal investigations, allowing culprits to escape justice by altering or deleting critical evidence. To overcome these limitations, this project proposes a Blockchain-based Criminal Evidence Management System that ensures secure, decentralized, and tamper-proof storage of evidence data. Blockchain technology stores data in the form of blocks distributed across multiple nodes, ensuring transparency and immutability. Each block is associated with a unique cryptographic hash, and any modification in data leads to a mismatch in hash values, thereby detecting tampering instantly. The system utilizes smart contracts developed using Solidity on the Ethereum blockchain to manage evidence records securely. These smart contracts define functions for storing and retrieving evidence details, ensuring controlled access and data integrity. The proposed system enables law enforcement agencies to securely record, access, and verify criminal evidence without the risk of unauthorized modifications. Experimental implementation demonstrates improved data security, transparency, and reliability compared to traditional systems. This approach provides a robust solution for maintaining the authenticity of evidence and strengthening the criminal justice system.

Keywords: ***Blockchain, Criminal Evidence Management, Ethereum, Smart Contracts, Data Security, Decentralization, Tamper-Proof Storage, Cybersecurity, Digital Forensics***

I.INTRODUCTION

In traditional crime evidence management systems, all evidence data is typically stored in centralized databases controlled by a single authority. While such systems are easy to manage, they are highly vulnerable to security

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

threats such as unauthorized access, data tampering, and insider attacks. Database administrators or malicious actors may alter or delete critical evidence, compromising the integrity of criminal investigations. Since evidence plays a vital role in identifying and prosecuting criminals, any manipulation can lead to severe consequences, including wrongful judgments. Moreover, existing systems lack proper mechanisms to detect such alterations, making them unreliable for handling sensitive forensic data. These challenges highlight the urgent need for a secure, transparent, and tamper-proof system for managing criminal evidence.

Blockchain technology has emerged as a powerful solution to address these security concerns due to its decentralized and immutable nature. Unlike traditional databases, blockchain stores data across multiple nodes, ensuring that no single entity has full control over the information. Each piece of data is stored in the form of a block, which is linked to previous blocks using cryptographic hash functions. Any attempt to modify data in a block results in a change in its hash value, which is immediately detected by the network. This makes blockchain highly secure and resistant to tampering. Additionally, blockchain provides transparency, traceability, and auditability of transactions, making it suitable for applications where data integrity is critical, such as criminal evidence management.

This project proposes a Blockchain-based Criminal Evidence Management System that leverages Ethereum smart contracts to securely store and manage evidence data. The system allows authorized users such as administrators and police officers to add, access, and verify evidence records in a decentralized environment. Smart contracts ensure that all operations are executed securely and automatically without human interference. The use of blockchain not only prevents unauthorized modifications but also maintains a transparent record of all transactions, including timestamps and unique hash values. This approach enhances trust, accountability, and efficiency in the criminal justice system, providing a reliable solution for secure evidence management.

II SURVEY OF RESEARCH

[1] The research by Satoshi Nakamoto (2008) introduced Blockchain technology as a decentralized digital ledger for secure transactions. The methodology uses cryptographic hashing and distributed

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

consensus mechanisms to ensure data integrity and prevent tampering. The results demonstrated that blockchain can securely store data without relying on a central authority. However, scalability and transaction speed remain challenges. This research forms the foundation for applying blockchain in secure data management systems such as criminal evidence storage.

[2] The study by Vitalik Buterin (2014) introduced Ethereum, a blockchain platform that supports smart contracts. The methodology enables programmable contracts that automatically execute predefined functions. The results showed that smart contracts can securely manage and automate transactions. However, vulnerabilities in contract design may lead to security risks. This research supports the implementation of smart contracts for managing evidence records in a decentralized system.

[3] The research by Melanie Swan (2015) explored the applications of blockchain technology beyond cryptocurrencies. The methodology highlights blockchain's use in areas such as healthcare, governance, and digital identity. The results demonstrated improved transparency and security in data management. However, adoption challenges and technical complexity remain. This research emphasizes the potential of blockchain in secure evidence management systems.

[4] The study by Joseph Bonneau et al. (2015) analyzed the security and privacy aspects of blockchain systems. The methodology evaluates cryptographic mechanisms and consensus protocols used in blockchain networks. The results showed that blockchain provides strong security guarantees, although privacy concerns and computational overhead exist. This research supports the use of blockchain for secure and tamper-proof storage of sensitive data.

[5] The research by Arvind Narayanan et al. (2016) discussed the practical applications and limitations of blockchain technology. The methodology examines real-world use cases and identifies challenges such as scalability and energy consumption. The results highlighted that blockchain can enhance data integrity and transparency in various domains. This research supports the feasibility of implementing blockchain-based systems for evidence management.

[6] The study by Gavin Wood (2014) focused on the technical architecture of Ethereum and

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

smart contract execution. The methodology explains how decentralized applications (DApps) operate on blockchain networks. The results showed that Ethereum enables secure and programmable data management. However, gas costs and performance limitations are concerns. This research is relevant for implementing decentralized evidence management systems using blockchain technology.

III. WORKING METHODOLOGY

The proposed Blockchain-based Criminal Evidence Management System follows a structured workflow that ensures secure, transparent, and tamper-proof handling of crime evidence data. Initially, the system sets up a private Ethereum blockchain network where all transactions related to evidence storage and retrieval are recorded. Smart contracts are developed using Solidity to define the structure and operations for managing evidence data. These smart contracts include functions for adding new evidence, retrieving stored records, and verifying transaction details. Once the smart contract is developed, it is deployed on the Ethereum blockchain using tools such as Truffle or Ganache. After deployment, a unique contract address is generated, which is used by the application layer to interact with the blockchain.

In the next phase, the system integrates a Python-based web application that acts as an interface between users and the blockchain. Authorized users such as administrators and police officers log into the system using secure credentials. The administrator is responsible for adding officer details and managing access control. Officers can add new crime evidence, including details such as case information, description, and images. When evidence is submitted, it is converted into a blockchain transaction and stored as a block. Each block contains a unique hash, timestamp, and transaction details, ensuring data integrity. If any attempt is made to alter the stored data, the hash value changes, and the system detects the tampering immediately.

In the final stage, users can retrieve and verify evidence data stored on the blockchain. The system allows officers and administrators to access evidence records using unique identifiers such as evidence ID. All retrieved data is verified using blockchain hash values to ensure authenticity. The system also logs all transactions, providing a transparent audit trail for every action performed. This methodology

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

ensures that evidence data remains secure, immutable, and traceable throughout its lifecycle. By combining blockchain technology with smart contracts and a user-friendly interface, the system provides a reliable and efficient solution for managing criminal evidence.

IV RESULTS EXPLANATIONS

In the existing system all crime and evidence details were managing in single centralized server whose database can easily tamper by database administrator to alter evidence details and there is no tool exists to detect such database alteration. In any crime evidence are the only source to capture correct culprit but alteration of evidences make culprit to easily play with the law. Culprit can bribe database administrator to tamper evidence database.

To combat against such database tamper we are employing Blockchain technology to manage evidences. Blockchain has inbuilt support for decentralized (data will be saved in Blocks at multiple nodes), secured and tamper proof storage. Blockchain sore data as block/transaction and associate each block with unique hash code and this hash code will get verify for each subsequent block storage, if data alter at any node then it will result into hash code mismatch and data tamper will get detected. This verification process of Blockchain make it secured and tamper proof data storage.

Blockchain can store and retrieve data using Smart Contracts which can be designed using Solidity programming. This contract contains functions which can be called using any programming language to store or retrieve data from Blockchain. In propose work to manage crime evidence details we have designed following contract.

In above contract we have defined functions to manage evidence details and above contract need to deployed in Blockchain Ethereum using below steps

First go inside ‘hello-eth/node-modules/bin’ folder and then look and double click on ‘runBlockchain.bat’ file to get below page

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

In above screen Ethereum started with default account and private keys and now type command as 'migrate' and then press enter key to deploy contract and get below page

In above screen in white colour text can see "evidence" contract deployed and got contract address also and this address need to specify in python programming to call Blockchain contract functions to save and get data. in below screen showing python code calling contract using address

In above screen read red colour comments to know about contract calling using contract address. In above black screen we have deployed contract and running successfully and let it run till you execute code.

Modules Information

To implement this project we have designed following modules

1) Admin Login: police department admin can login to system using username and password as 'admin and admin'.
2) Add Officer Details: after login admin will use this module to add officer and police station details to Blockchain. Admin will issue login details to all officers such as Forensic expert, enforcement officers etc.
3) View Officer: using this module admin can view list of available officers posted in different police station address.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

4) View Evidence: admin can view list of evidences and crime added by different officers
5) Officer Login: any area officer can login to system using login details given by admin
6) Add New Evidences: using this module officer will record all crime and evidence details to Blockchain
7) Access Evidences: using this module officer can access crime and evidence details saved in Blockchain.

In above screen admin can view list of added criminal evidences details from Blockchain

V. CONCLUSION

The proposed Blockchain-based Criminal Evidence Management System provides a secure, transparent, and tamper-proof solution for managing sensitive crime evidence data. By leveraging blockchain technology, the system eliminates the limitations of centralized databases, ensuring that no single authority can alter or manipulate stored evidence. The use of Ethereum smart contracts enables automated, secure, and controlled access to evidence records, while cryptographic hashing ensures data integrity and immediate detection of any tampering attempts. The system enhances trust, accountability, and transparency in the criminal justice process by maintaining an immutable audit trail of all transactions. Although challenges such as scalability and implementation complexity exist, the proposed approach demonstrates significant improvements in data security and reliability. Overall, this system offers a robust and efficient solution for modern evidence management, supporting law enforcement agencies in maintaining authentic and trustworthy records.

RE.FERENCES

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

[2] V. Buterin, “A next-generation smart contract and decentralized application platform,” Ethereum White Paper, 2014.

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

[4] J. Bonneau, A. Miller, J. Clark, et al., "SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies," in *Proc. IEEE Security and Privacy*, 2015.

[5] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies*, Princeton University Press, 2016.

[6] G. Wood, "Ethereum: A secure decentralized generalized transaction ledger," Ethereum Yellow Paper, 2014.

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

[8] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE BigData Congress*, 2017.

[9] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond Bitcoin," *Applied Innovation Review*, 2016.

[10] D. Tapscott and A. Tapscott, *Blockchain Revolution*, Penguin, 2016.

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

[12] NIST, "Blockchain technology overview," NISTIR 8202, 2018.

[13] IEEE, "Standards for blockchain and distributed ledger technologies," 2020.

[14] M. Pilkington, "Blockchain technology: Principles and applications," in *Research Handbook on Digital Transformations*, 2016.

[15] F. Tian, "An agri-food supply chain traceability system for China based on blockchain technology," in *Proc. IEEE Service Systems and Service Management*, 2016.

[16] K. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications Policy*, 2017.

[17] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and solutions," 2016.