ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Impact Factor: 8.206

Volume 8, Issue 4, April 2025

© 2025 IJMRSET | Volume 8, Issue 4, April 2025| DOI:10.15680/IJMRSET.2025.0804286

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

An Implementation of Blockchain Technology in Forensic Evidence Management

D. Sathwik[1], K. Sathish Kumar[2], A. Sathvika[3], P. Sejal[4], R. Shailaj[5], Gifta Jerith[6]

Student, Department of Artificial Intelligence and Machine Learning, Malla Reddy University, Hyderabad, India[12345]

Dean, Department of Artificial Intelligence and Machine Learning, Malla Reddy University, Hyderabad, India[6]

ABSTRACT: Evidence management is crucial in the field of forensic science. Evidences obtained from a crime scene are important in solving the case and delivering justice to the parties involved. Hence, protecting these evidences from any form of alteration is of utmost important. Chain of Custody is the process which maintains the integrity of evidence. Inability to maintain the chain of custody will make the evidence inadmissible in court, eventually leading to the case dismissal. Digitalization of forensic evidence management system is a need of time as it is an environment friendly model. Blockchains are digitally distributed ledgers of transactions signed cryptographically in chronological order that are sorted into blocks and is completely open to anyone in the blockchain network. Hyperledger Fabric is a consortium blockchain framework created by the Linux foundation and is mainly used for enterprise use. Based on the concept of Hyperledger Fabric, present study aimed to create a framework and further propose an algorithm to implement Blockchain Technology to digitalize forensic evidence management system and maintain Chain of Custody.

KEYWORDS: Blockchain technology, Forensic Evidence, Chain of custody (CoC), Cryptography, Smart contracts, Proof of Work (PoW), Proof of Stake (PoS), Consortium Blockchain, Hyperledger Fabric.

I. INTRODUCTION

The management and documentation of evidence are key concerns in forensic investigations. From collection to the final court judgment, preserving the integrity of the evidence is crucial. Chain of Custody (CoC) refers to the documentation of evidence handling throughout the investigation, recorded in chronological order. Maintaining the CoC is essential for evidence to be accepted in court. There are specific criteria that must be followed during the CoC process, including:

- Preventing corruption or alteration of evidence.
- Ensuring traceability of evidence from collection to court submission.
- Establishing a clear link between the evidence and the crime it pertains to.
- Ensuring that each individual who handles the evidence can verify the process.
- Restricting access to the evidence to authorized personnel only, to avoid tampering or manipulation.

Digitalizing the forensic evidence management system offers numerous advantages, including space-saving, environmental benefits, and cost- efficiency. Blockchain technology can help preserve the authenticity and legitimacy of CoC, making evidence admissible in court. Blockchain allows for secure storage of various system details within a single network, making it both accessible and tamper-proof. Reviewing physical documents can be time-consuming, but utilizing blockchain technology can minimize this effort.

Chain of Custody (CoC)

Evidence plays a pivotal role in criminal investigations, helping determine the guilt or innocence of the accused. Without evidence, it's challenging to direct a case effectively. Proper handling and careful packaging are critical for maintaining the integrity of the evidence. Chain of Custody is the documentation process that tracks evidence from its discovery at the crime scene to its presentation in court. It is the responsibility of the investigating officer to ensure that only authorized individuals handle the evidence and that all required documentation is completed according to standard procedures. The evidence must be collected, packed, preserved, and stored with an evidence log to prevent damage or tampering.

Established protocols and procedures must be followed during evidence collection to maintain its legitimacy. While these protocols may vary by country, the general principles remain the same. Evidence sent to forensic science

laboratories for analysis must be labeled and sealed to ensure its integrity upon arrival, free from alteration or tampering.

The Chain of Custody document should include the following information:

1. **Date and Time of Collection**: The precise moment the evidence is found at the crime scene.
2. **Evidence Description**: A detailed description, including size, shape, and condition.
3. **Identification**: A unique identifier for each piece of evidence to ensure it can be traced throughout the investigation.
4. **Personnel Handling the Evidence**: Names and signatures of everyone who handles the evidence, with corresponding dates and times.
5. **Storage Locations**: Details on where the evidence is stored at each stage, ensuring traceability to its last known location.
6. **Transfer Records**: Documentation of any transfers between custodians, ensuring evidence is always accounted for and handled properly.

Implementing **blockchain technology** in CoC management can greatly improve security, transparency, and traceability of evidence. Blockchain offers a decentralized and immutable ledger, which is ideal for preserving the integrity of forensic evidence.

Advantages of Blockchain for Chain of Custody:

- **Immutability**: Once recorded, CoC information cannot be changed or deleted, ensuring authenticity.
- **Transparency**: All actions related to the evidence are visible to authorized users, making it easy to detect unauthorized access.
- **Decentralization**: Multiple copies of evidence documentation are stored across different nodes, reducing the risk of tampering by any single individual or group.
- **Efficiency**: Blockchain allows for real-time tracking of evidence, speeding up the process and reducing delays tied to traditional documentation.

By transitioning to a blockchain-based system for evidence tracking, forensic investigators can streamline the process, reduce human error, and ensure that evidence is easily accessible and verifiable—both within the investigation and in the courtroom.

In summary, maintaining the integrity of evidence throughout an investigation is crucial for ensuring a fair legal process. Blockchain technology can significantly enhance the security and transparency of Chain of Custody documentation, making the entire process more efficient and supporting the admissibility of evidence in court, ultimately aiding the pursuit of justice.

II. LITERATURE SURVEY

1. **Smith, J., et al. (2018). "Blockchain in the Forensic Sciences: A Comprehensive Review"**
   The study by Smith, J., et al. (2018), titled "Blockchain in the Forensic Sciences: A Comprehensive Review," aimed to provide an in-depth evaluation of how blockchain technology could be applied within forensic science. The goal was to explore how blockchain could address challenges in managing and maintaining the integrity of forensic evidence and its potential to enhance the efficiency and credibility of forensic processes.
2. **Brown, A., et al. (2019). "Enhancing Forensic Evidence Management with Blockchain: A Case Study"** The paper by Brown, A., et al. (2019), titled "Enhancing Forensic Evidence Management with Blockchain: A Case Study," discusses the importance of forensic evidence in the criminal justice system, particularly its role in solving crimes and ensuring justice. It also addresses the limitations of traditional evidence management systems, which are prone to issues like tampering, human error, and cyber threats. In response to these challenges, the paper explores the potential of blockchain technology to revolutionize the management of forensic evidence.
3. **Gupta, S., et al. (2020). "Challenges and Considerations for Blockchain in Forensic Evidence Management"**
   The objective of the study by Gupta, S., et al. (2020) was to investigate the challenges and considerations involved in implementing blockchain technology for managing forensic evidence. The research sought to provide a detailed understanding of both the benefits and the obstacles associated with integrating blockchain into forensic evidence management systems.

© 2025 IJMRSET | Volume 8, Issue 4, April 2025| DOI:10.15680/IJMRSET.2025.0804286

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

III. PROPOSED METHEDOLOGY

In the proposed system, the author suggests using **Blockchain technology** to store crime forensic data due to its inherent ability to create tamper- proof records. Forensic evidence plays a crucial role in accurately identifying the perpetrator of a crime, and it is essential that this data remains secure and unaltered.

Currently, evidence data is managed either manually or recorded in centralized servers. Manual recording is a time-consuming process and susceptible to human error, making it vulnerable to alterations. On the other hand, centralized server systems can be hacked by attackers, allowing for the potential modification of critical evidence. Blockchain technology, with its decentralized and immutable nature, offers a solution to these vulnerabilities by ensuring the integrity of forensic data and making tampering nearly impossible. This approach enhances the security, transparency, and accountability of the forensic evidence management system.

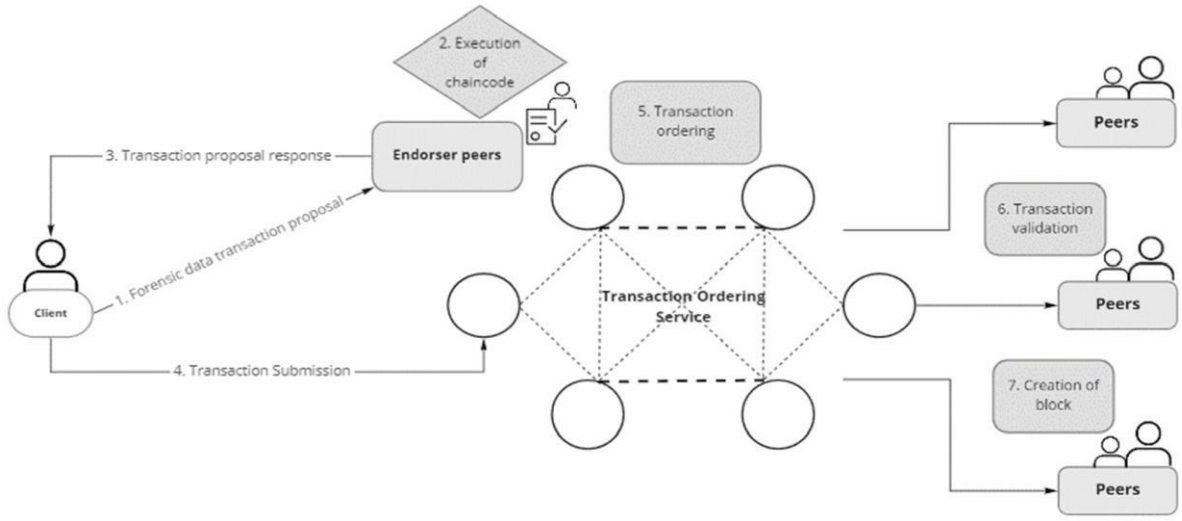

Fig. 1 HFCC framework for Chain of Custody (CoC)

IV. FRAMEWORK OF HYPERLEDGER FABRIC FOR CHAIN OF CUSTODY (HFCC)

The **Hyperledger Fabric Chain of Custody (HFCC)** framework uses blockchain technology to track and document the movement of evidence, ensuring that transactions are immutable, traceable, and valid. The framework, as illustrated in Figure 1, enables the creation of exact copies of the ledger across nodes in the network to document the transfer of evidence between personnel. Only authorized individuals can access these transactions, ensuring data security. Cryptography guarantees the integrity of evidence by preventing tampering and ensuring traceability.

The process based on **Hyperledger Fabric**
proceeds as follows:

Transaction Request:

The process begins when a client, such as the **Evidence Collection Unit (ECU)**, sends a request to initiate a transaction.

1. **Transaction Proposal Creation**: A transaction proposal is generated by the **Software Development Kit (SDK)** application. This proposal is then sent to the endorsing peers' nodes, such as the Director or Head of the team. The application formats the proposal and creates a unique signature using the encrypted credentials of the client.

2. **Proposal Verification**:
   The endorsing peers verify the
   transaction proposal to ensure it meets specific criteria:
   - The proposal is properly formatted.
   - The signature is valid.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- The proposal has not been submitted previously.
- The client is authorized to perform the proposed operation on the channel.

3. **Invocation of Chaincode**: The endorsing peers take the transaction proposal inputs and invoke the **chaincode** (or smart contract) against the database. This process generates a transaction response.

4. **Proposal Response**: The response from the endorsing peers includes their signatures, which are then verified and compared by the SDK application. The application checks whether all endorsement policies have been satisfied before submitting the proposal.

5. **Broadcasting the Transaction**:
   The validated transaction is broadcasted to the **ordering nodes**, which may include entities like the court of law, forensic department, or police stations. The transaction message includes:
   - The write/read sets.
   - The signature of the endorsing peers.
   - The channel ID.

The ordering service's role is to arrange the transactions chronologically according to their channels in the network and create the appropriate blocks.

6. **Block Validation**:
   The newly created blocks are sent to all peers within the channel. These blocks are validated to ensure the endorsement policy is satisfied. Based on this validation, the blocks are marked as **valid** or **invalid**.

Appending the Block:
The validated block is appended to the channel's chain by each peer, and the block is added to the database. A confirmation message is then sent to the client, indicating that the transaction has been permanently added and confirming the transaction's validity.

REFERENCES

[1] Bonomi, S., Casini, M., & Ciccotelli, C. (2018). "B-CoC: A 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). "Digital Forensics using Blockchain." *International Journal of Recent Technology and Engineering*, 8(2S11), 182–184. https://doi.org/10.35940/ijrte.b1030.0982s1119
[3] Bou Abdo, J., El Sibai, R., & Demerjian, J. (2020). "Permissionless Proof-of-Reputation-X: A Hybrid Reputation-based Consensus Algorithm for Permissionless Blockchains." *Transactions on Emerging Telecommunications Technologies*, 32(1), 1. https://doi.org/10.1002/ett.4148
[4] Varshney, T., Sharma, N., Kaushik, I., Bhushan, B. (2019). "Authentication & Encryption Based Security Services in Blockchain Technology." *International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, India, 63-68. doi: 10.1109/ICCCIS48478.2019.8974500
[5] Kahate, A. (2003). *Cryptography and Network Security*. McGraw-Hill Education.
[6] Dominique Guegan. (2017). "Public Blockchain versus Private Blockchain." *halshs- 01524440*.
[7] Blockchain Technology Overview. (2018, October). https://doi.org/10.6028/NIST.IR.8202

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com