Forensic Evidence Protection in the Digital Era: The Blockchain Advantage

[1]Y Vaishnavi, [2]Dr.M.Dhanalakshmi
[1]*MCA Student, Department of Information Technology, Jawaharlal Nehru Technological University, India*
[2] *Professor of IT, Department of Information Technology, Jawaharlal Nehru Technological University, India*

Abstract: In the discipline of forensic science, evidence management is essential. Evidence acquired from a crime scene is critical in solving the case and bringing the persons involved to justice. As a result, securing from any sort of altering is important. The procedure of maintaining the integrity of evidence is known as chain of custody. The inability to maintain the chain of custody may make the evidence inadmissible in court, resulting in the case being dismissed. The digitalization of forensic evidence management systems is an urgent need since it is an environmentally friendly concept. 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, our 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.

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

1. INTRODUCTION

In the field of forensic science, the careful handling of evidence is crucial for maintaining the integrity of investigations and the credibility of the judicial process. From the start of a criminal investigation to its conclusion in court, preserving the integrity of evidence is of utmost importance. The journey of evidence, from its collection to its presentation in court, requires strict adherence to protocols to prevent contamination, tampering, or loss.

Central to this process is the Chain of Custody (CoC), which meticulously documents the handling of evidence throughout the investigation. As highlighted by Jayaraman and Natarajan (2015), the CoC acts as a chronological record of the custody, control, transfer, and analysis of evidence, ensuring its reliability and admissibility in court. The CoC not only promotes transparency but also protects against challenges to the evidence's credibility, thereby upholding the justice system's integrity.

Within the CoC framework, several key criteria dictate the procedures for managing evidence. First, preventing the corruption or alteration of evidence is fundamental to maintaining its integrity. Every stage of the evidence's journey, from collection to court submission, must be meticulously documented to prevent any suspicion of tampering. Second, the evidence must be directly related to the crime under investigation, serving as proof of the alleged offense. Additionally, transparency is essential, as every entity handling the evidence must be able to verify the integrity of the custodial process, instilling confidence in the evidence's reliability in court.

In today's forensic science landscape, modernizing evidence management systems is increasingly necessary. Digitalization offers a transformative shift, addressing space constraints, environmental sustainability, and cost efficiency. It streamlines documentation and ensures the accessibility and retrievability of evidence records, enhancing operational efficiency and speeding up judicial proceedings.

Amid discussions on digital transformation, blockchain technology stands out as a revolutionary force in forensic evidence management. Blockchain's decentralized and immutable ledger system provides

unmatched security and transparency for documenting the chain of custody. By using blockchain technology, forensic agencies can strengthen the authenticity and legitimacy of CoC records, improving the admissibility of evidence in legal proceedings.

In summary, evidence management is critical in forensic science, significantly impacting justice and individual liberties. As forensic investigations navigate technological advancements and procedural integrity, maintaining evidential integrity remains crucial. By integrating robust custodial protocols with innovative digital solutions, forensic science can effectively handle contemporary legal complexities, ensuring the pursuit of truth and justice.

2. LITERATURE SURVEY

Forensic science, operating at the crossroads of law and technology, is essential in solving intricate criminal cases and ensuring justice is delivered. With continuous technological advancements reshaping forensic investigations, effective evidence management has become a crucial aspect, requiring a deep understanding of custodial protocols and innovative solutions to maintain evidential integrity. This literature review examines key studies addressing the complexities of evidence management in the digital era, focusing on how blockchain technology and forensic science converge to enhance the reliability and admissibility of evidence.

Bonhomie, Cassini, and Ciccotelli (2018) conducted a groundbreaking study titled "CoC: A Blockchain-based Chain of Custody for Evidence Management in Digital Forensics" [1]. They propose a blockchain-based solution to improve the chain of custody (CoC) process, utilizing blockchain's immutable characteristics to ensure the integrity and traceability of evidence records. This decentralized ledger system provides exceptional transparency and security, reducing the risk of tampering or manipulation during the investigation.

Adding to this conversation, Gopalan et al. (2019) explore "Digital Forensics using Blockchain" [2]. Their study highlights the transformative potential of blockchain technology in enhancing the reliability and credibility of digital forensic investigations. By leveraging blockchain's cryptographic security and decentralized structure, forensic experts can authenticate digital evidence with greater confidence, thus improving the effectiveness of criminal investigations.

Varshney, Sharma, Kaushik, and Bhushan (2019) further this field with their research on "Authentication & Encryption Based Security Services in Blockchain Technology" [4]. They discuss how authentication and encryption methods enhance the security of blockchain networks. Strong cryptographic protocols protect sensitive evidence data from unauthorized access or alteration, reinforcing the CoC process's integrity.

A solid grasp of cryptography is crucial for understanding blockchain technology. Kahate (2003) provides an extensive discussion in "Cryptography and Network Security" [5], covering encryption, digital signatures, and cryptographic hash functions. This work is essential for forensic experts aiming to master blockchain-based evidence management.

Dominique Guegan (2017) offers insights into "Public Blockchain versus Private Blockchain" [6], explaining the unique characteristics of each type and their relevance to forensic investigations. Public blockchains provide unmatched transparency and decentralization, while private blockchains offer greater control and privacy, addressing various forensic needs.

To fully leverage blockchain technology, forensic experts need a thorough understanding of its principles. The National Institute of Standards and Technology (NIST) provides a detailed overview in "Blockchain Technology" [7], discussing its fundamental concepts, architecture, and potential applications in forensic science. This foundational resource is crucial for practitioners integrating blockchain into evidence management.

Castor (2017) presents "Blockchain Consensus Protocols" [8], detailing the different consensus mechanisms that support blockchain networks. By explaining the strengths and weaknesses of protocols like proof of work and proof of stake, Castor helps forensic experts choose the best blockchain framework for managing evidence.

Goodell and Aste (2019) envision "A Decentralized Digital Identity Architecture" [11], investigating how blockchain could transform identity management in forensic investigations. Decentralizing digital identities and using cryptographic methods can reduce identity fraud risk and improve the verifiability of

evidence records, thereby enhancing the CoC process's integrity.

In summary, integrating blockchain technology with forensic science marks a significant shift in evidence management, offering unmatched transparency, security, and reliability. Combining cryptographic principles, decentralized systems, and robust custodial protocols allows forensic experts to handle modern investigations with increased confidence and efficiency. As forensic science evolves, collaboration among law enforcement, academia, and industry will be crucial in fully realizing the potential of blockchain-enabled evidence management.

3. METHODOLOGY

a) Proposed Work:

Our proposed system aims to transform forensic evidence management by utilizing blockchain technology [3], addressing current system deficiencies and improving integrity, security, and efficiency.

By leveraging blockchain's immutable ledger, every interaction with evidence is recorded as an unalterable transaction, ensuring transparency and accountability throughout the chain of custody.

Evidence data is securely stored on a decentralized network of nodes, eliminating single points of failure and minimizing the risk of data loss or tampering.

Cryptographic techniques [6] are used to protect the confidentiality and privacy of sensitive evidence data, while still allowing authorized parties to verify the authenticity of evidence records.

The system provides real-time monitoring and alerts for any suspicious activities or attempts to tamper with evidence. Unauthorized changes to evidence records trigger immediate notifications, enabling prompt intervention to maintain evidence integrity [1,2].

By implementing a blockchain-based forensic evidence management system, forensic agencies can significantly enhance the reliability, transparency, and security of their evidence management processes. This leads to more accurate and timely forensic investigations, thereby increasing public trust in the criminal justice system.

b) System Architecture:

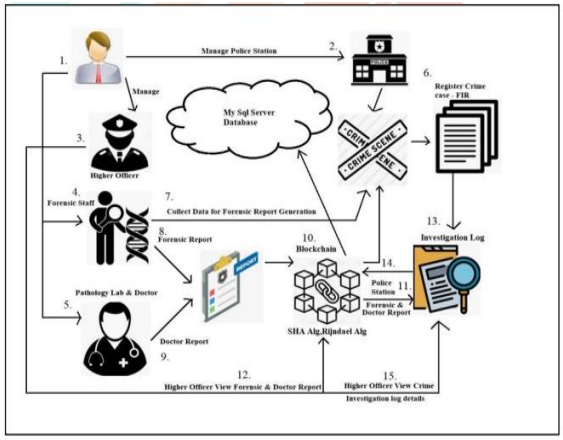


Fig1 Proposed Architecture

The system architecture consists of two main components: the Admin interface and the Blockchain.

Admin Interface:

The Admin interface facilitates system interaction, providing functionalities like fetching and adding evidence [1,2] to the blockchain. In the "Check and validate evidence" module, the Admin accesses the blockchain to retrieve detailed information about each piece of evidence stored within the system. This information is presented to the Admin for review and analysis.

In the "Add evidences" module, the Admin uploads new evidence details into the blockchain by inputting relevant information such as its description, chain of custody data, and associated metadata. The Blockchain [3] securely stores this information in a decentralized and immutable ledger, ensuring its integrity and verifiability over time.

Overall, the system architecture seamlessly integrates the Admin interface with the Blockchain, facilitating efficient management and retrieval of evidential data while leveraging the inherent security and transparency of blockchain technology.

c) Lab Login:

The Lab Login module serves as a secure gateway for authorized users, such as administrators or law enforcement personnel, to access the system. Users input their credentials, including a username and password, to authenticate their identity. Upon successful verification, users are granted access to the system's functionalities, enabling them to manage forensic evidence data efficiently and securely.

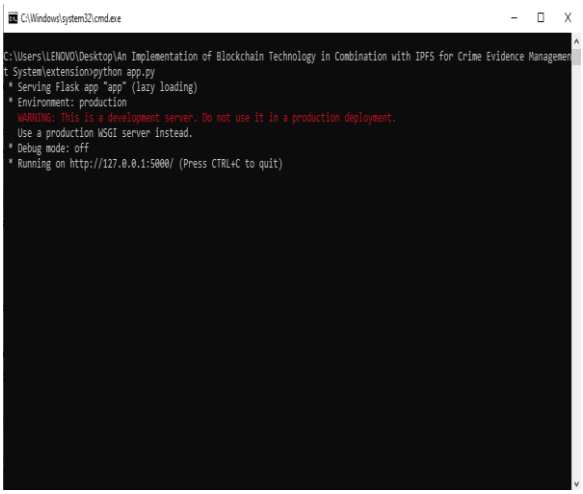
d) Add Evidences to Blockchain:
In the "Add Evidence" module, authorized users can input new forensic evidence data into the blockchain-based system. Users provide relevant details, including evidence descriptions, case particulars, location, and metadata, through forms or input fields. The system validates and processes this data for accuracy before securely recording it onto the blockchain. Leveraging blockchain's tamper-proof nature ensures the immutability and integrity of the stored evidence, maintaining its reliability for forensic investigations.

e) Fetch Evidences from Blockchain:
In the "Check and validate evidence" module, authorized users can retrieve forensic evidence data stored within the blockchain. This streamlined process enables users to access and view accurate, unaltered evidence data effortlessly. By providing authorized individuals with easy access to evidence data, this module facilitates efficient legal proceedings and analysis, ensuring transparency and reliability in forensic investigations.

f) Blockchain Integration:
Blockchain technology is utilized to securely store forensic evidence data. When new evidence is collected, it undergoes encryption before being stored on the blockchain, ensuring the confidentiality and integrity of sensitive crime data. User details related to evidence management are stored on the blockchain, protecting them from unauthorized alterations.
Smart contracts written in Solidity streamline the storage of forensic evidence processes, including decryption and retrieval. Data integrity is maintained in the system through the use of the SHA-256 algorithm (Secure Hash Algorithm 256-bit). Each block in a blockchain is linked with a unique hash code. These blocks are maintained across multiple nodes or servers. Before storing new records, the blockchain verifies the hash code of each block. If any block data is modified, it results in a different hash code, triggering security alarms and ensuring the data's integrity and immutability.

4. EXPERIMENTAL RESULTS

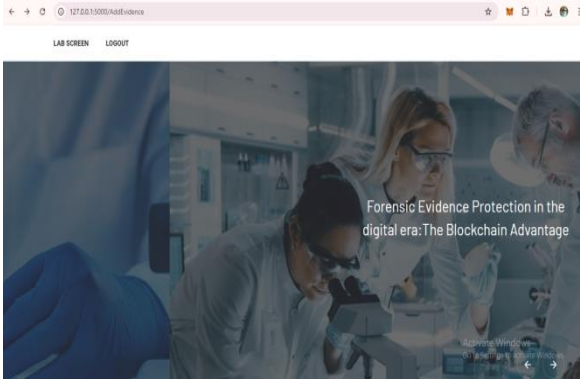
Now Blockchain setup and now double click on 'run.bat' file to start DJANGO python server and to get below screen



In above screen python DJANGO server started and now open browser and enter URL as http://127.0.0.1:5000/ and then press enter key to get below application home screen

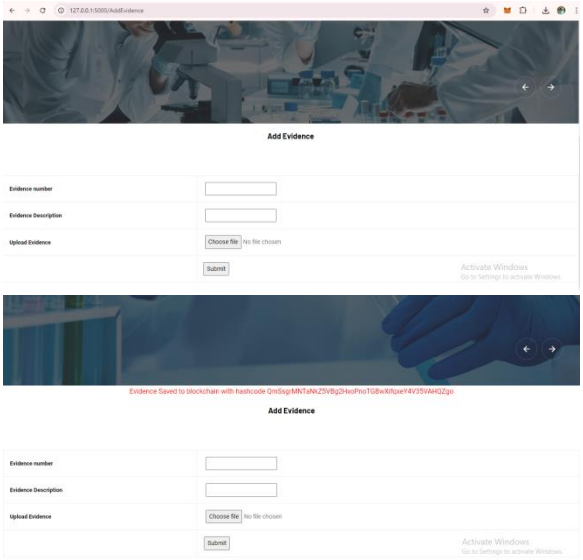
In above screen click on 'Login' link to get below login screen

In above screen enter username as 'Lab' and password as '1234' and then press 'Login' button to get below screen



In above screen now admin can click on 'Lab Screen' the 'Add Evidence' link to get below screen and to record evidences

In above screen police or lab or hospital personnel may record all crime and evidences details and then click on 'Submit' button to get below screen



In above screen in red colour text we can see data saved in Blockchain and now click on 'Fetch Evidences from Blockchain' link to get all details

5. CONCLUSION

The project aimed to revolutionize forensic evidence management by leveraging blockchain technology [3] rather than traditional methods. This innovation has the potential to significantly alter how critical evidence is handled in legal contexts.

Blockchain's tamper-proof characteristics were utilized to protect forensic evidence from unauthorized access or modifications, thereby enhancing the security and trustworthiness of evidence in legal proceedings.

The project sought to streamline evidence management, making the process more efficient and straightforward. This improvement aimed to minimize errors and ensure accurate tracking and preservation of evidence [1,2] throughout its lifecycle, which is vital for maintaining the integrity of evidence in judicial processes.

Law enforcement agencies stand to benefit from enhanced evidence management, which aids in investigations and ensures the reliability of the evidence.

Thus, this project exemplifies how blockchain technology can transform forensic evidence management. It showcases the technology's ability to enhance the security, efficiency, and reliability of evidence handling, ultimately fostering a more transparent and trustworthy legal system.

6. FUTURE SCOPE

In the future, combining the blockchain-based system with cutting-edge technologies such as artificial intelligence (AI), machine learning (ML), and the Internet of Things (IoT) offers significant potential. This integration can enhance the system's abilities in areas such as data analysis, evidence verification, and continuous monitoring. Additionally, creating decentralized marketplaces or platforms for trading forensic services, expertise, or assets related to evidence could open up new possibilities for forensic professionals, researchers, and organizations, promoting innovation and collaboration within the forensic science field.

7. REFERENCES

[1] Bonomi, S., Casini, M., & Ciccotelli, C. (2018). "BCoC: 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] Guegan, D. (2017). "Public Blockchain versus Private Blockchain." ⟨halshs-01524440⟩

[7] "Blockchain Technology Overview." (2018, October). https://doi.org/10.6028/NIST.IR.8202

[8] Castor, A. (2017). "A Short Guide to Blockchain Consensus Protocols." Coindesk. https://www.coindesk.com/shortguideblockchain consensus-protocols

[9] Nguyen, C.T., Hoang, D.T., Nguyen, D.N., Niyato, D., Nhuyen, H.T., & Dutkiewicz, E. (2019). "Two-level Blockchain System for Digital Crime Evidence Management." Sensors, 21(9), 3051. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8746079

[10] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., et al. (2018). "Hyperledger Fabric." Proceedings of the Thirteenth EuroSys Conference, 1–15. https://doi.org/10.1145/3190508.3190538

[11] Goodell, G., & Aste, T. (2019). "A Decentralized Digital Identity Architecture." Frontiers in Blockchain, 2, 1. https://doi.org/10.3389/fbloc.2019.00017

[12] Krstić, M., & Krstić, L. (2020). "Hyperledger Frameworks with a Special Focus on Hyperledger Fabric." Vojnotehnicki Glasnik, 68(3), 639–663. https://doi.org/10.5937/vojtehg68-26206

[13] Kate-Deshmukh, P.N., Bhilare, T., Mohite, R., Sonawane, S., Wahgmare, P., et al. "Security of Forensic Evidence Using Blockchain." IRJMETS Open Access. Available at https://www.irjmets.com/uploadedfiles/paper//issue_1_january_2024/49050/final/fin_irjmets1706771110.pdf

[14] Sharma, D., & Sakshi, et al. "Blockchain-Based Digital Forensics Investigation." IJSR Open Access. Available at https://www.ijsr.net/archive/v12i1/SR221101114528.pdf

[15] Rao, S., Fernandes, S., Raorane, S., & Syed, S., et al. "A Novel Approach for Digital Evidence Management Using Blockchain." SSRN Open Access. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3683280

[16] Chen, S., Zhao, C., Huang, L., Yuan, J., Liu, M., et al. "Study and Implementation on the Application of Blockchain in Electronic Evidence Generation." ScienceDirect Open Access. Available at https://www.sciencedirect.com/science/article/abs/pii/S2666281720300573

[17] Mehta, S., Kumari, K.S., Jain, P., Raikwar, H., Gore, S., et al. "Blockchain Driven Evidence Management System." IEEE Open Access. Available at https://ieeexplore.ieee.org/document/10134799

[18] Anderes, D., Baumel, E., Grier, C., Veun, R., & Wright, S. "The Use of Blockchain within Evidence Management Systems."

[19] Sathyaprakasan, R., Govindan, P., Alvi, S., Sadath, L., Philip, S., & Singh, N. "An Implementation of Blockchain Technology in Forensic Evidence Management."

[20] Kim, D., Ihm, S.Y., & Son, Y. "Two-level Blockchain System for Digital Crime Evidence Management." Sensors, 21(9), 3051, 2021.

[21] Rao, S., Fernandes, S., Raorane, S., & Syed, S. "A Novel Approach for Digital Evidence Management Using Blockchain." Proceedings of the International Conference on Recent Advances in Computational Techniques (IC-RACT), June 2020.

[22] Leible, S., Schlager, S., Schubotz, M., & Gipp, B. "A Review on Blockchain Technology and Blockchain Projects Fostering Open Science." Frontiers in Blockchain, 16, 2019.

[23] "Design and Implementation of an E-Policing System to Report Crimes in Nigeria."

[24] Jain, A., Bhatia, D., & Manish, K. "Extractive Text Summarization using Word Vector Embedding," 2017.

[25] Hingorani, I., Khara, R., Pomendkar, D., & Raul, N. "Police Complaint Management System Using Blockchain Technology," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), December 2020, 1214-1219.

[26] Gupta, A., & Vilchez Jose, D. "A Method to Secure FIR System Using Blockchain," International Journal of Recent Technology and

Engineering (IJRTE), 8(1), 2277-3878, May 2019.

[27] Tabassum, K., Shaiba, H., Shamrani, S., & Otaibi, S. "e-Cops: An Online Crime Reporting and Management System for Riyadh City," 2018 1st International Conference on Computer Applications Information Security (ICCAIS), Riyadh, 1-8, 2018.

[28] Iyer, A., Kathale, P., Gathoo, S., & Surpam, N. "E-Police SystemFIR Registration and Tracking through Android Application," International Research Journal of Engineering and Technology, 3(2), 1176-1179, 2016.

[29] Pillai, S., Omoregbe, P., Misra, N., Maskeliunas, S., & Damasevicius, R. "Online FIR Registration and SOS System," International Journal of Engineering and Computer Science, 5(4), December 2017.

[30] "Design and Implementation of an E-Policing System to Report Crimes in Nigeria."