BioGecko

Vol 12 Issue 03 2023

ISSN NO: 2230-5807

# An Implementation of Block chain Technology in Forensic Evidence Management

**Mrs. J. Alisha Reddy[1], T. Veera Subhashini[2], Ch. Amulya[3], P. Sruthi[4]**

*[1]Assistant Professor, Computer Science and Engineering, Sridevi Women's Engineering College, Hyderabad, India*
*[2]Computer Science and Engineering, Sridevi Women's Engineering College, B.Tech IV Year Hyderabad, India*
*[3]Computer Science and Engineering, Sridevi Women's Engineering College, B.Tech IV Year Hyderabad, India*
*[4]Computer Science and Engineering, Sridevi Women's Engineering College, B.Tech IV Year Hyderabad, India*

## Abstract

The forensic science discipline places a premium on evidence management. Crime scene evidence is crucial to solving cases and bringing those responsible to justice. Therefore, it is crucial to safeguard these items from being tampered with in any way. The integrity of proof is protected via a procedure known as "chain of custody." Failure to preserve the chain of custody renders the proof inadmissible in court and might result in the dismissal of the case. The current paradigm for managing forensic evidence is not eco-friendly, hence digitizing this process is essential. Open to anybody in the blockchain network, the blockchains are digitally distributed ledgers of transactions signed cryptographically in chronological order and grouped into blocks. Hyperledger Fabric was developed by the Foundation for Linux as a consortium blockchain architecture for business applications. This research set out to develop a framework for using Blockchain Technology to digitally transform the criminal record management system and keep the Chain of Custody in place; this work was inspired by the ideas of Hyperledger Fabric.

## 1. INTRODUCTION

Effective evidence handling is crucial to the field of forensic science. The main challenges in conducting a forensic investigation are evidence management and recording. Evidence must be protected from the point of collection until the court renders its decision. The paper trail that the investigation's evidence left behind when it was moved from one person to another is referred to as the "Chain of Custody" (CoC). You must maintain the CoC in good condition if you want your testimony to stand up in court. The following requirements must be met for the Certificate of Compliance (CoC) process to be successful: Evidence must not be tampered with or compromised in any way. A paper trail should be left behind at every stage of the inquiry, from acquiring evidence to presenting it in court. The evidence must be convincing and pertinent to the act. The veracity of the evidence must be attested to by all persons who had a hand in gathering it. No unauthorised personnel are permitted to handle the evidence in order to avoid any potential tampering or manipulation. The forensic evidence management system's digitization not only frees up physical space but also cuts waste and expenses. A CoC may be used as evidence of validity and legal standing in court of law. These might be updated and secured using blockchain technology. With the use of blockchain technology, we are able to keep all the data about a system in a single, secure area. The use of contemporary technologies may aid to shorten the time spent reviewing physical papers. To prove guilt or innocence in a criminal case, the chain of custody (CoC) evidence is essential. Without evidence, a case might be taken in the incorrect direction. Evidence needs to be handled and packed carefully to maintain its integrity. Evidence must follow a process called "Chain of Custody," which entails painstakingly documenting the evidence's travel from the scene of the crime to the courtroom.

The trustworthiness of the evidence depends on the chain of custody (CoC). One of an investigating officer's duties is to make sure that only authorised persons handle evidence and that all paperwork is completed accurately and promptly. All of the evidence has been carefully gathered, wrapped, and preserved along with the evidence record. For evidence gathering to be credible, it must follow accepted norms and standards of practise. From one country to the next, these procedures' specifics could be a little different. To avoid contamination or damage in transit, evidence that is being transferred to a forensic science lab for analysis must be properly tagged and sealed.

## 2. RELATED WORKS

**"A Blockchain-based Ring of Possession for Evidences Handling in Digital Forensics"**

Handling evidence in digital forensics poses significant challenges, particularly in ensuring its integrity and maintaining a clear chain of custody. Throughout an investigation, various parties involved may have temporary ownership of the evidence from collection to its utilization in a court of law. However, if the "Chain of Custody" (CoC) is broken at any point, tampered evidence becomes inadmissible in court. Currently, the CoC for digital evidence is manually maintained, with each entity responsible for completing supporting documentation.To address these issues and ensure the auditable integrity of gathered evidence and traceability of owners, this article proposes a decentralized approach called Blockchain-based Chain of Custody (B-CoC). By utilizing blockchain technology, we aim to streamline the CoC process. As a proof-of-concept, we have developed an Ethereum-based system for B-CoC and conducted a thorough analysis of its functionality and operation.

**Blockchain Technology for Digital Investigations. A Global Perspective on Emerging Technologies and Engineering,"**

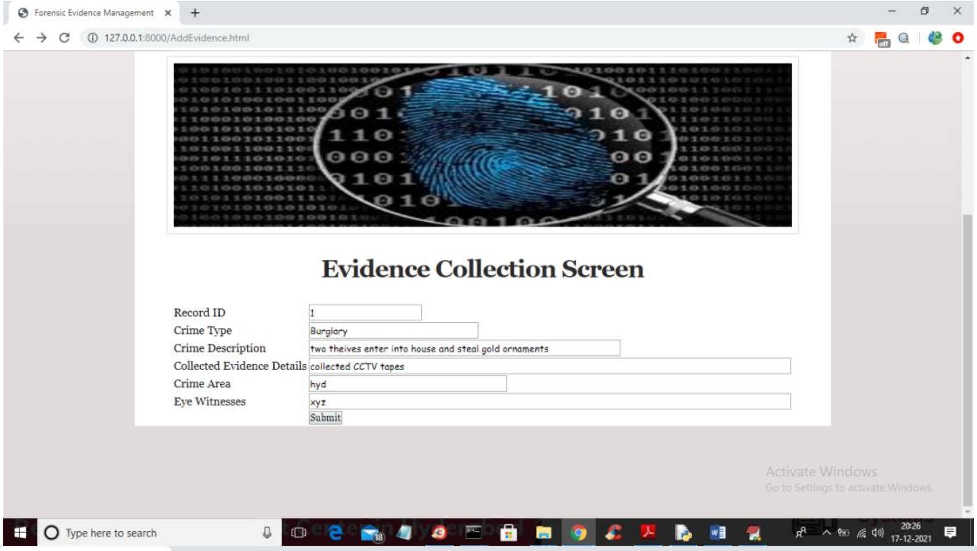
Preserving the integrity of digital evidence is crucial to protect against potential risks such as tampering or destruction. To ensure the reliability of evidence presented in court, it is necessary to implement safeguards against these threats. The concept of "Chain of Custody" refers to the systematic documentation of information. In the context of criminal investigations, detectives rely on the Chain of Custody to determine the reliability of the information they are working with. The significance of the Chain of Custody lies in the fact that it establishes the evidence was not tampered with from the time of collection until its presentation in court. Without a trustworthy Chain of Custody, the gathered evidence cannot be deemed reliable.One approach to strengthen the trustworthiness of evidence is by utilizing blockchain technology. Blockchain, currently used in cryptocurrencies like Bitcoin, involves hashing and storing data blocks on a distributed ledger. We propose employing blockchain for the Chain of Custody process, enabling better monitoring of data access and enhancing the credibility of evidence during courtroom proceedings. The terms "Chain of Custody" (CoC), "Blockchain-Based Chain of Custody" (B-CoC), and "Proof of Work" (PoW) are all acronyms associated with this concept and its implementation using blockchain technology.

## 3. METHODOLOGY

The adaptability of digital data storage is one of its main advantages. It is easily accessible to authorised staff. A file can be copied multiple times and stored without compromising the original. The entire world has easy access to it. It is possible to send many files at once. Finding the same information that is kept in paper form takes far longer than finding the same information that is saved digitally. Documents used as evidence may become damaged as a result of a natural or man-made disaster. Therefore, including blockchain technology into the Chain of Custody process may lessen the risk of harm to these documents. This technology may also help to eliminate human error.The world is getting more and more digital, so it is essential that forensic evidence management solutions capitalise on this development. Access to a permissioned blockchain, also known as a private blockchain, is restricted to a small number of network nodes. One must first obtain authorization from a governing entity in order to participate in authenticating the transactions. This blockchain implementation may be useful for the business world. These types scale well, are safe, and offer excellent performance. They can also be adjusted in various ways. The integrity and dependability of the participants guarantee the security of the system. Among the blockchains that include permissions are Ripple, Corda, and Hyperledger Fabric. The public, or permissionless, blockchain is the second type of blockchain. Using this blockchain arrangement, anyone on the network can take part in processing transactions and confirming them. All network participants have access to the ledger. There is no centralised control over the blockchain, and the nodes' anonymity is preserved. They are dependable and a secure choice. Examples of permissionless blockchains include Dash, Bitcoin, and Ethereum.

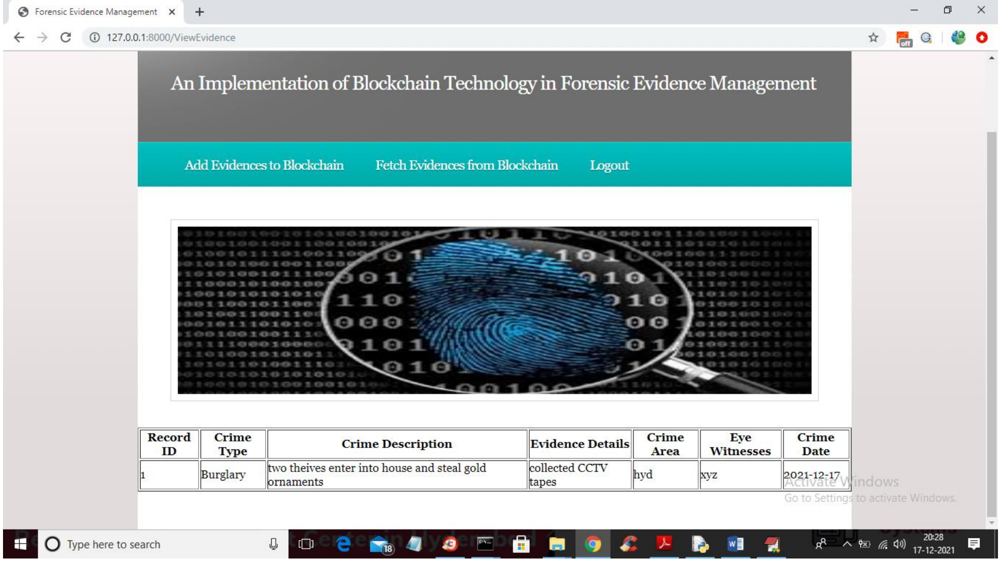
## 4. RESULT AND DISCUSSION

After filling out the information on the previous page, police officers or administrators may submit the report by clicking the "Submit" button.


Forensic Evidence Management
127.0.0.1:8000/AddEvidence.html
Activate Windows
Go to Settings to activate Windows.
Type here to search

Evidence Collection Screen

| | |
|---|---|
| Record ID | 1 |
| Crime Type | Burglary |
| Crime Description | two theives enter into house and steal gold ornaments |
| Collected Evidence Details | collected CCTV tapes |
| Crime Area | hyd |
| Eye Witnesses | xyz |
| | Submit |


Forensic Evidence Management
127.0.0.1:8000/ViewEvidence
Add Evidences to Blockchain
Fetch Evidences from Blockchain
Logout
Activate Windows
Go to Settings to activate Windows.
Type here to search

An Implementation of Blockchain Technology in Forensic Evidence Management

| Record ID | Crime Type | Crime Description | Evidence Details | Crime Area | Eye Witnesses | Crime Date |
|---|---|---|---|---|---|---|
| 1 | Burglary | two theives enter into house and steal gold ornaments | collected CCTV tapes | hyd | xyz | 2021-12-17 |

The information shown in the previous window comes directly from the Blockchain and may be used as evidence in a legal proceeding. A similar number of crimes' information may be entered by the administrator and stored in Blockchain.

## 5. CONCLUSION

Evidence must be kept secure from the moment it is obtained at the scene of a crime until a verdict is reached in a court of law. Chain of custody documentation shows whether or not evidence was tampered with throughout the gathering and examination phases. By digitising the chain of custody, Blockchain technology can guarantee the safety, veracity, and integrity of forensic data exchanges. Blockchain's use will not only improve environmental friendliness, but also security thanks to encryption that can only be viewed by approved users from afar. We want to develop a protocol, based on blockchain technology and more especially Hyperledger Fabric, that implements the chain of custody procedure. Even more importantly for forensics, we can combine blockchain with AI/ML to create a powerful tool.

## 6. REFERENCES

1. Bonomi, S., Casini, M., & Ciccotelli, C. (2018). BCoC: A Blockchain-based Chain of Custody for Evidences 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. BouAbdo, 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. Public Blockchain versus Private blockchain. 2017. ⟨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/short-guide-blockchainconsensus-protocols
9. Cong T. Nguyen, Dinh T. Hoang, Diep N. Nguyen, DusitNiyato, Huynh TuongNhuyen&ErykDutkiewicz. (2019). https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnum ber=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
10. 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. VojnotehnickiGlasnik, 68(3), 639–663. https://doi.org/10.5937/vojtehg68-26206