International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

An Implementation of Blockchain Technology in Forensic Evidence Management.

Mrs. K. Sneha
Computer Science and Engineering
(JNTUH)
Sphoorthy Engineering College
(JNTUH)
Hyderabad, India
kunasneha92@gmail.com

Eedulakanti Sowmya
Computer Science and Engineering
(JNTUH)
Sphoorthy Engineering College
(JNTUH)
Hyderabad, India
sowmyaedulakanti@gmail.com

Morla Brundavani
Computer Science and Engineering
(JNTUH)
Sphoorthy Engineering College
(JNTUH)
Hyderabad, India
brundavanimorla@gmail.com

Harshitha Reddy Bandameedi
Computer Science and Engineering
(JNTUH)
Sphoorthy Engineering College
(JNTUH)
Hyderabad, India
harshitha16reddy@gmail.com

***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 block chain network. Hyperledger Fabric is a consortium block chain 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.**

Keywords—Block chain technology, Forensic Evidence, Chain of custody (CoC), Cryptography, Smart contracts, Proof of Work (PoW), Hyper ledger Fabric.

I. INTRODUCTION

This Evidence management is critical in the field of forensic science. Main concerns in forensic investigation are the management of evidences and their documentation. Starting from the point of collection till the final judgment from the court of law, maintaining the integrity of the evidence is of utmost importance. Chain of Custody (CoC) is the documentation of the evidences handled throughout the investigation in chronological order. It is essential to maintain the CoC for the evidence to be accepted in court. There are certain criteria that need to be met during the CoC procedure, such as the following:

- The corruption and alteration of the evidence is to be avoided.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

- From the time the evidence is collected till its submission in the court, the movement of the evidence throughout the investigation should be traceable.
- The evidence should be able to relate to the crime and act as a proof.
- Each and every entity that has come in contact with the evidence must be able to verify the process.
- No unauthorized person is allowed to deal with the evidence, to avoid any sort of alteration or manipulation of the evidence.

Digitalization of forensic evidence management system saves space and at the same time makes it environment friendly and cost-efficient. Authenticity and legitimacy of COC make evidence admissible in the court of law. These can be maintained by using block chain technology.

Block chain technology enables us to store various details of a system within a single network making it secure and accessible to its users. Reviewing the documents in physical format can be time consuming which can be minimized by utilizing the technology.

Evidence is the most important aspect of any crime scene as it helps in proving guilt or innocence of the accused. Without evidence, it is very difficult to steer a case in the right direction. Proper handling and careful packaging are vital in maintaining the integrity of evidence.

Chain of Custody is the process of documentation of evidence from the time evidence is found at the crime scene till it reaches the court for trial. CoC plays an important role in maintaining the authenticity and credibility of evidence. It is an investigating officer's duty to ensure that only authorized person handle the evidence and all the documentation is completed as per standard procedure. All the evidence is collected, packed, preserved and stored along with evidence log without getting damaged. Established standard protocols and rules of procedure must be practiced during collection of evidence to maintain legitimacy. These protocols may differ slightly from country to country. All the evidence that is to be sent to the forensic science laboratory for examination must be labeled and sealed which ensures they stay intact when they reach the lab, without any contamination or damage.

II. WHY USE BLOCKCHAIN IN COC

Flexibility is one of the main advantages of saving information in a digital format. It can be easily accessed by authorized personnel. Multiple copies can be created and saved without causing any damage to the original document. It can be easily accessed from anywhere in the world. Multiple documents can be transferred instantly. It increases productivity as it takes only a few seconds to search for the information that is saved in digital format whereas it'll take a lot more time when you have to look for physical documents. Natural or man-made disaster puts evidence documentations at risk to get damaged. Thus, implementation of block chain technology in the process of Chain of Custody will mitigate the risk of damaging these documents. Using this technology will also help in irradiating human error. As the world is moving towards digitization, it is really important to implement such technologies in forensic evidence management system.

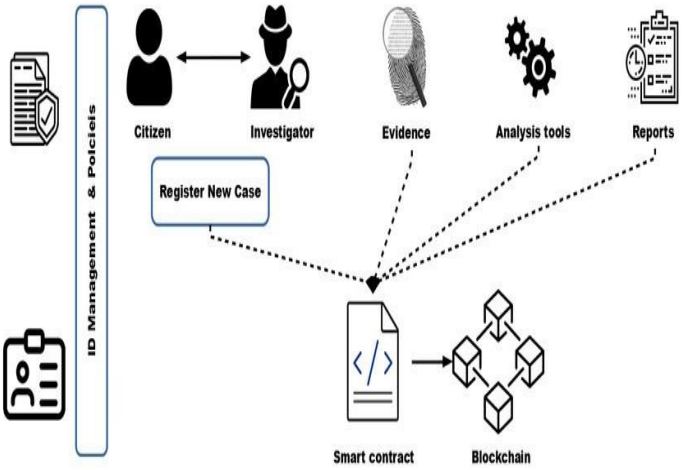

Fig.1 Forensic evidence management architecture

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

III. LITERATURE SURVEY

Digital evidence is the focus of digital forensics, a subfield of forensics. In digital forensics, material stored electronically is detected, acquired, processed, analyzed, and reported on. The integrity and security of digital forensics can be a problem. Security and integrity concerns for IoT devices put cybercrime agencies at risk while collecting digital forensic evidence. A major concern for academics working on IoT based digital forensics is that the data they collect may be compromised due to lack of adequate safeguards against unauthorized access. Digital forensics have been the subject of numerous studies utilizing Block chain technology to ensure their own integrity and security.

The system uses encryption to provide integrity and it is maintained throughout with help of cryptography and decryption with use of a private key.

It verifies authenticity and integrity of collected data in case of possible tampering.

The proposed framework will be using MFI (Multi-Factor Integrity) system which is a multiple block chains platforms at less cost. It is difficult to tamper or alter the data. All of these systems are based on smart contracts, making communication between them simple. To decrease the amount of data posted on public block chains, hash algorithms are utilized.

According to recent research and investigations, tampering and security-related problems in digital forensics are still present. In order to keep the system safe and secure, it is necessary to have a model that is both effective and clever. As a result, we're putting forward a solution that makes use of both Block chain and the hashing algorithm.

IV. IMPLEMENTATION

MODULES:

To implement this project we have designed following modules

- **Admin Login**: Using this module, police can login to the application by using the username and password.
- **Add Evidences to Block chain**: Using this module, police can add evidence to the Block chain Ethereum tool.
- **Fetch Evidences from Block chain**: Using this module, police can extract the evidence stored in the Block chain. Authorized user can only extract evidences from Block chain.

BLOCKCHAIN HASH FUNCTION:

A hash function takes an input string (numbers, alphabets, media files) of any length and transforms it into a fixed length. The fixed bit length can vary (like 32-bit or 64-bit or 128-bit or 256-bit) depending on the hash function which is being used. The fixed-length output is called a hash. This hash is also the cryptographic by-product of a hash algorithm. The hash algorithm has certain unique properties: It produces a unique output (or hash). It is a one-way function. In the context of cryptocurrencies like Bitcoin, the blockchain uses this cryptographic hash function's properties in its consensus mechanism. A cryptographic hash is a digest or digital fingerprints of a certain amount of data. In cryptographic hash functions, the transactions are taken as an input and run through a hashing algorithm which gives an output of a fixed size. Since the Hash function is a one-way function, there is no way to get back entire text from the generated hash. This is different from traditional cryptographic functions like encryption where you can encrypt something using the key and by using decryption, you can decrypt the message to its original form.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

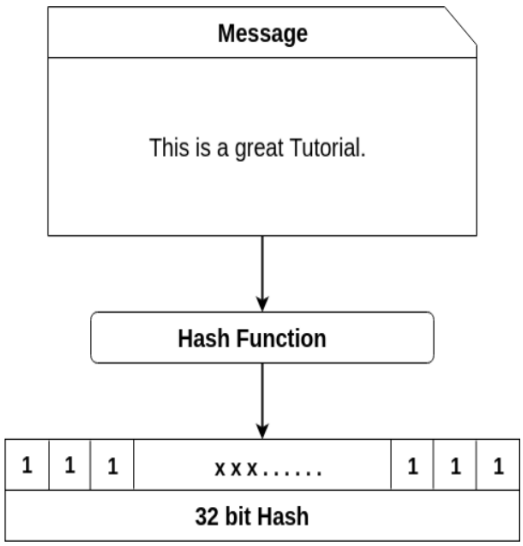

Fig. 2 This figure shows how a hash address is generated.

During a crime investigation, the evidences collected by police are to be secured without any tampering. So, by this application, police secure the evidences by digitalizing them by implementing block chain technology. At first a private blockchain need to be set up, and start the Django python server. Open the browser and enter the URL and you get navigated to the application home screen. Only authorized person can login to the application by clicking the administrator button. Admin need to enter username and password to login to the application. Admin needs to select whether he needs to add the evidences to fetch the evidence from blockchain. In order to add evidences admin needs to fill necessary information like record id, crime type, crime description, collected evidence details, crime area and eye witness. The by submitting evidence will be saved in the block chain. After clicking fetch evidence, all the evidences saved in blockchain can be seen by the admin. He can use those evidences to show in the court and get justice. Similarly, admin can any number of crime details in this application and record in block chain.

V. RESULTS

5.1 Login Page:

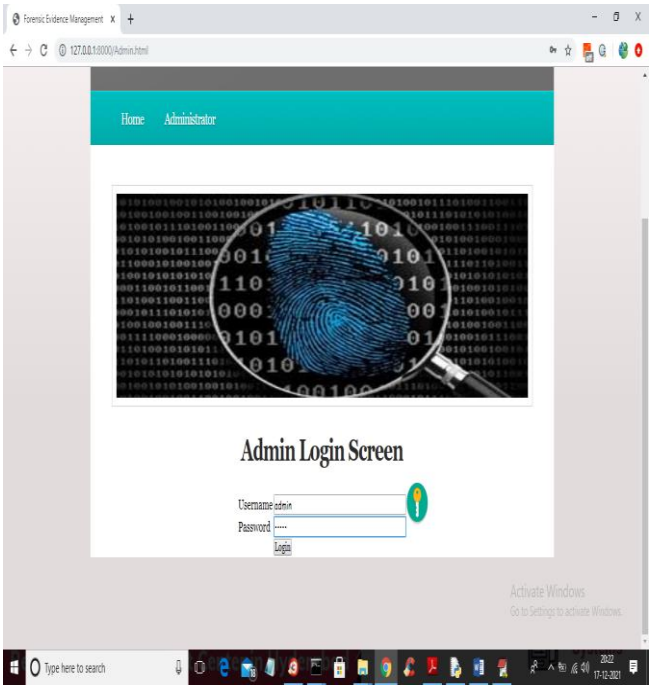

Fig. 3 The above diagram shows the login page where the authorised person need to enter the username and password.

5.2 Page to add evidences to blockchain:

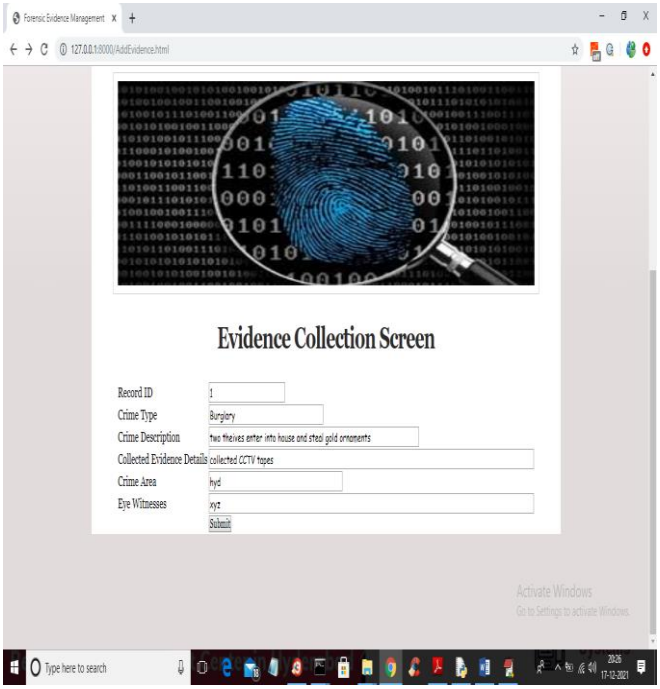

Fig. 4 The above diagram shows the page where authorized person can enter the evidence details to be saved in blockchain.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

5.3 Page to fetch evidences from blockchain:

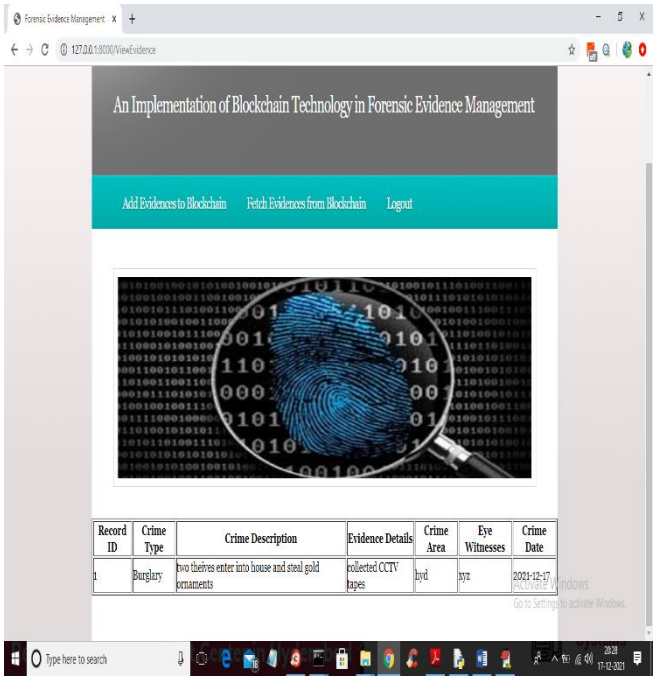

Fig. 5 The above diagram shows the page where authorized person can fetch the evidence details saved in blockchain.

VI. Conclusion And Future Works

From the time evidence is collected from the crime scene until court of law make the judgment, maintaining the integrity of the evidence is of most importance. Maintaining the chain of custody is important as it can prove if the evidence is tampered or not during the collection and analysis process. Implementation of Block chain technology to digitalize chain of custody will ensure security, authenticity and integrity of the forensic data transactions. Application of block chain will not only make it environment friendly but also increase security with the help of encryption which can be accessed remotely by authorized personnel. We intend to work on an algorithm that executes the chain of custody process utilizing block chain technology, specifically Hyper ledger Fabric. Furthermore, we can couple block chain technology with artificial intelligence/ machine learning which will help in forensic investigation.

VII. Acknowledgment

We would also like to thank our university for giving us this opportunity and also providing us with resources and knowledge. We are also thankful to our internal guide Mrs. K. Sneha for the constant support and encouragement for the completion of the paper.

VIII. 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.

[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).

[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.

[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).

[8] Castor, A. (2017). A short guide to blockchain consensus protocols. Coindesk.

[9] Cong T. Nguyen, Dinh T. Hoang, Diep N. Nguyen, Dusit Niyato, Huynh Tuong Nhuyen & Eryk Dutkiewicz. (2019).

[10] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., et al. (2018). Hyperledger fabric. Proceedings of the Thirteenth EuroSys Conference, 1–15.

[11] Goodell, G., & Aste, T. (2019). A Decentralized Digital Identity Architecture. Frontiers in Blockchain

[12] Krstić, M., & Krstić, L. (2020). Hyperledger frameworks with a special focus on Hyperledger Fabric. Vojnotehnicki Glasnik, 68(3), 639–663.