AN IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

Edakula Shivani[1], Gone Vidyadhari[2], DondetiSumanth Reddy[3], Raheem Unnisa[4]

[1]B. Tech Student, Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India, shivanireddyedakula@gmail.com

[2]B. Tech Student, Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India, vidyadharigone@gmail.com

[3]B. Tech Student, Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India, sumanthreddydondeti@gmail.com

[4]Assistant Professor, Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India, raheemaswcet.17@gmail.com

Abstract : Evidence management is pivotal in the field of measurable science. To settle a case and deal with those capable, proof accumulated from the location of a crime is fundamental. Subsequently, shielding these confirmations from altering of any kind is fundamental. Chain of guardianship is the strategy for protecting the respectability of proof. The proof will be unacceptable in court in the event that the chain of authority isn't saved, and the case will be excused. Because of its harmless to the ecosystem nature, digitalizing measurable proof administration frameworks is a dire necessity. Blockchains are painstakingly circled records of cryptographically checked trades in consecutive solicitation that are arranged into blocks and are totally available to anybody in the blockchain network. The Hyperledger Texture consortium blockchain innovation was created by the Linux Establishment and is fundamentally used for business purposes. Measurable proof administration frameworks can be digitalized and Chain of Care safeguarded utilizing Blockchain Innovation, as per the ongoing review's system and calculation.

Index Terms : Blockchain, Hyper ledger, Forensic evidence

.

1. INTRODUCTION

Evidence management is significant in the field of scientific science. In legal examination, the essential contemplations are proof dealing with and recording. From the time the proof is accumulated to the court's official choice, protecting its integrity is fundamental. The Chain of Custody (CoC) is the sequential documentation of the confirmations took care of during the examination. For the proof to be acknowledged by the court, keeping the CoC is fundamental. During the CoC cycle, various necessities should be met, including the accompanying:

Corruption and tampering with evidence must be avoided.

From the time it is accumulated until it is introduced in court, the development of the evidence during the examination should be perceptible.

The evidence should give confirmation and be relevant to the crime. The technique should be affirmed by each substance that has come into contact with the evidence.

No unauthorised person is permitted to handle the evidence in order to prevent any tampering or manipulation.

Digitalization of forensic evidence administration frameworks decreases costs, saves space, and is better for the climate. Evidence that can be used in court is acceptable due to the CoC's authenticity and legality. Blockchain technology can be used to keep them current. We can store multiple system data in a single network using blockchain technology, making them safe and accessible to customers. Utilizing technology can cut down on the amount of time required for paper examinations.
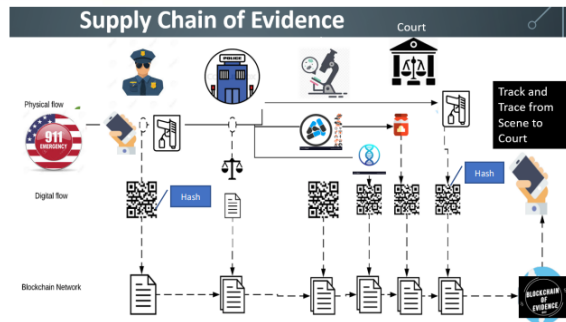
Fig 1 Example Figure

Since Blockchain supports tamper-proof and decentralized (data stored at multiple nodes or servers) data storage, which means that no one can modify data saved on Blockchain due to its data encryption and hash code approach, all businesses are now migrating their corporate data to Blockchain. Blockchain stores every exchange as a block of information and connects every exchange with a hashcode; prior to putting away any new block, the hashcode of past blocks is checked; The hashcode verification is successful if no data are altered, and the new block is added; The node is considered to be under attack if the verification fails.

The creator of a proposed study to store criminal legal information recommends utilizing Blockchain innovation attributable to its underlying capacity for sealed. The data of crime forensic evidence must be tamper-resistant because it is essential for determining the correct perpetrator. Previously, evidentiary data was either recorded on a centralized server or manually preserved.

Centralized recording can be hacked and data altered by an attacker, while manual recording is a time-consuming task that can be altered.

The author of this study is recording forensic evidence using Blockchain to address the aforementioned issues. Blockchain provides the following services:

1. There is no way to change records.
2. Each record will be checked as PROOF OF WORK, and new records will be kept with their hashcode.
3. Each block will be saved and encrypted.
4. Both public and private key generation are supported.

Blockchain can be thought of in two ways: private Blockchain, which is permissioned, and public Blockchain, which is permissionless. We are utilizing Ethereum, a permissionless Blockchain technology, in this project.

2. LITERATURE SURVEY

BCoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics.

The administration of proof is quite possibly of the main test in advanced legal sciences. From the time they are gathered until they are utilized in an official courtroom, different members in the examination can see the proof, and they take brief responsibility for. Despite the fact that various organizations control the proof, this strategy, known as Chain of Custody (CoC), should guarantee that it doesn't change during the examination for it to be acknowledged in a court. Computerized confirmations of CoC are presently totally constrained the hard way, and associations in the chain are expected to finish up going with documentation. To guarantee auditable proof honesty and proprietor recognizability while dematerializing the CoC cycle, we propose a Blockchain-based Chain of Custody (B-CoC) technique in this work. We tried the exhibition of an Ethereum-based B-CoC model.

Digital Forensics using Blockchain.

At the point when we center around the honesty of electronic proof specifically, we can see that it should be shielded from different unwanted results, such as altering or annihilation. We should be keeping watch for these and different situations while endeavoring to safeguard the immaculateness of proof and the trustworthiness of the framework for it to be acknowledged in court. The sequential recording of records is all that makes up the chain of custody. The Chain of Care contains each of the cycles that a criminal examiner should take to guarantee that the data is precise. Since it is difficult to demonstrate that proof was not changed during its assortment and use in court, the Chain of Custody (COC) is critical. Thus, the gathered proof isn't solid. By hashing and putting away information in blocks, blockchain innovation, a decentralized organization utilized by Bitcoin and other digital currency organizations, makes a protected data set. For the COC methodology, we suggest utilizing blockchain

innovation since it assists keep with following of who approaches the information and guarantees that the data submitted to the court is exact.

Authentication & Encryption Based Security Services in Blockchain Technology

Block chain is a technique that is comprehensively material without the requirement for incorporated power and has shown huge commitment for making secure associations with IoT without the mediation of an outsider. By joining the two innovations, the framework's throughput could be gotten to the next level. It is widely used in almost every industry because of its many uses, making it vulnerable to a variety of threats. This study has looked at the important characteristics of the blockchain architecture. The remainder of the article discusses numerous network threats and responses as well as security concepts like confidentiality, integrity, and availability.

A Decentralized Digital Identity Architecture.

Present day distinguishing proof frameworks depend on brought together, hierarchical frameworks that depend on respectable specialists and administrators from outsiders. According to the point of view of common liberties, we examine computerized ID, with an emphasis on personality frameworks in created countries. We contend that people should have the option to deal with their own data in different settings and that this expects them to have the option to make various irrelevant personalities. As an outcome of this, we start by characterizing a bunch of essential limitations that computerized personality frameworks should stick to shield and advance security, which is vital to the freedom of people. Considering these constraints, we propose a disseminated record innovation and shrewd administration way to deal with working with many-to-numerous associations between significant specialist organizations. Our way to deal with trust varies from others in that we don't endeavor to lay areas of strength for out adaptability by connecting qualifications to one another or to a commonly confided in power. Since the framework doesn't verifiably urge clients to hold a solitary collected character may conceivably be restricted or remade against their inclinations, people and

associations are allowed to embrace the framework and receive its rewards.

Forensic-chain: ethereum blockchain based digital forensics chain of custody

In cybercrime examinations, advanced proof is pivotal in light of the fact that associating individuals to criminal behavior is utilized. As an outcome of this, it is extremely vital to ensure the auditability, legitimacy, and respectability of computerized proof as it travels through various degrees of ordered progression in the chain of guardianship during an examination concerning cybercrime. For the legal sciences local area, the capability of blockchain innovation to give a total image of exchanges (occasions/activities) back to their starting points is huge. In this review, we recommended utilizing a blockchain for legal purposes, explicitly to safeguard the computerized criminology chain of guardianship from altering and uprightness.

3. METHODOLOGY

Evidence management is significant in the field of scientific science. In legal examination, the essential contemplations are proof dealing with and recording. From the time the evidence is gathered to the court's final decision, it is essential to preserve its integrity. In order to solve a case and bring those responsible to justice, evidence gathered from the scene of a crime is essential.

difficulties in settling the dispute and ensuring that the parties involved receive justice.

Chain of custody is the methodology for safeguarding the respectability of proof. The evidence will be unacceptable in court in the event that the chain of guardianship isn't safeguarded, and the case will be excused. Because of its harmless to the ecosystem nature, digitalizing legal proof administration frameworks is a critical prerequisite. Blockchains are painstakingly coursed records of cryptographically stamped trades in successive solicitation that are arranged into blocks and are totally open to anybody in the blockchain network. The Hyperledger Texture consortium blockchain innovation was created by the Linux Establishment and is principally used for business purposes. In view of the Hyperledger Texture idea, the ongoing review endeavored to plan

a structure and afterward propose an execution calculation.

Benefits

1. The forensic evidence administration framework will be digitalized and the Chain of Custody will be safeguarded utilizing blockchain innovation.

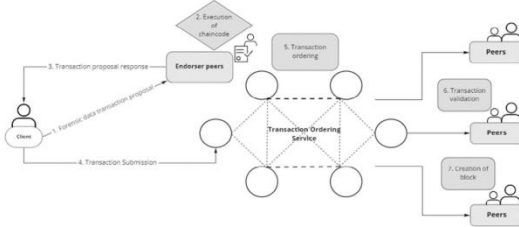2. Consequently, it is essential to safeguard these evidences against any kind of tampering.


Fig 2 Proposed Architecture

Modules:

The following modules were developed to assist us in completing this task.

1. Login as Admin: Using the username and password "admin," police officers can use this module to access the program.

2. Contribute Blockchain-Based Evidence: Police officers can upload evidence to the Ethereum Blockchain tool using this module.

3. Retrieve Blockchain-based Evidence: With this module, police officers can access all Blockchain-stored evidence; only authorized officers can access Blockchain-stored evidence.

4. IMPLEMENTATION

Blockchain Hash Function

An information string (numbers, letter sets, or media documents) of any length is changed into a line of a foreordained length utilizing a hash capability. Contingent upon the hash calculation utilized, the proper piece length might shift (for instance, 32 pieces, 64 pieces, 128 pieces, or 256 pieces). A hash is the result with a proper length. A hash estimation's cryptographic outcome is moreover this hash. The representation beneath assists us with understanding.
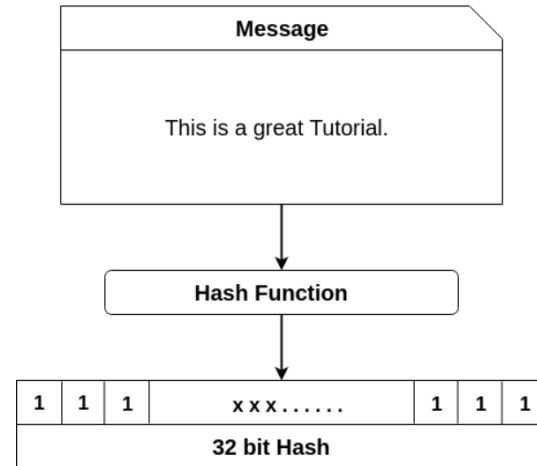
The qualities of the hash calculation are as per the following: It delivers a special result, otherwise called a hash. There is just a single way it very well may be utilized. The blockchain's agreement cycle utilizes the qualities of this cryptographic hash capability with regards to digital forms of money like Bitcoin. A condensation, or computerized finger impression, of a bunch of information is a cryptographic hash. Cryptographic hash capabilities accept exchanges as info and cycle them through a hashing interaction to create a fixed-size yield.

The subsequent hash can't be utilized to recover the whole text in light of the fact that the Hash capability is one-way. This is not the same as standard cryptographic tasks like encryption, where you utilize the way to encode something and afterward use unscrambling to decipher the message back to its unique structure.

Block chain

Blockchain is a dispersed, unchanging record that simplifies it to monitor resources and record exchanges in a business organization. Elusive resources incorporate protected innovation, licenses, copyrights, and land, among other actual resources. Nearly anything of significant worth can be checked and sold on a blockchain network, bringing down hazard and expenses for all gatherings included.

Data is an organization's soul. The sooner it is gotten and the more exact it is, the better. Since it conveys prompt, shareable, and straightforward information put away on a permanent record that must be seen by

network clients with authorization, blockchain is great for giving such data. Orders, installments, records, and creation can be generally followed by a blockchain network. You can likewise see all parts of an exchange from start to finish since individuals have a bound together viewpoint of reality. This gives you more certainty and opens up new open doors and efficiencies.

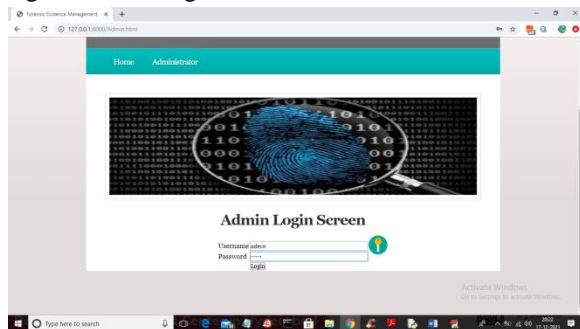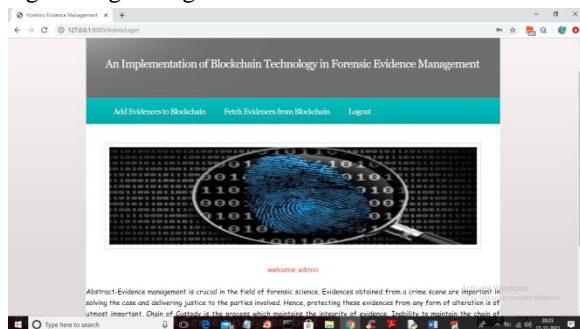## 5. EXPERIMENTAL RESULTS

Fig 3 Home Page

Fig 4 Login Page
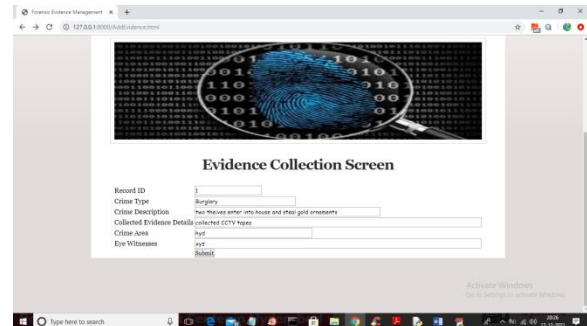

Fig 5 Add evidences block page
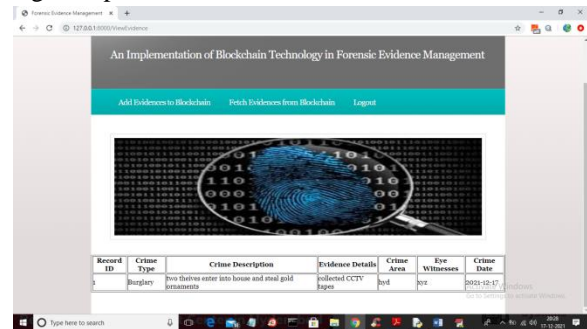

Fig 6 Upload values

Fig 7 Prediction Result

6. CONCLUSION

From the moment evidence is obtained from the scene of the crime until a decision is made by a court, it is essential to preserve its integrity. It is essential to preserve the chain of custody because it may demonstrate whether the evidence was tampered with during the process of collecting and processing it. The digitalization of the chain of custody through the application of Blockchain technology guarantees the security, validity, and integrity of forensic data exchanges. Not only will the use of blockchain make it better for the environment, but it will also improve security thanks to encryption, which can only be viewed remotely by authorized individuals. The chain of custody procedure will be carried out by an algorithm that will make use of blockchain technology, specifically Hyperledger Fabric.

Science and Engineering, Guide and Teaching and Non-Teaching faculty members for giving valuable suggestionsand guidance in every aspect of our work

8. FUTURE SCOPE

Also, forensic examinations can profit from the incorporation of blockchain innovation with artificial intelligence and machine learning.

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] 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. 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, Dusit Niyato, Huynh TuongNhuyen& Eryk Dutkiewicz. (2019). https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnu m 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

[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. VojnotehnickiGlasnik, 68(3), 639–663. https://doi.org/10.5937/vojtehg68-26206