Evidence Vault

Shubham Rajaram More,
Cyber Security Department,
Shah And Anchor Kutchhi
Engineering College
Mumbai, India
shubham.more15780@sakec.ac.in

Kshitij Siddharth Sonawane,
Cyber Security Department,
Shah And Anchor Kutchhi
Engineering College
Mumbai, India
kshitij.sonawane15860
@sakec.ac.in

Sanket Singh,
Cyber Security Department,
Shah And Anchor Kutchhi
Engineering College
Mumbai, India
sanket.singh15689@sakec.ac.in

Milind Sunkari,
Cyber Security Department,
Shah And Anchor Kutchhi
Engineering College
Mumbai, India
milind.sunkari15854@sakec.ac.in

Prof. Meghali Kalyankar,
Cyber Security Department
Shah And Anchor Kutchhi
Engineering College
Mumbai, India
meghali.kalyankar@sakec.ac.in

Abstract -
Ensuring the integrity of evidence is paramount within the realm of digital forensics. The preservation of evidence gathered at a crime scene is essential for concluding investigations and delivering justice to those involved. Hence, it is imperative to safeguard this evidence from any form of tampering.

The process that upholds the reliability of evidence is known as the "chain of custody." Failure to maintain the chain of custody can render the evidence inadmissible in court, potentially resulting in the dismissal of the case. To address these challenges and promote an eco-friendly approach, there is a need to modernize the forensic evidence protection system through digitalization.

Blockchain technology offers a promising solution in this regard. Blockchains are decentralized digital ledgers that chronologically record transactions through cryptographic signatures. These transactions are organized into blocks and are accessible to all participants within the blockchain network. In conjunction with this, the Interplanetary File System (IPFS) serves as a network file system that complements the blockchain.

The current research aims to develop a system that leverages blockchain technology to digitize the forensic evidence protection system while preserving the chain of custody. This approach is rooted in the principles of blockchain and the utilization of IPFS.

Keywords: Evidence, Blockchain Technology, Digital Forensics, Chain of Custody, IPFS, Cryptography.

I. INTRODUCTION

In the contemporary digital age, the widespread use of the internet and its associated services is a well-recognized fact. Unfortunately, with the increased access to the internet worldwide, the incidence of cybercrimes is also on the rise. In these cases, the role of evidence is crucial for investigations and solving criminal cases.

To address this challenge, a solution has been proposed that leverages blockchain technology to establish an evidence protection system. This system offers a secure and unalterable method for safeguarding digital evidence, such as documents, photos, videos, and other electronic data. It operates in a transparent and tamper-proof manner. Blockchain technology is the key enabler behind this system, providing a decentralized approach to ensure the integrity of digital evidence. Through blockchain's decentralized architecture, no single entity has full control over the evidence, enhancing security and trust.

The evidence protection system not only aids in preserving the credibility of digital evidence but also contributes to the efficient and trustworthy resolution of cybercrime cases. By creating an immutable and transparent ledger of digital evidence, it provides a high level of accountability and trust, which is crucial in the digital age.

In a world where technology continually advances, an evidence protection system using blockchain technology is a significant development. It offers a reliable and secure means of managing digital evidence, which is essential for upholding the rule of law and ensuring justice in the digital era. As internet usage and digital services continue to grow, the need for such systems will only increase, making blockchain technology a crucial tool in addressing the challenges of our interconnected world.

Chain of Custody (CoC)

The cornerstone of any criminal investigation is the evidence, as it serves as the foundation for the prosecution's case, establishing the guilt or innocence of the accused. Without evidence, progressing a case in the right direction becomes an exceedingly difficult task. The preservation of evidence is of paramount importance and requires careful handling and meticulous packaging to maintain its integrity. The process of meticulously tracking evidence from the moment it is discovered at the crime scene until it is presented in court for a trial is commonly referred to as the "chain of custody" (CoC). The chain of custody is indispensable for upholding the reliability and truthfulness of the evidence. It is the duty of the investigating officer to ensure that only authorized individuals have access to the evidence and that all necessary documentation is diligently completed in accordance with established protocols. This ensures that not only the evidence itself but also all related items are collected, packaged, preserved, and stored appropriately.

II. WHY USE BLOCKCHAIN TECHNOLOGY IN CoC

Storing information in a digital format offers several key advantages, primarily cantered around flexibility and accessibility. Authorized personnel can easily access digital documents without harming the original, even when creating and saving multiple copies. Digital information can be accessed from anywhere in the world, allowing for instant document transfers, which significantly boosts productivity by reducing the time needed to retrieve information compared to traditional paper-based systems.

However, documentation of evidence is susceptible to damage during natural or man-made disasters. To mitigate this risk and reduce the potential for corruption, blockchain technology can be integrated into the Chain of Custody process. By adopting blockchain technology, the potential for human error can also be eliminated. Incorporating such technology into forensic evidence management systems is increasingly crucial as the world progresses toward digitalization.

1) Permissioned Blockchain: Also known as a private blockchain, a permissioned blockchain restricts access to a limited number of network nodes. Participation in certifying transactions on this type of blockchain requires approval from a central authority. Enterprises often find permissioned blockchains advantageous as they offer greater scalability, controlled access, and the ability to customize performance levels. Security is influenced by the integrity of the participating members. Examples of permissioned blockchains include Ripple, Corda, and Hyperledger Fabric.

2) Permissionless Blockchain: Public blockchains, or permissionless blockchains, are open to anyone on the network for transaction processing and validation. The ledger is accessible to all network members, and anonymity is maintained among the nodes. There is no external entity overseeing the blockchain, making them highly trustworthy and secure. Examples of permissionless blockchains include Ethereum, Bitcoin, and Dash.

III. COMPONENTS OF BLOCKCHAIN

Encryption:

Encryption is the process of transforming plain text into an unreadable format that can only be deciphered by authorized individuals through the use of specific algorithms that generate variables required for decrypting the message. Encryption and decryption are fundamental components of cryptography.

In the context of blockchain technology, encryption plays a critical role in safeguarding data, concealing sensitive information, and providing a high level of security. This feature enables the handling of substantial volumes of data while ensuring the confidentiality of the information. Encrypted data can only be accessed using a secret key shared exclusively between the involved parties, making it significantly more secure compared to other systems.

A) Cryptographic Hash Function: Cryptographic hash functions play a pivotal role in blockchain technology. These functions are algorithms or processes used in cryptography to transform existing data into encrypted data of a fixed length. A message digest, often described as a fingerprint or summary of a message, is produced as a result. Cryptographic hash functions are primarily employed to verify the authenticity and integrity of data. Any alteration to the input data will yield a message digest that differs from the original one, making it easy to detect changes in the original data. Some crucial properties of hash functions required for security reasons include:

i) Preimage Resistance: Reversing a specific hash function, meaning finding an input value that corresponds to a given hash value, is computationally extremely challenging, if not practically impossible. In other words, if "h" represents the hash function and "o" is the output digest, it is highly difficult to discover an input value "i" that hashes to the same output.

ii) Second Preimage Resistance: Given an input and its corresponding hash value, it is challenging to find another input that produces the same hash value. In this case, if "h" is the hash function, "i" is the input, and "o" is the output, it is difficult to identify a different input "p" such that h(p) = h(i).

iii) Collision Resistance: It is highly improbable to find two distinct inputs that yield the same hash output, meaning it is challenging to identify two separate inputs "i" and "p" that hash to the same value.

B) Asymmetric Key Cryptography: Asymmetric cryptography, also known as public key cryptography, utilizes a pair of keys consisting of a private key and a public key. The public key is accessible to everyone, while the private key is restricted to authorized nodes. Each public key is associated with a corresponding private key. Data encryption and decryption are carried out using this key pair. This cryptographic approach establishes trust among users by providing a mechanism to verify the integrity and authenticity of transactions when they are public. In blockchain technology, public keys play a significant role in wallets and transactions. Key pairs are used, with one key for encrypting, accessible to all, and the other for decrypting, only accessible to the intended recipient. These keys are instrumental in verifying signatures generated using private keys. Private keys are exclusive to authorized entities with access and are used for digitally signing transactions.

In contrast, symmetric key cryptography relies on a single key for both data encryption and decryption. This form of cryptography is also known as secret key cryptography because the key is shared solely between the sender and receiver. Although symmetric cryptography is simpler, faster, and offers security, a significant drawback is that if the key falls into the wrong hands, the information can be easily altered. This limitation poses a major security concern for symmetric key cryptography.

C) Transaction: A transaction refers to the interaction between two parties, such as individuals or organizations. In the context of cryptocurrencies like Bitcoin, a transaction involves the transfer of cryptocurrency between users. Additionally, transactions are a fundamental way to record various activities in a business-to-business (B2B) model.

In the blockchain, each block can either contain no transactions or multiple transactions. In many blockchain systems, a continuous stream of new blocks is generated, even when there are zero transactions. This practice helps ensure the security of the blockchain network by guarding against tampering or alterations by malicious users.

While the specific data included in a transaction may vary in different implementations of blockchain technology, the fundamental process of a transaction remains similar. A node within the network initiates a transaction by sending information to the blockchain. This information typically comprises the sender's address, the sender's public key, a digital signature, and details about the transaction inputs and outputs.

D) Distributed Ledger: A ledger is essentially a repository of transactions, often stored in sizable databases and managed by a centralized and trustworthy third-party organization on behalf of users. These ledgers can be implemented using either a centralized or distributed approach.

The distributed approach is widely preferred due to its trustworthiness, security, and reliability. In this method, the blockchain network is distributed by creating multiple backup copies of the ledger data and ensuring synchronization among peers. Each user can maintain a personalized copy of the ledger. When new nodes join the network, they connect with existing nodes to locate other full nodes and request a complete copy of the ledger.

Nodes within a blockchain network play a critical role in verifying the validity of transactions and preventing the dissemination of invalid transactions among nodes. All accepted transactions are recorded in the distributed ledger of the blockchain network, and when constructing a new block, reference to the previous block is essential.

Blockchain networks utilize cryptographic techniques such as cryptographic hash functions and digital signatures to generate tamper-proof ledgers. Attempts to compromise the blockchain are thwarted by the resilience of the honest nodes within the system. In the event that a specific node is compromised, it would only impact that particular node.

E) Consensus Protocol: The Raft consensus algorithm is a distributed consensus technique designed to facilitate agreement among nodes in a network regarding the sequencing of transactions or data processing. Unlike some more complex consensus algorithms like Paxo's, Raft was specifically created with simplicity and ease of understanding in mind.

Raft operates in terms, with each term representing a distinct time interval. It follows a leader-based approach, where a single node serves as the leader, proposing changes to the distributed log and ensuring that other nodes (known as followers) execute the proposed modifications. To ensure that there is only one leader at any given time, the algorithm includes a leader election process. In the event of leader failure, a new leader is elected to maintain network stability.

Log replication is a fundamental aspect of Raft, involving the duplication of log entries to followers. Once an entry has been successfully replicated to the majority of nodes, it is considered committed, ensuring data durability. Raft provides a straightforward framework for maintaining consensus in distributed systems, with safety and durability mechanisms built in to withstand network partitions. It is a suitable choice for scenarios where robustness and clarity are essential due to its straightforward implementation.

IV. INTERPLANATARY FILE SYSTEM (IPFS)

The InterPlanetary File System, or IPFS, is a decentralized network for storage and delivery with the goal of improving the resilience, efficiency, and openness of the internet. Faster and more dependable access is made possible via IPFS, which distributes data throughout a network of peer nodes in contrast to traditional web servers that host material centrally. IPFS files are uniquely identifiable by content identifiers (CIDs), which facilitates effective versioning and retrieval. By reducing data loss, this technology not only improves data accessibility but also helps to preserve digital history. Based on content-based addressing and peer-to-peer networking, IPFS provides a more robust and egalitarian alternative to the internet's existing setup.

V. FRAMEWORK OF HYPERLEDGER FABRIC

HFCC, which stands for Hyperledger Fabric Chain of Custody, is a framework that leverages blockchain technology to maintain an immutable record of transactions related to the transfer of evidence from one authorized personnel to another. The framework ensures that only authorized individuals have access to these transactions, and the use of cryptography guarantees the immutability, traceability, and validity of the evidence.

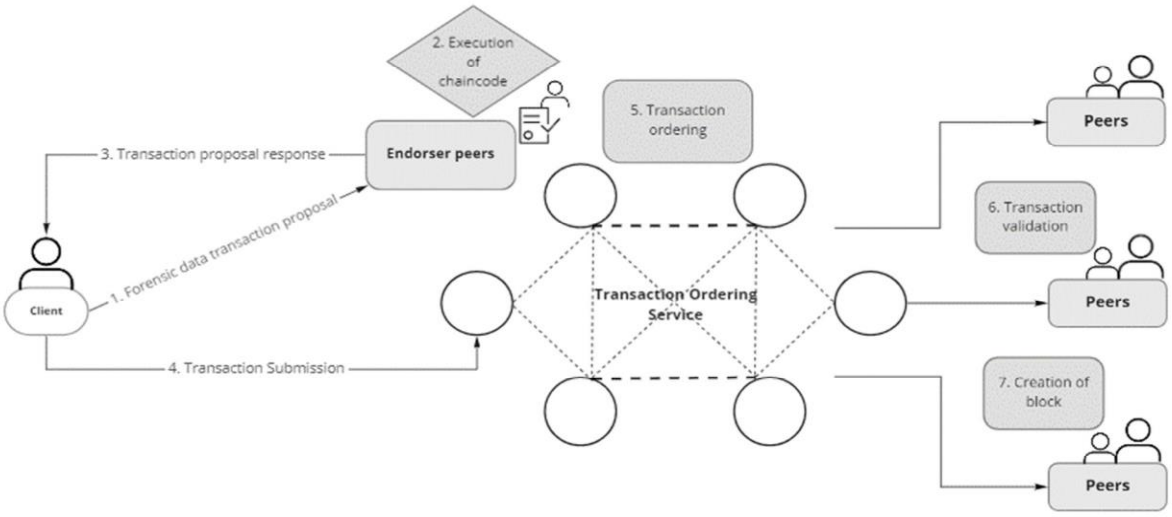
2. Execution of chaincode
5. Transaction ordering
3. Transaction proposal response
Endorser peers
1. Forensic data transaction proposal
Client
4. Transaction Submission
Transaction Ordering Service
Peers
6. Transaction validation
Peers
7. Creation of block
Peers

Figure 1 Transaction Flow of Hyperledger

The process within Hyperledger Fabric involves the following steps:

1. A client, such as the Evidence Collection Unit (ECU), initiates a transaction request.

2. A transaction proposal is generated by the Software Development Kit (SDK) application and sent to endorsing peer nodes, such as the Director or Head of the team. This application formats the proposal correctly and creates a unique signature using the client's encrypted credentials.

3. The endorsing peers validate the proposal by checking if it adheres to specific standards, including proper formatting, a valid signature, no previous submission, and authorization of the client for the proposed operation on the channel.

4. The endorsing peers take the transaction proposal inputs as an argument and invoke the chain code or smart contract against the database to generate a transaction response.

5. The proposal response includes the endorser peers' signatures, which are verified and compared by the SDK application. The application ensures that all mentioned endorsement policies are satisfied before submission.

6. The transaction is then broadcast to ordering nodes, which can include entities like the court of law, forensic departments, and police stations. The transaction message includes write/read sets, the signatures of endorser peers, and the channel ID. The ordering service organizes the transactions chronologically by channel and creates blocks accordingly.

7. These blocks are sent to all peers within the channel, and they are validated to confirm that the endorsement policy has been met. The blocks are marked as valid or invalid accordingly.

8. Each peer appends the updated block to the channel's chain and adds it to the database. A confirmation message is sent to the client, indicating that the transaction has been permanently added along with its validity.

The HFCC framework for Chain of Custody provides a secure and transparent way to document evidence transactions, ensuring the integrity and trustworthiness of the process.

V. CONCLUSION AND FUTURE WORKS

CONCLUSION

1) Blockchain technology holds substantial promise in the development of evidence protection systems designed to guarantee the integrity and authenticity of digital evidence.
2) Implementing evidence protection systems based on blockchain technology can effectively address the challenge of tampering with digital evidence, a critical issue in legal and forensic investigations.
3) Through the utilization of a decentralized and immutable platform, blockchain technology offers the potential to create a transparent and highly secure system.

Please note that for real-world applications, it is essential for the organization implementing this system to employ a consortium blockchain and a customized platform similar to IPFS. This approach ensures that the data stored remains private and exclusive to the organization, enhancing security and privacy.

FUTURE SCOPE

Looking ahead to the future of our project, the incorporation of an Authentication Module, Chain of Custody, Admin Panel, and SSL Encryption for data during transit will play pivotal roles in safeguarding the security and integrity of our system. With the growing menace of cyberattacks and data breaches, it becomes imperative to establish a resilient and secure system capable of safeguarding sensitive data and preserving user privacy.

The Authentication Module will be instrumental in ensuring that access to sensitive information is restricted solely to authorized individuals. Concurrently, the Chain of Custody will meticulously maintain an audit trail of all data-related activities, providing transparency and accountability in the system.

The Admin Panel serves as a centralized hub for system administrators, facilitating the efficient management and monitoring of system settings and user activities. This centralized control enhances our ability to promptly identify and address any anomalies or security breaches.

Furthermore, the deployment of SSL Encryption for data during transit establishes secure communication channels between users and the system. This critical measure effectively thwarts unauthorized access attempts and fortifies our defences against potential data breaches.

By integrating these robust security features, we are poised to construct a system that is future-proof, capable of withstanding emerging threats, and steadfastly upholding the confidentiality, integrity, and availability of critical information.

VI. ACKNOWLEDEMENT

We have great pleasure in presenting the project on “EVIDENCE VAULT”. We take this opportunity to express our sincere thanks to our Guide Ms. Meghali Kalyankar, the faculty in the Department of Cyber Security in Shah and Anchor Kutchhi Engineering College for guiding us and suggesting regarding the line of work. We would like to express our gratitude towards their constant encouragement, support and guidance throughout the progress.

Also, we would like to thank our principal – Dr. Bhavesh Patel and Dr. Nilakshi Jain, Head of Cyber Security Department, for their help, support & guidance for this project.

We are also thankful to all Faculty members of our department for their help and guidance during completion of our project.

REFERENCES

1. Mar Gimenez-Aguilar , Jose Maria de Fuentes , Lorena Gonzalez-Manzano ,David Arroyo(2021) – Achieving cybersecurity in blockchain-based systems: A survey. www.elsevier.com/locate/fgcs[1]
2. Abin Oommen Philip, RA K Saravanaguru (2022) - Smart contract based digital evidence management framework over blockchain for vehicle accident investigation in IoV era. www.sciencedirect.com[2]
3. Jingyu Zhang, Siqi Zhong, Tian Wang, Han-Chieh Chao, Jin Wang - Blockchain-based Systems and Applications: A Survey. DOI: 10.3966/160792642020012101001. https://drive.google.com/file/d/12haTnLrVzhfDzLW4xxgT8b54SW3s3RJv/view?usp=share_link[3]
4. Gongzheng Liu , Jingsha He , and Xinggang Xuan (2021) - A Data Preservation Method Based on Blockchain and Multidimensional Hash for Digital Forensics. Volume 2021, Article ID 5536326, https://doi.org/10.1155/2021/5536326[4]
5. Maria Stoyanova , Yannis Nikoloudakis , Spyridon Panagiotakis , Evangelos Pallis, and Evangelos K. Markakis - A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 22, NO. 2, SECOND QUARTER 2020. https://creativecommons.org/licenses/by/4.0/[5]
6. Sharon Philip, Nrashant Singh (2021) - An Implementation of Blockchain Technology in Forensic Evidence Management. 2021 International Conference on Computational Intelligence and Knowledge Economy

(ICCIKE) March 17–18, 2021, Amity University Dubai, UAE. [6]

7. Dr.S. Harihara Gopalan, S. Akila Suba, C. Ashmithashree,□A. Gayathri, V. Jebin Andrews – Digital Forensics Using Blockchain. International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-2S11, September 2019.https://www.sciencedirect.com/science/article/pii/S1319157822001719?via%3Dihub [7]
8. Derick Anderes, Edward Baumel, Christian Grier, Ryan Veun, and Shante Wright - The Use of Blockchain within Evidence Management Systems. Alister INC [8]
9. Mr.S. Nelson M E., Mr. K. Ponvasanth B.Tech., Mr. S. Karuppusamy B.Tech., Mr. R. Ezhumalai B.Tech. - Blockchain based Digital Forensics Investigation Framework in the Internet of Things and Social Systems. International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181, www.ijert.org [9]
10. Junho Jeong*, Donghyo Kim**, Byungdo Lee***, and Yunsik Son** - Design and Implementation of a Digital Evidence Management Model Based on Hyperledger Fabric Journal of information processing systems. https://doi.org/10.3745/JIPS.04.0178 [10]
11. Prasanth Varma Kakarlapudi and Qusay H. Mahmoud - Design and Development of a Blockchain-Based System for Private Data Management. MDPI. https://www.mdpi.com/2079-9292/10/24/3131 [11]
12. Halima Mhamdi , Manel Ayadi 2, Amel Ksibi 2,* , Amal Al-Rasheed 2, Ben Othman Soufiene 3 and Sakli Hedi - SEMRAchain: A Secure Electronic Medical Record Based on Blockchain Technology. MDPI. https://www.mdpi.com/2079-9292/10/24/3131 [12]
13. Dr. Reshma Banu, Deeksha G, M Preethi, BLOCKCHAIN TECHNOLOGY FOR SECURING FORENSIC EVIDENCE. IJCRT, Volume 10, Issue 6 June 2022 | ISSN: 2320-2882. www.ijcrt.org [13]
14. Yogita K Borse, Deepti J Patole, Gaurav Navnit Chawhan - Advantages of Blockchain in Digital Forensic Evidence Management. https://ssrn.com/abstract=3883953c [14]
15. Donghyo Kim , Sun-Young Ihm and Yunsik Son - Two-Level Blockchain System for Digital Crime Evidence Management. MDPI. https://www.mdpi.com/2079-9292/10/24/3131 [15]
16. Eko Yunianto, Yudi Prayudi - B-DEC: Digital Evidence Cabinet based on Blockchain for Evidence Management . https://www.researchgate.net/publication/331802213 [16]
17. https://www.researchgate.net/publication/341745800_Tainted_Digital_Evidence_and_Privacy_Protection_in_Blockchain-Based_Systems [17]
18. https://eudl.eu/pdf/10.4108/eai.3-6-2022.174089 [18]
19. https://arxiv.org/ftp/arxiv/papers/2107/2107.14050.pdf [19]
20. https://ijcrt.org/papers/IJCRT22A6867.pdf [20]
21. https://www.researchgate.net/publication/354964804_Evidence_Management_System_Using_Blockchain_and_Distributed_File_System_IPFS [21]
22. https://www.sciencedirect.com/science/article/pii/S1319157822001719?via%3Dihub [22]
23. https://www.hindawi.com/journals/complexity/2021/5536326/ [23]
24. https://www.ijrte.org/wp-content/uploads/papers/v8i2S11/B10300982S1119.pdf [24]
25. https://www.ijert.org/research/blockchain-based-digital-forensics-investigation-framework-in-the-internet-of-things-and-social-systems-IJERTCONV8IS12026.pdf [25]
26. http://jips-k.org/digital-library/23797 [26]
27. https://www.researchgate.net/publication/362153704_Digital_Forensics_using_blockchain?enrichId=rgreq-0d70d28db3138b4f1c7c4e90f5f78a85-XXX&enrichSource=Y292ZXJQYWdlOzM2MjE1MzcwNDtBUzoxMTgwMTYxNDkxOTEwNjU2QDE2NTgzODM4MzQ5Mzc%3D&el=1_x_2&_esc=publicationCoverPdf [27]
28. https://ijcrt.org/papers/IJCRT22A6867.pdf [28]