2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)
March 17–18, 2021, Amity University Dubai, UAE

2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE) | 978-1-6654-2921-4/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICCIKE51210.2021.9410791

An Implementation of Blockchain Technology in Forensic Evidence Management

Revathy Sathyaprakasan,
Department of Forensic Science,
Amity University Dubai
revathyP@amitydubai.ae

Pratheeksha Govindan,
Department of Forensic Science,
Amity University Dubai
pratheekshaG@amitydubai.ae

Samina Alvi,
Department of Forensic Science,
Amity University Dubai
saminaA@amitydubai.ae

Lipsa Sadath,
Department of Computer Science,
Amity University Dubai
lsadath@amityuniversity.ae

Sharon Philip,
Department of Forensic Science,
Amity University Dubai
sphilip@amityuniversity.ae

Nrashant Singh*,
Department of Forensic Science,
Amity University Dubai,
nsingh@amityuniversity.ae

*Corresponding Author

***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 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, 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 of Custody.**

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

I. INTRODUCTION

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.
- ✓ From the time the evidence is collected till it's submission in the court, the movement of the evidence throughout the investigation should be traceable [1].
- ✓ 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 [2].

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 blockchain technology. Blockchain 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.

Chain of Custody (CoC)

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 is 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

978-1-6654-2921-4/21/$31.00 ©2021 IEEE

contamination or damage.

II. WHY USE BLOCKCHAIN TECHNOLOGY 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 blockchain technology in the process of Chain of Custody will mitigate the risk of damaging these documents. Using this technology will also help in irradicating human error. As the world is moving towards digitization, it is really important to implement such technologies in forensic evidence management system.

1) *Permissioned Blockchain:* Permissioned blockchain is also known as private blockchain and its access is restricted to a few nodes in the network [3]. Those who want to take part in validating the transactions need to be approved by a central authority. This type of blockchain is useful for enterprise use. These types are highly customizable, have better scalability, have controlled access and are very efficient in performance. Security of the system depends on the members and their integrity. Ripple, Corda and Hyperledger Fabric are few examples of permissioned blockchain.

2) *Permissionless Blockchain:* Permissionless blockchains are also known as public blockchain. This type of blockchain allows anyone on the network to participate in the transaction process and also in validating these transactions. Everyone in the network has a copy of the ledger. There is no third party controlling the blockchain and the anonymity of the nodes are maintained. They are reliable and very secure. Ethereum, Bitcoin and Dash are few examples of permissionless blockchain.

III. COMPONENTS OF BLOCKCHAIN

Encryption:
Encryption is a process in which a normal text can be converted to an unreadable text which can only be decoded by the authorized personnel by making use of various algorithms which can help in producing variables suitable for decrypting the message. Encryption and decryption together form the basis of cryptography.

Encryption is a very important aspect in blockchain technology as it can resist hacking, hide and protect the confidential data easily. Due to this feature, huge volumes of data can be handled. The encrypted data can only be opened by a secret key between the parties involved making it hundred times secure than any other system [4].

A) Cryptographic Hash Function: Cryptographic Hash Functions are one of the most important components in blockchain technology. They are algorithms or functions that are used in cryptography to convert an already existing data into enciphered data of a fixed length. A message digest is a fingerprint or the summary of a message [5]. They are mainly used for checking the authenticity of a given data and to verify their integrity. Any change in the input data will result in a message digest that is not identical to the original one. Hence, any change in the original input data can be identified easily.

Some of the properties of hash functions that are required for security reasons are:

i) ***Preimage Resistance*** – It is nearly impossible to reverse a particular hash function, i.e., if h and o are the hash function and the output digest respectively, then it is computationally very difficult to find an input value i that hashes to o.

ii) ***Second Preimage Resistance*** – For a given input and its hash value, it would be difficult to attain another input with the same hash value, i.e., if h is the hash function and i and o are the input and the output respectively, then it is difficult to find another input p such that h(p) = h(i).

iii) ***Collision Resistance*** – Two different inputs that hashes the same output cannot be or are nearly impossible to be found, i.e., it is difficult to attain two separate inputs i and p such that they have the same hash value.

B) Asymmetric Key Cryptography: Asymmetric cryptography makes use of a pair of keys in which one is private and the other is a public key [6]. Everyone can access the public key whereas the private key can only be accessed by authorized nodes. Each public key comes along with a private key. The encryption and decryption of the data can be done with the help of the public and private key. This form of cryptography creates a trust factor among the users by contributing a mechanism that can validate the integrity as well as the authenticity of the particular transaction when it is public.

Public key plays an important role in blockchain wallets and transaction. It makes use of keypairs, one for enciphering, that can be accessed by all and the other for deciphering which can only be accessed by the intended receiver. They are used to validate the signatures that are generated using private keys. Private keys are only for the authorities who have access to it and can be used to sign the transactions digitally.

Contrastingly, symmetric key cryptography makes use of only a single key for encrypting as well as decrypting a data. Since the key is known only to the sender and receiver, it is also known as secret key cryptography. Though it is simpler, quicker and more secure, once it reaches the hands of the intruder, the information can be changed easily and hence is a major drawback in this form of cryptography.

C) Transaction: The interaction between two individuals, organizations etc., is known as a transaction. For example, between bitcoin users, the transfer of cryptocurrency is known as transaction. This is a method used to document the various activities in a business-to-business (B2B) model [7]. Every block may contain zero transactions or may contain more than one. In several blockchain systems, a continuous supply of new blocks is needed even if it's a zero transaction which make sure that the blockchain network is secured from any alteration caused by malicious users. For various implementations of Blockchain technology, the data that includes a transaction maybe different but the process of transaction is similar.

A node in the will sends information to the blockchain network. The sent information will contain the sender's address, sender's public key, a digital signature, transaction inputs and outputs [7].

D) *Distributed Ledger:* A ledger is a collection of transactions that are stored in large databases that are operated by a centralized and trustworthy 3rd party organization on behalf of the users. Ledgers can be implemented in either a distributed or centralized approach [7].

Distributed approach is more popular owing to its trustworthiness, security and reliability. The distribution of blockchain network is achieved by generating multiple backup copies and syncing all of it to the same ledger data amongst peers. A personalized copy of the ledger can be kept by each user. While joining the network, the new nodes reach out to the existing network to find other full nodes and appeal for a full copy of its ledger.

The nodes in a blockchain network must ensure that the transactions made are valid and prevent propagation of invalid transactions between nodes. All the transactions that have been accepted are held in the distributed ledger of the blockchain network. A reference to the previous block needs to be made while building a new block.

Blockchain network uses cryptographic mechanisms such as cryptographic hash functions and digital signatures to produce tamper-proof ledgers [7]. Targeting the blockchain would be countered with the resistance of the honest nodes present in the system. If any specific node was not recovered, it would only affect that particular node.

E) *Consensus Protocol:*

i. ***Proof of Work***

Proof of Work (PoW) is the original consensus algorithm in a Blockchain network. In the PoW protocol, miners compete with each other on a network to solve complex computational puzzles. When a miner finds the solution to the given complex puzzle, they will then broadcast the solved block into the network and all the remaining miners then check the solution and verify if it is correct [8].

In Blockchain, this protocol is used for confirming transactions and producing blocks that are new in the chain.

ii. ***Proof of Stake***

Proof of Stake (PoS) is commonly used instead of the proof of work protocol. In this protocol, the person or the validator must validate the block depending on the number of coins they have. The bigger the stake, the bigger the chances of solving the block [9]. Therefore, more the coins a validator or a miner has, more mining power they have and will get to assign the block. This consensus method was created in order to mitigate the issues inherited by the PoW protocol.

Smart contracts

Smart contracts are agreements made between two parties which are present in computer codes. It doesn't require an additional party to deal with it. Smart contracts work in the same way as a normal contract in which certain codes can be added directly and the involved parties can examine them before the required time. These contracts have certain terms and conditions which are to be maintained. The anatomy of a smart contract involves identifying an agreement, setting conditions, coding the logic of the business, encrypting in the blockchain technology which can help in securing and verifying the messages that it consists of, executing and processing and finally the updating of the network. Since it deals with blockchain, it is preserved in a database and is irreversible. All transactions in a smart contract need to be dealt with by the blockchain technology primarily and hence a third party is not needed, which in turn reduces the time as well.

IV. HYPERLEDGER FABRIC

Hyperledger Fabric is a modular open-source system for installing and operating permissioned blockchains. It is a consortium blockchain in which there are many channels for different organizations and only authorized nodes can access the network. It is used for building a blockchain network structure for transactions between businesses (B2B) and between businesses and consumers (B2C) [10].

Hyperledger Fabric uses features such as public key cryptography and digital certificates for access control and the identity and roles of the nodes in the network. Hence, using this technique ensures integrity of the participating nodes and only those nodes that are authorized are allowed to participate in the transactions and validation process.

Hyperledger Fabric uses features such as public key cryptography and digital certificates for access control and the identity and roles of the nodes in the network. Hence, using this technique ensures integrity of the participating nodes and only those nodes that are authorized are allowed to participate in the transactions and validation process.

V. FRAMEWORK OF HYPERLEDGER FABRIC FOR CHAIN OF CUSTODY (HFCC)

HFCC is a framework for chain of custody using blockchain technology, as shown in Figure 1, which helps in producing exact copies of ledgers across the nodes in the network for documenting transaction of the evidence from personnel to personnel. Only authorized personnel will access these transactions. The use of cryptography will ensure immutability, traceability and validity of the evidences.

The Hyperledger fabric based on blockchain technology goes through the following process:

a. A client, for example, The Evidence Collection Unit

(ECU), sends a request for transaction.

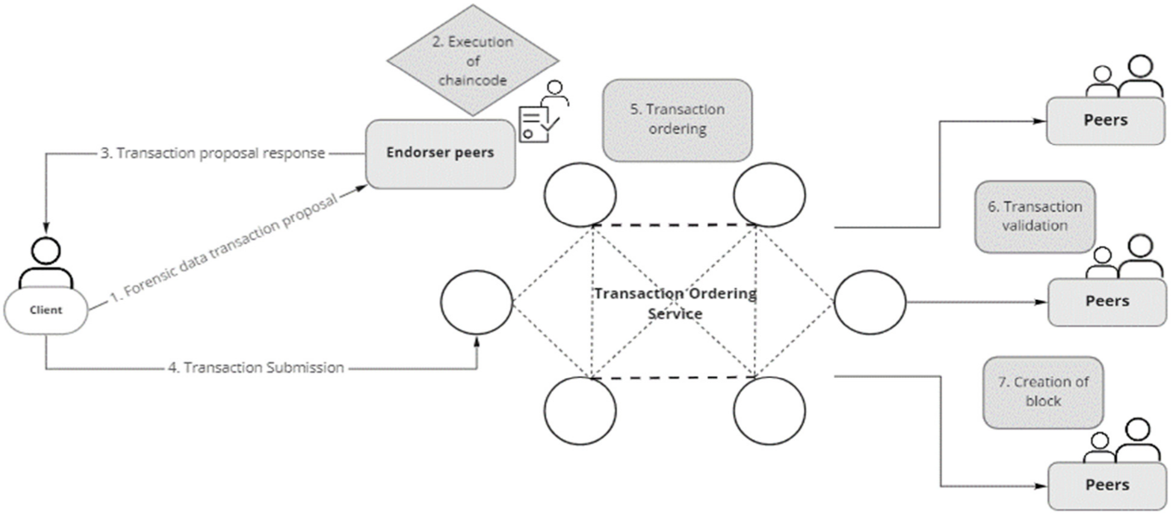
2. Execution of chaincode
5. Transaction ordering
Endorser peers
3. Transaction proposal response
1. Forensic data transaction proposal
Client
Transaction Ordering Service
4. Transaction Submission
Peers
6. Transaction validation
Peers
7. Creation of block
Peers

Fig. 1 HFCC framework for Chain of Custody (CoC)

b. A transaction proposal is then created by the SDK (software development kit) application which is then sent to the endorsing peers' nodes, the Director/Head of the team. This application properly formats the proposal and produces a signature that is unique using the encrypted credentials of the client.

c. The endorsing peers then check and verify if the proposal has followed certain standards that include:

- The proposal is well formatted
- The signature is a valid or not
- If the proposal has been submitted previously or not
- If the client is authorized to conduct the operation that was proposed on the channel.

d. The transaction proposal inputs are taken by the endorsing peers as an argument that invokes the chaincode or smart contract against the database in order to provide a transaction response.

e. The proposal response includes the endorser peer's signature which is verified and compared by the SDK application. The application decides whether all the mentioned endorsement policies have been satisfied before its submission [11].

f. The transaction is then broadcasted to the ordering nodes which may include the court of law, forensic department, the police station etc., by providing a transaction message which consists of the write/read sets, the signature of the endorser peers and the ID of the channel. The job of the ordering service is to simply order the transactions chronologically according to their channels in the network and create blocks respectively.

g. These blocks are sent to all the peers that are present in the channel. It is then validated to make sure the endorsement policy is satisfied and accordingly the blocks are labeled as valid or invalid.

h. This updated block is finally appended to the channels chain by each of the peers and is added to the database [12]. A confirmation message is sent to the client stating that the transaction has been permanently added along with the validity of the transaction.

V. 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 Blockchain technology to digitalize chain of custody will ensure security, authenticity and integrity of the forensic data transactions. Application of blockchain 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 blockchain technology, specifically Hyperledger Fabric. Furthermore, we can couple blockchain technology with artificial intelligence/ machine learning which will help in forensic investigation.

VI. ACKNOWLEDEMENT

We would also like to thank our university for giving us this opportunity and also providing us with resources and knowledge.

REFERENCES

[1] Bonomi, S., Casini, M., & Ciccotelli, C. (2018). B-CoC: 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-blockchain-consensus-protocols

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