Digital Forensics Using Blockchain

**Dr.S. Harihara Gopalan, S. Akila Suba,
C. Ashmithashree, A. Gayathri, V. Jebin Andrews**

Abstract--- On considering the integrity of electronic evidence, in particular,we can see that such evidence needs to be protected from a number of undesirable outcomes namely, alteration or destruction. We need to guard against these events and others when trying to maintain system integrity and preserve the purity of evidence so that it could be acceptable in the court. Chain of Custody is nothing but the consecutive documentation of records. The Chain of Custody has all the necessary steps that a crime investigator must follow to make sure whether the information is honest. The Chain of Custody is significant because it cannot be proven that evidence was not altered during the time between collection and its usage in court. Then the collected evidence is not credible. Blockchain technology,a decentralized network currently used by Bitcoins and other Cryptocurrency networks, helps provide a secure database with the help of hashing the data and storing it in blocks.We propose to implement blockchain technology for the process of Chain of Custody, which helps in tracking the people whoaccess the data and assist in assuring the credibility of the data provided during the time of submission in court.

Keywords--- Chain of Custody(CoC), Blockchain-Based Chain of Custody (B-CoC), Proof of Work (PoW).

I. INTRODUCTION

One of the most important problems in digital forensics is the management of evidence. Digital proof plays a very important role in crime investigation because it is employed to link persons with criminal activities. It is of extreme importance to guarantee integrity, authenticity, and auditof digital evidence as it moves along different levels of hierarchy i.e. from first responder to higher authorities responsible for handling cybercrime investigation. Digital proof comes with its own distinctive challenges associated with chain of custody. Blockchain technology's capability to sectionalize comprehensive read of transactions back to origination provides monumental promise for the rhetorical community. Basically, it is a distributed information that maintains an incessantly growing tamper proof arrangement blocks that hold batches of individual transactions. It implements a decentralized fully replicated append-only ledger in a peer-to-peer network, originally deployed for the Bitcoin cryptocurrency. All participating nodes maintain a full local copy of the blockchain. The blockchain consists of a sequence of blocks containing the transactions of the ledger. Transactions within blocks are sorted chronologically and every block contains a cryptographic hash of the previous block within the chain. Each block contains a timestamp and data link that points to a previous block. Blockchain has 4 elements that are replicated: the ledger, cryptography, consensus and business logic. The Hyperledger is a Linux Foundation project which is an open-source collaborative effort created to advance cross-industry Blockchain technologies. CoC is extensively used as evidence, to be acceptable in a court or in legal procedures, must be proved to be not altered during investigations. The issues of CoC become very important, as authenticity of evidence must be maintained in accordance with the condition when it was first discovered until later presented in court. Thus, a decent CoC method ought to use typical procedures for dealing and handling evidence (digital or not), in spite of whether or not the proof is utilized in an attempt or not.

The main requirements of a CoC process are:

Integrity: Throughout the transfer, the proofhas not been altered or corrupted.

Traceability: The proof should be derived from the time of its collectionuntil it's ruined.

Authentication: All the witness interacting with associate proof should offer an associate positive sign as recognizable proof of their identity.

Verifiability: The entire method should be verifiable from each entity concerned within the method.

Security: Tampering proof - Changeovers of evidence cannot be altered or corrupted. Leveraging on these features, we define an architecture able to support the CoC process. In specific, we intend to come up with a non-public permission blockchain and enforce a wise contract to keep track of the possession changes throughout the proof lifecycle.

II. BACKGROUND STUDY

A.Blockchain

The blockchain is a growing list of records. With the invention of Bitcoin in 2008, the blockchain was evolved. It is something that promises to have an impact on every industry, including but not limited to the financial sector, government, media, law and arts. The ledger or records is distributed between multiple participants, called nodes on peer to peer networks. The blockchain can be categorized into different subcategories depending on whether authorisation is required for network nodes to act as verifier[5].In Blockchain, each block contains secured hash of previous block, current block and timestamp. When records are added to the blockchain it gets added with previous hash value if anyone tries to modify the existing data, the hash value varies and the chain breaks.

Manuscript received September 16, 2019.

Dr.S. Harihara Gopalan, Sri Ramakrishna Engineering College, Coimbatore. T.N, India. (e-mail: hs@srec.ac.in)

S. Akila Suba, Sri Ramakrishna Engineering College, Coimbatore. T.N, India.(e-mail: akilasuba.1701009@srec.ac.in)

C. Ashmithashree, Sri Ramakrishna Engineering College, Coimbatore. T.N, India. (e-mail: ashmithashree.1701016@srec.ac.in)

A. Gayathri, Sri Ramakrishna Engineering College, Coimbatore. T.N, India.(e-mail: gayathri.1701046@srec.ac.in)

V. Jebin Andrews, Sri Ramakrishna Engineering College, Coimbatore. T.N, India. (e-mail: jebinandrews.1701059@srec.ac.in)

B.Chain of Custody

CoC is nothing but the consecutive documentation that records the order of custody, control, transfer, analysis and physical or electronic evidence. CoC contains perilous steps during the investigation and the procedure of submitting the evidence in court. Each and every individual is responsible for the evidence taken by him/her. Any sign of change in evidence would prove it to be invaluable at the time presented in court [3]. Collection techniques involve preservation, packaging, transportation, storage and creation of the inventory list founding the CoC. All data including documentation of the location of the data recovery, the time and date or description of the item, condition of the item and any uncommon markings on or changes to the item [4]. A blockchain is simply an accounting system - a ledger. The blockchain is a distributed ledger that records transactions where values are exchanged. Distributed meaning that there are multiple copies of the ledger in existence. The ledger is distributed between multiple participants, called nodes on a Peer-to-Peer network [5].

- CoC should be protected from changes in the evidence after their collection. Hence it is a necessity to store the evidence in a way that is impossible to tamper so that it would be easy to present the evidence the court without any doubt on its purity.
- Collection of evidence plays a vital role as further investigation is totally dependent upon the type of evidences collected. Analysing the evidence could give a better understanding of the crime occurred and come up with why and how a crime occurred. CoC helps show where the possible evidence might lie, where it came from, who created it, and the type of equipment that was used.
- The evidence collected are uploaded to the blockchain to make them tamper-proof as the copies of evidences are stored as a distributed ledger so as to preserve the purity of evidences when submitted in the court.
- The hash value that is generated in each block makes the system more secure by breaking the link between the blocks if any changes occur to the data since it is vital to confirm that the whole CoC is conferred alongside the proof at the court.

C.Issues Facing in the Chain of Custody

- Due to the increase in data volume there is reduction in flexibility and capability of document.
- Making use of digital evidence and documentation to create the CoC.
- CoC documentation, considering that evidence can move from one party to another.
- One of the judge and jury to take a decision is the way to present information that can be understood by both the judges and other law enforcement agencies. In this case, CoC must provide 2 aspects of information, i.e. information that is directly related to the case as well as information related to the source, originality and the process for obtaining such evidence.

III. METHODOLOGY

In order to ensure that the CoC is as authentic as possible, a series of steps must be followed

Step1: The evidence, from the crime scene or the place of investigation, are collected in form of DNA analyser, video, audio, text, images or even system logs including the time of the evidence collected to make a timeline.

Step2:The collected data are uploaded to the database which helps to store the case details. A URL is generated according to the data uploaded to it.The generated URL is extracted and used for hashing in the blockchain.

Step3:The extracted URL is considered as string and it is passed through hash algorithm for hashing. The timestamp also hashed along with URL for more integrity. The hashed value is stored in the block itself.

Step4:The block is created along with timestamp. The timestamp helps to find when the evidence was uploaded to the blockchain.Incase of any tamper it will change, which leads to breaking of chain. If the chain is not broken, itensuresthe block is in proper state.

Step5:PoW is a method to ensure whether the evidence have been tampered, as the connection of the blocks would've been lost after a certain point. This can be done by rehashing the existing blocks to cross-reference with the current data.

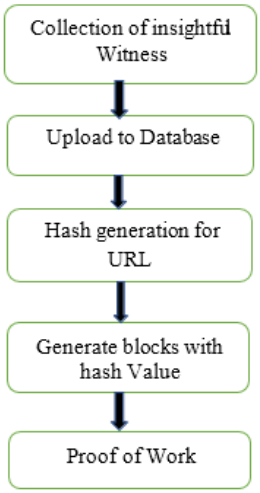

Fig. 1: Flow Idea of B-CoC

IV. RESULTS

Thus blockchain helps to implement the CoC in a tenable way. Afterthe creation of block, it contains hashed value, timestamp, and the previous hash value which helps to track the block. This also creates a user friendly approach for access, so anyone can view the details. It satisfies all the requirements of CoC i.e. It provides integrity and authenticity by issuing user id for every user for using the database and the block undergoes mining to assure it is secure and tamper-proof. By implementing the proposed idea through an application resulted in creating a chain of custody with blockchain. Fig 2 consists of working of android application and Fig 3.1 and Fig 3.2 containscreenshots.

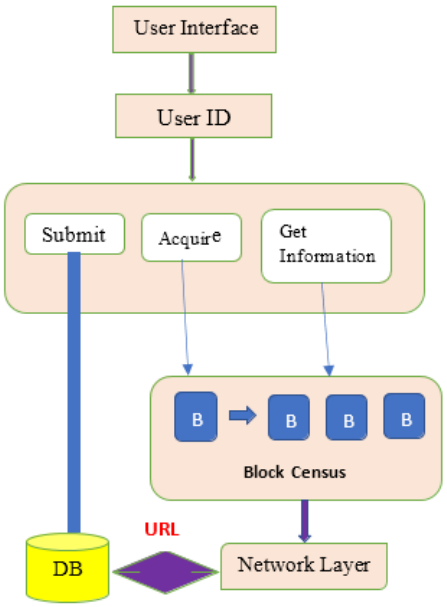

Fig. 2: Application Oriented B-CoC

Fig. 3.1: Authorisation and Case View Screen

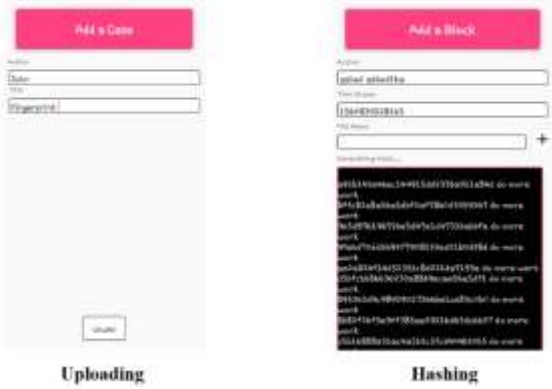

Fig. 3.2: Uploading and Hashing Phase

V. CONCLUSION

Blockchain by proposal harvests the best of security, integrity, transparency and audit thus making it the unsurpassed choice for maintaining and securing the forensicCoC. Blockchain decreases conflict and increases belief through the distributed blockchain making it impossible to alter every block. Blockchain is the most effective solution for CoC for the digital era of forensics. This paper presented on Digital Forensics in Blockchain: We provide a detailed study of the blockchain using CoCand the proposed method of providing the service to the forensics community for their use.

REFERENCES

1. Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. Digital Investigation, 28, 44-55.
2. https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/legal-and-ethical-principles/chain-of-custody-in-computer-forensics/#gref
3. https://en.wikipedia.org/wiki/Chain_of_custody.
4. https://projects.nfstc.org/property_crimes/module03/pro_m03_t17.html.
5. Hreinsson, E. M., & Blöndal, S. P. The future of blockchaintechnology and cryptocurrencies (Doctoral dissertation).
6. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
7. Singh, S., & Singh, N. (2016, December). Blockchain: Future of financial and cyber security. In 2016 2nd *International Conference on Contemporary Computing and Informatics (IC3I)* (pp. 463-467). IEEE.
8. Buterin, V. (2013). Ethereum white paper.(2013). URLhttps://github. com/ethereum/wiki/wiki/White-Paper.
9. 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.
10. Lone, A. H., & Mir, R. N. (2018). Forensic-chain: ethereum blockchain based digital forensics chain of custody. *Sci. Pract. Cyber Secur. J.*
11. Huckle, S., Bhattacharya, R., White, M., & Beloff, N. (2016). Internet of things, blockchain and shared economy applications. *Procedia computer science*, 98, 461-466.
12. Halpin, H., &Piekarska, M. (2017, April). Introduction to Security and Privacy on the Blockchain. In 2017 *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 1-3). IEEE.
13. Tasatanattakool, P., &Techapanupreeda, C. (2018, January). Blockchain: Challenges and applications. In 2018 *International Conference on Information Networking (ICOIN)* (pp. 473-475). IEEE.
14. Flores, D. A., &Jhumka, A. (2017, August). Implementing Chain of Custody Requirements in Database Audit Records for Forensic Purposes. In 2017 IEEE Trustcom/BigDataSE/ICESS (pp. 675-682). IEEE.
15. Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., &Amaba, B. (2017, June). Blockchain technology innovations. In 2017 *IEEE Technology & Engineering Management Conference (TEMSCON)* (pp. 137-141). IEEE.
16. Dorri, A., Kanhere, S. S., Jurdak, R., &Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In 2017 *IEEE international conference on pervasive computing and communications workshops (PerCom workshops)* (pp. 618-623). IEEE.
17. Karame, G., & Capkun, S. (2018). Blockchain security and privacy. *IEEE Security & Privacy*, 16(4), 11-12.