Advantages of Blockchain in Digital Forensic Evidence Management

Yogita K Borse
Assistant Professor,
Information Technology Department,
K J Somaiya College of Engineering,
Somaiya Vidyavihar University,
Mumbai, India
yogitaborse@somaiya.edu

Deepti J Patole
Assistant Professor,
Information Technology Department,
K J Somaiya College of Engineering,
Somaiya Vidyavihar University,
Mumbai, India
deeptipatole@somaiya.edu

Gaurav Navnit Chawhan
Undergraduate Student,
Information Technology Department,
K J Somaiya College of Engineering,
Somaiya Vidyavihar University,
Mumbai, India
gaurav.chawhan@somaiya.edu

Geeta Jethanand Kukreja
Undergraduate Student,
Information Technology Department,
K J Somaiya College of Engineering,
Somaiya Vidyavihar University,
Mumbai, India
geeta.kukreja@somaiya.edu

Harsh Mukesh Parekh
Undergraduate Student,
Information Technology Department,
K J Somaiya College of Engineering,
Somaiya Vidyavihar University,
Mumbai, India
harsh.parekh@somaiya.edu

Rishabh Rajmal Jain
Undergraduate Student,
Information Technology Department,
K J Somaiya College of Engineering,
Somaiya Vidyavihar University,
Mumbai, India
rishabh28@somaiya.edu

***Abstract*— The importance of digital evidence has been accepted by the judiciary over the globe. The digital evidence plays a very crucial role in the judgment of the crime. The protection of integrity, authenticity, admissibility of such evidence should always be given highest priority. A log of digital evidence handling, which can be verified for any tampering, but does not allow any of the stakeholders to erase such traces of tampering is the need of today. This can guarantee a full proof maintenance of chain of custody for the digital evidence. Blockchain technology and using its core feature can make the process of a chain of custody(CoC) more efficient and reliable. This work proposes a hybrid blockchain solution for maintaining CoC(Chain of Custody), making the evidence and the transaction of the evidence transparent. The proposed system is designed to underline the advantages and allow the stakeholders of the system to view the evidence transaction during the complete legal process, but does not allow any sort of tampering of the same.**

Keywords—Hyperledger Composer, Private Blockchain (Permissioned), Chain of Custody, Evidence Integrity, Digital Forensics, Digital Evidence Management.

I. Introduction

One of the main issues of investigation of various cases, including digital evidence is the protection of such evidence throughout the process. The complete process consisting the police investigation to judgement by court of Law, is built on the pillar of evidence supporting the investigation process. The evidence once found gets into the hands of various authorities for its thorough forensic analysis and investigations. Therefore it is more important to protect the evidence in all the possible ways so that it does not get tampered and is admissible, authentic and reliable in the courtroom.

Digital forensic evidence is only considered to be acceptable in the judicial court if the evidence fulfills the following criteria, which include: complete, authentic, believable and reliable; moreover, the two main aspects for digital forensic evidence to be admissible in a judicial court. First, the legal aspect that is the authenticity of the evidence, how accurate it is and its completeness and second, the technical aspects are transparency of evidence, explainability and its chain of evidence, i.e. who all accessed the evidence before it has been considered in the courtroom. Digital evidence as compared to physical evidence is difficult to grip and store because of the characteristics like they are transmitted easily and are fragile, as well as they can get tampered very easily.

Chain of Custody is stated as the action of keeping the record of every transaction related to the digital forensic evidence and documenting the history of storing digital forensic evidence from the time of its creation. Chain of Custody is the step taken to validate how the evidence was found and preserved properly on its way to court. However, with the help of CoC of digital forensic evidence, the investigator can prove the evidence to be admissible in the court. It is also essential to prove that the evidence hasn't been changed during the procedure of investigation. Thus, it is essential to have a standard way of maintaining CoC, regardless of whether they have been used in the trial or disposed of later.

A. Requirements of a Chain of custody:

- Evidence Integrity:

Digital evidence is not changed, modified during its transmission. Digital evidence may come from different types of sources. That may include seized hard-drives from computers, e-mail boxes of the suspect in real-time, user chat logs, Internet-SP logs and records, digital directories, wireless devices, portable memory cards, cameras, etc. The process to maintain the integrity of the digital evidence is a very crucial task that digital forensic examiners have to consider. Vendors have given the help of many different tech solutions to extract this digital evidence and once this process is done then the digital evidence has been acquired, and protecting the digital integrity becomes the main concern for prosecutors, investigators, etc.

- Traceable:

The digital evidence is tracked starting from the time of its discovery and until it is disposed of. The reason for a criminal logical examination can be built up by either distinguishing the guilty party of a case or setting up a proof to fabricate a body of evidence against the wrongdoer. As the two circumstances are regular in the law requirement point of view, the capacity to follow the source to proof or the other way around is fundamental. Moreover, another impediment is the agreeableness of evidence that varies in every one of these circumstances. There is additionally an issue of starting

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

point ID and cross-referencing in the examination process. Subsequently, the discernibility data is imperative to keep away from the loss of choice and essential data in gathering and dissecting during the examination procedure.

- Authenticity:

The entities interacting with evidence must provide proof of their identity. For a physical archive, its legitimacy includes some characteristics, such as the condition of being devoted to a unique, uncorrupted and with a confirmed provenance. Although electronic proof has different attributes to paper, the standards of evidence that have been created regarding the verification of proof, especially narrative proof, are still profoundly relevant to electronic proof.

- Verifiability:

The procedure of maintaining CoC must be provable. Digital information is of two forms. It could be static, that is, it is stored on physical memories like hard drives, CDs and other memory storage devices. It may be dynamic, meaning the information may be moving on a particular medium, i.e. internet. For example, if a file has been shared over WhatsApp groups and other active members, it would be travelling from one to another network or device. In both cases, it is essential to preserve its verifiability if it is a part of an investigation. In an age where a lot of information is stored in the cloud storage, maintaining the verifiability of data for investigation purposes has become more challenging. It requires the active participation of the companies that are providing these cloud storage facilities.

- Need to maintain the evidence Tamper proof:

The digital evidence which undergoes through the phase of analysis should always be ensured about its integrity. The practice of performing analysis on a secondary copy which is verified for its integrity against the primary copy Hash value is followed by professional investigators. This prevents the evidence from any kind of tampering. Hence, record of every step of investigators across all the phases evidence life cycle plays vital role in proving Tamper proof nature of the digital Evidence in court of Law.

B. *Challenges in Chain of Custody:*

The world is encountering an extreme development in data and media transmission usage. Electronic frameworks are developing in multifaceted nature and assorted variety, getting inescapable, implanted and interconnected. Simultaneously, there is an extreme increment in the amount of data generated, scattered and streamed between servers, PCs, handhelds, cell phones, worldwide or individual systems, and any sort of cutting edge gadgets. Another issue is that the present examinations depend on computerized programming apparatuses. Therefore, the correctness of examination results is subject to the accuracy of such devices and their application procedure. Accordingly, the apparatuses utilized in an examination must be reviewed to guarantee that the instrument, strategies and techniques are reliable and capacity as proposed. The specialized sufficiency makes it increasingly hard to get secure and dependable outcomes through any scientific examination. Late examinations confirm the recognition that the existing pattern of digital proof is getting mind-boggling, and each stage expands the likelihood of a penetration that can damage the chain of care.

Improving Chain of Custody and computerized proof Integrity with timestamp: The uprightness of advanced proof assumes a significant job in the advanced procedure of criminological examination. Appropriate chain of guardianship must remember data for how evidence is gathered, shipped, examined, taken care of, and saved. There are a few adjusted techniques for proof advanced marking to prove the respectability of digital proof. Most scientific apparatuses and applications utilize a particular sort of hashing calculation to permit examiners later to confirm the circle or picture respectability. In this procedure, there is an issue of restricting uprightness, personality and date and time of access to digital proof.

As a result of the far-reaching improvement of ICT, particularly web and electronic correspondences, development of proof is a lot more prominent today than at any time in recent memory. As advanced evidence is in bit/byte structure, it is straightforward to move it to another side of the world in no time flat. One of the most significant things in the scientific procedure is the support of computerized proof chains of guardianship. Timestamps are accessible from the safe outsider (Time Stamp Authority) and are utilized to demonstrate when the staff gets to the proof in any phase of the measurable examination. Further research will be centered around the following issue of the chain of care where digital proof is handled, and by what means can a protected "Advanced Evidence Management Framework" be created. That pushes examiners to deal with proof securely, and store a hash of documents in a digitized structure, just as a biometric signature, time stamp, and attributes of spots from where all evidence was collected.

II. Literature Review

Digital Forensics initiates to begin and shows its roles and contribution as an answer in disclosure of crime to the society. The number of cybercrimes is on the rise in today's digital world [1]. Also, cybercrime urges digital evidence teams to acquire more precise evidence administration because the main aim of digital forensics is to find, investigate and preserve evidence. Linking individuals with their criminal activity makes digital proof a vital factor. Also, a highly maintained integrity of the digital forensic evidence plays an essential part in this entire procedure of their forensic investigation. From the recording of digital evidence and maintaining its integrity until presenting in court is the whole process of the chain of custody [2]. Presenting the un-manipulated and authenticated digital proof to the court of the law becomes the mandatory objective. It includes all the individual units involved in the entire process of acquisition, collecting of data, analysing the proof as well as contextual data, which consists of its labelling and the laboratory that offers evidence. The main aim is securing digital evidence and maintaining its integrity. Chain of custody paperwork is very much vital since it keeps the authenticity of the digital proof in the court of law [3]. It will provide authenticity and integrity of digital evidence so that it is acceptable in the court of law because the blockchain has the capability of secure transactions, providing access to only authorized users and other essential features. Digital Forensics would receive an untampered, secured and more reliable chain of custody based on blockchain.

One of the investigations showed a blockchain-based computerized crime scene investigation chain of custody that includes Proof of Concept (PoC). The Linux Foundation that hosted rapidly increasing projects is the Hyperledger Composer [4]. Hyperledger composer is the best option to develop blockchain-based apps instantly. It assists and lives on the uppermost part of an already existing hyper-ledger fabric blockchain framework and runtime. This permits for plug-type blockchain agreement rules to make sure that the transactions are approved as per given policy determined by the appointed member of the business network.

To handle digital proof, it raises many distinct challenges since the facts state that they are dormant, strained or uneasy, delicate and can cross authority borders very fast also easily. In most of the cases, it can be time-dependent too. To collect and change the authority of the evidence in a digital environment even in a legal process and the authenticated procedure is quite a tough challenge [5]. The practitioner getting principle evidence is regarded as precise by the court. If there is any disagreement or argument, then, more in detail investigation is initiated to find authenticity and integrity. For the acceptance of the digital evidence in the court of law, the investigator's name, the place where the crime took place and the hash value of that file are no longer enough. There are many more requirements like, all the people who had the authority to gain the evidence, correct identification of all the people involved in the forensic scene, the artifacts like the digital signature of every evidence found, the precise location of each object of the proof, etc.

The model proposed would fill in as spine for many criminological examinations maybe or for a review in the trail when all is said and done with the help of an association permitting to utilize a process model for examination.

Participants: To store transaction data in any net -work they are considered to be the actual actors. They generally represent business but have the capability of representing different persons, managers, directors or various shareholders. In the suggested model, part taker is the investigators and their job is to collect data and collect it to the maximum about the digital proof and then document it. Also at any point in the investigating scene all the requirements of the detailed evidence are needed in the chain of custody, so they also act as participants and then to integrity is maintained properly due to the blockchain. No unauthorized person is permitted to see the details of any specific evidence and to alter the condition of forensic chain [4].

Model Front-End: Its front-end can be made with assistance of two frameworks, that are composer rest server and the other is Yeoman and both are tied up with hyper - ledger composer.

Fundamental Modules: It eases to convey with a blockchain network. All the people like a prosecutor, defense known as participants keep and call a suitable fundamental module to recover the proof description..

Blockchain-Network: It mainly consists of two things, p2p net- work and Agreement rule.

Distributed Evidence Store: It consists of distributed storage with authorization and verification chunk to carefully lays in and preserve the actual proof.

A. *Types of Evidences in Real Time*

Digital evidence may come from different types of sources that may include seized hard-drives from computer, e-mail box of the suspect in real-time, user chat logs, Internet-SP logs and records, digital directories, wireless devices, portable memory cards, and cameras. The crucial task is the Digital forensic examiners have to consider the process to maintain the integrity of the digital evidence. Vendors have given help of many different tech solutions to extract this digital evidence and once this process is done then the digital evidence has been acquired, the main concern for prosecutors, investigators, etc has become to protect the digital integrity.

B. *Conventional procedure for collection of Evidence in Chain of Custody*

In the moment where the crime is occurred has come into picture the officer must take all the necessary steps to obtain maximum evidence and to secure it. He/she must work according to the guidelines provided. He must report the matter to the IPF, RPF and Sr. DSC about the matter with all the details available.

The IPF must nominate an officer and sent to the Place of Occurrence by the first means. The Sr. DSC concerned must satisfy himself of requirements of the cyber investigation officer and must report the same to the nearest Cyber Cell office and must gain assistance of the Cyber cell to retrieve the information in a secure manner. The Cyber Cell sends the Assistant Enquiry Officer (A.E.O) and he informs and authorizes the Enquiry Officer (E.O) and must gain the full picture of the offense. The procedure for the collection of evidence is as follows:

Pre-investigation assessment: The In-charge/Cyber cell (AEO) shall collect all the necessary information like profiles of the suspect, location of the crime, circumstances, circumstances and the computer system involved in the crime. The officer must proceed to the crime location with all the necessary tools and equipment required [7].

Evaluation of the Crime Scene: The digital evidences are very volatile in nature. Those could be available in a number of devices such as standard computer/storage devices, hubs, routers, dongles, copiers and fax machines can also have vital information relevant to the case. Hence, the crime scene should be carefully evaluated before the collection of evidences. The crime scenes could be broadly categorized as — (a) House of an individual/s having one or more computer/networks, (b) Office or shop of an individual/company and (c) A public place like- a Cyber Café. The pre-investigation assessments should be modified on the basis of evaluation of the crime scene. The evidence to be noted are: Number of computer systems present, no. of them having LAN or interact connections. Types of connections (Wi-Fi-Ethernet). Computer peripherals used personal appliances (like- hearing aids or spectacles etc.). Network topology and client-server architecture. CCTV/web camera clippings if any, user management software installed if any, log register maintained if any etc [7].

Collection of physical evidences: The physical evidences may include manuals/user guides or receipts of the cyber appliances, left behind diaries. Notes/passwords on slips, e-mail IDs. Contact numbers or bank account numbers etc. It is also important to note & sketch the position of the various equipment at the scene of crime. Collection of the Digital Evidences: This can be retrieved from forms of devices such as (a) A Switched Off System, (b) A Switched On System, (c) Cellphone System and other portable devices. This can be duplicated in various forms such as (a) Logical backup, (b) Bit Stream Imaging, (c) WriteBlocker. They must be secured by packing the physical devices, labeling and transporting the devices and get the concerned data from the agencies about the related data that helps in tracking.

TABLE I. ADVANTAGES OF BLOCKCHAIN BASED COC

Operations	**Conventional Chain of Custody**	**Blockchain based Chain of Custody**
Traceability	The origin of the evidence is hard to track if tampering is done in the intermediate document	No chance of tampering hence evidence can be tracked and easily
Integrity	Can be modified as it is manual and can be manipulated.	It's integrity is maintained as blocks in the chain cannot be manipulated in the blockchain technology.
Security	Hard to ensure security as it is physical and can be damaged by various means.	The blockchain is a Distributed technology and has distributed Storage and network it has ensures security in the network.
Authenticity	Since it is not 100% tamperproof it cannot assure the authenticity of the document.	It assures authenticity of the document as various miners into the system verified it.
Confidentiality	It cannot assure confidentiality as various people can access if hard copy is leaked publicly.	Only the authorized people can access the document and hence can be confidential in all forms.

The table I describes advantages of blockchain based system for maintaining chain of custody (CoC) over the conventional method. Blockchain technology has the properties which are essential in maintaining chain of custody of any piece of digital evidence. Thus the system requirements get fulfilled in the blockchain based system than that of conventional system. The evidence can be presented in court of law by having complete traceability of the investigation and transfer process carried over the piece of evidence under trial. The ability of the conventional system to prove authenticity of any digital evidence is built on trustworthiness of the stakeholders involved, whereas blockchain technology follows a trustless model. The human factor plays a crucial role in claiming authenticity of evidence in conventional method. The Blockchain based method is based on the transactions occurring on the Digital evidence. Each and every transaction gets logged in a distributed ledger and this entry is permanent, thus removing the need for reliance on trustworthiness of stakeholders involved. This can help in complete admissible and traceable presentation of Digital evidence.

III. PROPOSED SYSTEM

The process of forensic investigation is done in a controlled environment and the assets in our case "Digital Evidences" are to be protected from corruption with the doubtful participants. Hyper ledger Composer from its basic structure model gives all required means to build a robust and secure system that would help in recording necessary details of the digital evidence for a particular case. The given model explained further will help to serve as a secured investigation process for cases related to an organization's investigation of digital forensics. Forensic-Chain architecture has five main components that include:

1) Users:

Users are meant to be the actors of the system and help to store the information that flows into the system. In the proposed model, they are the Criminological Analyst whose task is to assemble data about the computerized proof and document it on the blockchain. Investigator, Defense, and Magistrate additionally go about as members because they need insights regarding the CoC for the keep criminal offense anytime in the criminological inspection. Just approved members are permitted to see the subtleties of the specific proof.

2) Front-End:

Yeoman framework and composer-rest-server helps to develop the front-end into the system.

3) Source Code:

Encourages the correspondence with Blockchain System. Members accumulate and call a proper centre function to recover the proof subtleties from the Forensic-Chain.

4) Backend Network:

It contains a Peer-to-Peer system and Consensus convention that administers the correspondence over Peer-to-peer organizations.

5) Distributed Evidence_Store:

It has distributed storage with approval and confirmation module for securely storing and protecting the first proof.

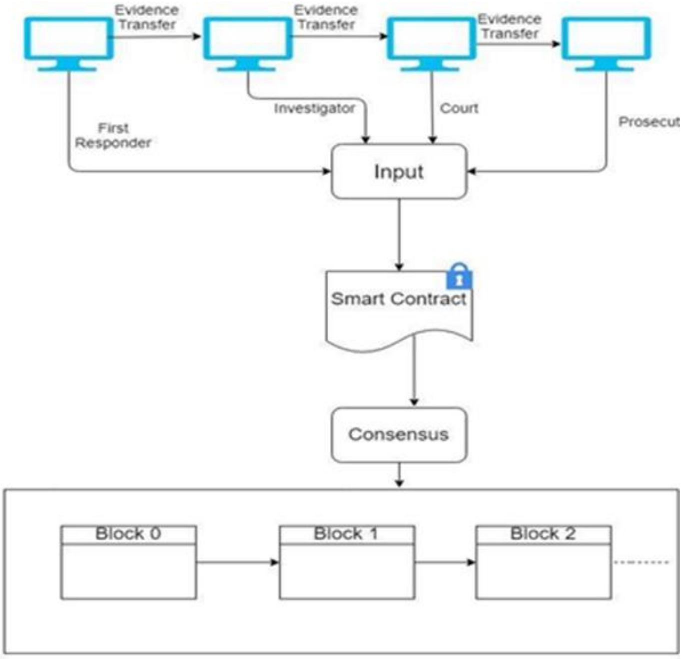

Fig. 1 : Digital Forensic Investigation

Fig. 1 demonstrates the simplified architecture of proposed model. Once the evidence is created, it may be transferred to many entities such as the investigating officer, the court or the prosecutor, but a smart contract is created so that no tampering of the evidence can take place. A smart contract takes the inputs from all the entities as evidence and it is created based upon the consensus, in which some protocols are defined. It is then registered into the forensic chain and assigned to the blocks. Each block consists of one transaction of specific evidence.

We first defined the advanced proof as an information structure as:

Evid_ID: Particularly classifies the automated proof of computerized proof and other associated data.

Initiator: Users who fill in the digital testimony into the block at the initial phase.

Current Evidence Holder: User with Evidence in proprietorship.

Evid_Description: Includes the basic ascribes identified with computerized proof.

Case_ID: This entity helps us to identify the case with a unique entity. This helps to categorize the evidence with similar cases. All the evidence belonging to a similar case will have common case id and different evidence id. Every occasion of a chain code/smart agreement speaks to an alternate case.

Transfer_Chain: A cluster consisting of the address of members who have been the proprietor of computerized proof during its life cycle.

Transfer_Time: A Cluster Containing date and time of proof exchanges.

The model includes essential capacities for making, moving and showing the proof data from the blockchain. The imperatives like people who should be assigned what task and under what circumstances the access must be allowed to members are all described in get to control manages in authorizations. Acknowledge document of model in Hyperledger Composer. The pseudo-code of the capacities is introduced underneath as calculations.

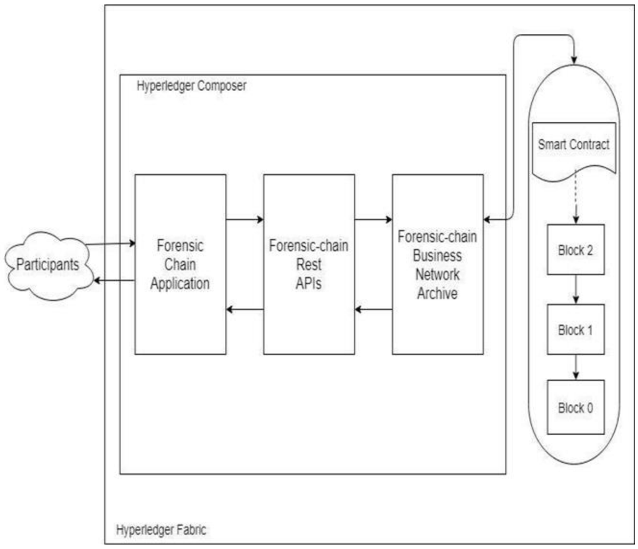

Fig. 2 : Proposed Model

The fig. 2 is a representation of proposed model and demonstrates how entities will be working in specified technology's environment. Participants connect and interact with the forensic chain as shown in the figure 2 below using an application that is created and generated. The data is shared through the specified channels of Hyperledger fiber/composer. Smart contracts are further used to automate access tracking and to also perform validating operations on inputs and tasks specified.

1) Evidence Creation:

It is a function that takes two inputs and then presents the newly created evidence to the forensic chain. It's two inputs consist of evidence ID and evidence description. Based upon its evidence creation function it generates an ID which is produced by calculating the hashed value of the evidence created digitally, subsequently, it is easy to maintain its trustworthiness of evidence digitally all through the life cycle. Many different properties are also set to participant identity who made it in the initial clock, attributes like creator and owner. The participant ID is then forwarded to the transfer chain, thereby demonstrating it, is the maker as well as the initial owner of that evidence that was digitally created. Note, the function of evidence creation then firstly confirms that the evidence with similar identity ever exists or not, if so, it then provides without making a copy of the evidence.

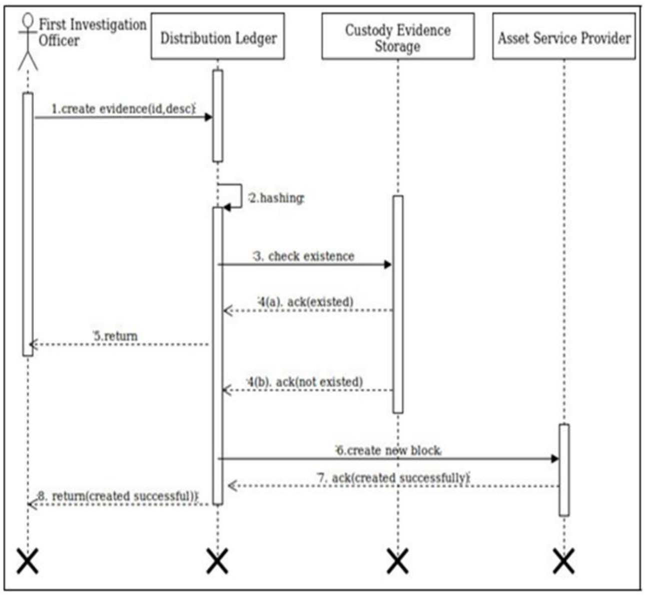

Fig. 3 : Create Evidence

In fig. 3, it is explained that how the creation of the evidence takes place, initially the function takes two inputs and then produces the newly created evidence. It's two inputs are evidence ID, and its description. It then creates the hashed value of the evidence. Further it is checked for the evidence existence and if it already exists then the evidence is not taken into consideration; otherwise a new block is created for the evidence and the registered into the forensic chain.

2) Evidence Transfer:

It is a function which provides transfer of ownership to the address provided or as stated. This function consists of two inputs as same as evidence creation, but this includes evidence identity and address as the two inputs and then, in turn, it provides the possession transfer as stated in the address. Before transferring the ownership it first checks whether the evidence ever existed and the one conjures the function is the one who has the possession of the evidence or not. If the one who has the possession of the evidence is found to be correct, then it sets the evidence of the already possessed person to the new person who takes the possession. It additionally brings another person which can have the possession to the transfer chain array and present time to transfer time array in this way keeping up the auditable chain relating to evidence transfer or confirmation of the move.

In fig. 4, the evidence transfer process is explained in which the function takes two inputs which are evidence Id and the address. Initially it is checked whether the evidence Id exists or not, and if it exists then also to check the ownership of the evidence. If it is found to be correct then the evidence ownership is transferred to a new owner mentioned in the address and the same is noted in the forensic chain.

3) *Evidence Display:*

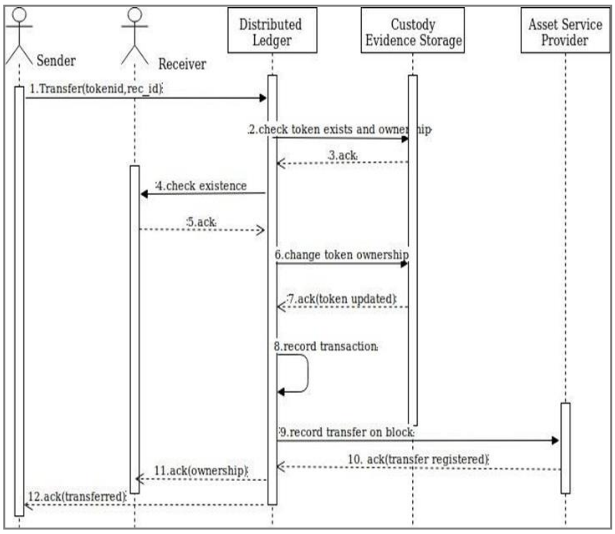

Fig. 4: Transfer Evidence

The Method for Evidence display requires Evidence ID for returning corresponding Evidence Information. The only validation for this method is to verify the existence of the given evidence input. The upper level of Hyperledger Composer that runs in a reserved and supervised environment, acts as a base for the Proposed Forensic-Chain model. In this way data about the proof is just kept to the members who are a piece of the blockchain i.e participants of blockchain, approved by administrator peers claimed by consortium's associations. In fig. 5, the evidence display is explained in which the function takes a single input as the evidence Id, it initially checks whether the evidence exists or not, if it does exists then the evidence details are successfully displayed and if there is no such evidence then it simply denies.

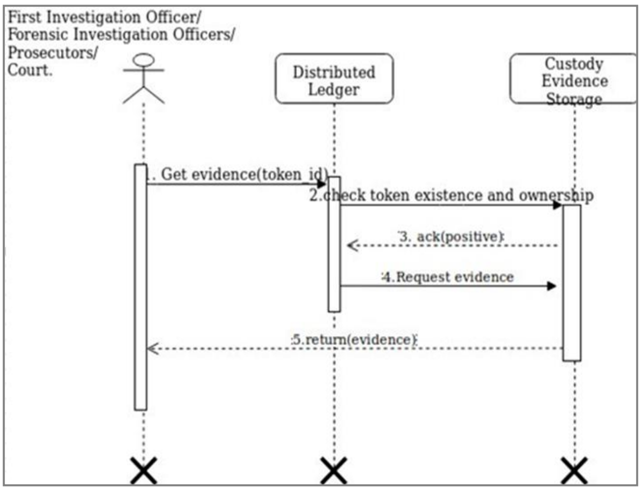
First Investigation Officer/
Forensic Investigation Officers/
Prosecutors/
Court.
Distributed Ledger
Custody Evidence Storage
1. Get evidence(token_id)
2.check token existence and ownership
3. ack(positive)
4.Request evidence
5.return(evidence)

Fig. 5: Get Evidence

Hyperledger Composer settles on its progressively appropriate decision for mimicking the elements of existing criminal judiciary systems. The channels in Hyperledger fabric/composer assist participants to share data secretly.

IV. CONCLUSION

The field of Digital Forensic is extending and there is a vast difference in management of Digital Evidences as compared to Physical Evidence management, traditionally presented in the Court of Law. Blockchain Technology has the potential to provide the features crucial in digital evidence management. Blockchain can be configured to provide authority, authenticity, integrity, transparency, auditability, and security. Therefore, Blockchain Technology has the advantage for keeping up, maintaining and following the forensic and scientific chain of custody over conventional methods. There is a great chance of decrease in conflict through expanded trust with blockchain and blockchain surely brings a genuine guarantee for the Forensic Network and Community in this manner. Hence, to avoid the manual errors to affect the admissibility of digital evidence in court of law, blockchain technology can be considered as a viable solution to maintain chain of custody of digital evidence.

REFERENCES

[1] Jasmin OSI and Miroslav Baa,‘ImProving Chain of Custody and Digital Evidence Integrity with Time Stamp', IT Section of Police Administration, Faculty of Organization and Informatics,502.V.bbr br.2, Bihac, BH

[2] Matthew N.O. Sadiku1, Adebowale E. Shadare, and Sarhan M. Musa: 'Digital Chain of Custody,' International Journals of Advanced Research in Computer Science and Software Engineering ISSN: 2277-128X (Volume-7, Issue-7), July 2017, Department of Electrical Computer Engg., Prairie View AM University, Prairie View, TX 77446, United States

[3] Claudio Ciccotelli Marco Casini and Silvia Bonomi,‘B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics', Research Center of Cyber Intelligence and Information Security,26 July 2017, Department of Computer, Control, and Management Engineering "A. Ruberti", Sapienza Universit' a di Roma, Via Ariosto 25, 00185 Roma, Italy

[4] Auqib Hamid Lone, Roohie NaazMir,‘Forensic-chain: Blockchain-based digital forensics chain of custody with PoC in Hyperledger Composer,' A.H. Lone, R.N. Mir / Digital Investigation 28 (2019) 44-55, January 2019, Department of Computer Science and Engineering, NIT Srinagar, Jammu and Kashmir, 190006, pp. 44-55.

[5] Asaf Varol and Yesim Ulgen Sonmez, 'Review of evidence analysis and Reporting phases in Digital Forensics process,' 2nd International

Conference on Computer Science and Engineering, 2017, Firat University, Faculty of Technology, Turkey.

[6] Standard Operating Procedure for Collection of digital evidences and cyber investigation techniques by S.K. Dubey, DIG/Proj./RPF &H.S.Papola,ASC/RPF,New Delhi.

[7] Auqib Hamid Lone and RoohieNaaz Mir, 'Forensic-Chain: Ethereum Blockchain based Digital Forensics Chain of Custody,' Scientific and Practical Cyber Security Journal, 2017, Department of Computer Science and Engineering NIT Srinagar, Jammu and Kashmir 190006, pp 21-27.

[8] Makhdoom Syed Muhammad Baqir Shah, Shahzad Saleem, and RohaZulqarnain,‘Protecting Digital Evidence Integrity and Preserving Chain of Custody,' Journal of Digital Forensics, Security and Law, vol. 12, no. 2, 2017, pp. 121-129

[9] Rafael Misoczki, Fernando MagnoQuinto Pereira, 'The computer for the 21st century: present security privacy challenges,' Journal of Internet Services and Applications, August 2018.

[10] Reza Montasari, 'A standardized data acquisition process model for digital forensic investigations ,' Int. J. Information and Computer Security, Vol. 9, No. 3, 2017, University of Derby, NL pp 229-249.

[11] Giuliano Giova,‘Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems', IJCSNS International Journal of Computer Science and Network Security, VOL. 11 No. 1, January 2011

[12] Gregory Epiphaniou,Haider Al-Khateeb, , and Herbert Daly, 'Blockchain for Modern Digital Forensics: The Chain-of-Custody as a Distributed Ledger,' Advanced Sciences and Technologies for Security Applications, 2019, University of Wolverhampton, Wolverhampton, UK, pp 149-167.

[13] M. Chopade, S. Khan, U. Shaikh and R. Pawar, "Digital Forensics: Maintaining Chain of Custody Using Blockchain," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2019, pp. 744-747, doi: 10.1109/I-SMAC47947.2019.9032693.