JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Blockchain-Enhanced Digital Forensics: Strengthening the Chain of Custody

BibiJainab Pathan , Najama Nadaf , Sachin Desai
MCA student, MCA student, Assistant Professor
Department of MCA,
K. L. S. GogteInstitute of Technology,Belagavi, Affiliated toVisvesvaraya Technological University,Belagavi, Karnataka, India

Abstract : Digital forensics entails the systematic application of scientific methods to preserve, collect, validate, identify, analyze, interpret, document, and present digital evidence. Effective management of digital evidence, crucial for linking individuals to criminal activities, faces significant challenges such as tampering risks and documentation errors during its transfer from initial investigators to judicial authorities. Traditional Chain of Custody (CoC) methods, typically involving paper or electronic forms, are insufficient to address these challenges due to their vulnerability to tampering and inconsistencies.

This paper proposes a Blockchain-based Chain of Custody (B-CoC) framework to enhance the security, transparency, and integrity of digital evidence management. Leveraging the inherent properties of blockchain technology, such as immutability, distributed ledger, and consensus mechanisms, the B-CoC framework provides a robust solution for maintaining the CoC in digital forensics.

The architecture is constructed upon a private, permissioned blockchain leveraging Ethereum and a Proof of Authority (PoA) consensus mechanism, thereby restricting participation to authorized nodes.
Smart contracts automate critical operations, including evidence entry creation, ownership transfer, and information retrieval, enhancing the security and traceability of digital evidence. This system logs all interactions immutably, providing a clear and tamper-proof chain of custody.

Key benefits of the B-CoC framework include increased security, transparency, and accountability in digital evidence management, potentially reducing costs and improving efficiency.

In conclusion, the B-CoC framework represents a significant advancement in managing digital evidence, ensuring its integrity and reliability, and thereby strengthening trust in legal proceedings and forensic investigations.

IndexTerms - Digital Forensics, Chain of Custody(COC), Blockchain, Blockchain based Chain of Custody(B-COC), Evidence Management, Ethereum, Private Blockchain, Smart Contracts, Proof of Authority.

I. INTRODUCTION

Digital forensics is essential in today's era of exponential digital data growth, involving the meticulous collection, preservation, analysis, and presentation of digital evidence for legal purposes . Central to ensuring the integrity and admissibility of digital evidence is the Chain of Custody (CoC), documenting its chronological handling from collection to courtroom [1].

Traditional methods of maintaining the CoC, which typically involve paper logs or electronic forms, are prone to human error, tampering, and unauthorized access.
These weaknesses can compromise the dependability of digital evidence within legal contexts. Consequently, there is a significant need for innovative solutions that enhance security and verifiability [1].

Blockchain technology, initially developed for cryptocurrencies, offers a decentralized and tamper-resistant method for recording transactions [2]. By leveraging the immutable ledger, cryptographic security, and decentralized consensus mechanisms inherent to blockchain technology, this paper proposes a Blockchain-based Chain of Custody (B-CoC) framework [8].

This B-CoC framework is designed to operate on a private, permissioned blockchain like Ethereum, utilizing a Proof of Authority (PoA) consensus mechanism. Smart contracts are employed to automate CoC processes, ensuring that access to the evidence is restricted to authorized personnel and maintaining a transparent, tamper-proof record of all evidence interactions [9].

By enhancing the security, transparency, and accountability of digital evidence management, the B-CoC framework seeks to increase trust in legal proceedings and forensic investigations [8][6]. This paper delves into the implementation and advantages of the B-CoC framework, underscoring its potential to revolutionize the management and presentation of digital evidence in legal contexts [8].”

.

II. BACKGROUND STUDY

1] Blockchain

Blockchain is a distributed ledger that has a continuously expanding list of records Blockchain technology[2], initially introduced in 2008 as part of the Bitcoin cryptocurrency system by Nakamoto, has since emerged as a disruptive force in various sectors. It offers the promise of secure and decentralized transactions, as noted by Olnes et al. (2017) and Yli Huumoetal. (2016). Functioning as a peer-to-peer distributed ledger system, Blockchain ensures robust security through public key cryptography and hashing techniques in transactions, as outlined by Drescher (2017). The term "Block" denotes the storage unit, while "Chain" signifies the link connecting these data blocks.[3]

The core components of Blockchain include:

1. **Transactions**: These involve the exchange of data, currency, or information between two nodes on the Blockchain. Transactions undergo eligibility checks before being accepted or rejected, utilizing Public Key Cryptography for non-repudiation and traceability.

2. **Block:** A block comprises valid transactions hashed together to form a unique block hash. Each block is linked to the next using this hash, ensuring the integrity of the chain. Any attempt to manipulate block data is evident in the chain due to this interconnectedness.

3. **Nodes or Participants:** These are stakeholders in the Blockchain ecosystem, operating within a trustless environment enabled by Blockchain mechanisms. Nodes may be incentivized or subject to penalties for their actions, contributing to the decentralized nature of Blockchain.

4. **Smart Contracts**: These are self-executing contracts encoded with predefined conditions, automating agreements across various domains.

5. **Consensus Mechanism:** This mechanism determines critical decision-making points within the Blockchain system, such as transaction validation and block creation, ensuring agreement among participants.

2] COC

The Chain of Custody (CoC) is the systematic documentation that monitors the custody, control, transfer, analysis, and storage of physical or electronic evidence.Chain of Custody (CoC) encompasses essential stages throughout an investigation and the procedure for presenting evidence in court. Each individual responsible for handling the evidence bears accountability for its integrity and security.Any indication of tampering can render the evidence inadmissible in court. The techniques for collecting evidence involve preservation, packaging, transportation, storage, and creating an inventory list to establish the CoC. This includes documenting the location and time of data recovery, item descriptions, conditions, and any unique markings or alterations.[4]

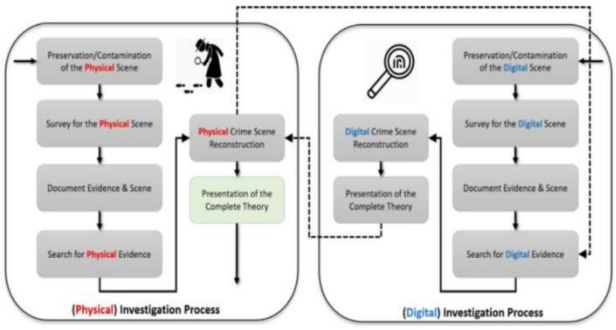

fig.1.Physical and digital investigation constructs

3] Issues encountered in maintaining the Chain of Custody

1. The growing volume of data reduces the flexibility and capability of documentation.
2. Utilizing digital evidence and records to establish the Chain of Custody (CoC).
3. CoC documentation must account for evidence transferring between different parties.
4. When presenting information to a judge and jury, it is crucial to make it comprehensible to both the judiciary and law enforcement agencies.
5. CoC should provide two types of information:

1.Details directly related to the case.

2.Information about the evidence's source, authenticity, and the process by which it was obtained.

4] Ethereum Blockchain

Ethereum is a significant application of blockchain technology. In addition to being a well-known cryptocurrency, Ethereum supports cross-platform deployment, making the use of blockchain more versatile and widespread.[9]

5] Smart Contract

A smart contract is an advanced application on the Ethereum blockchain that encodes business logic. It logs transaction details and participant agreements, executing actions automatically when specific conditions are met. In essence, a smart contract serves as a "mechanism involving digital assets and participants," allowing parties to invest and redistribute assets. These transactions are verified by network nodes, ensuring the contract's integrity [12].

III. UNDERSTANDING CoC AND B-CoC

1. Traditional CoC Approach

The chain of custody (CoC) involves managing and preserving digital evidence from its initial collection to its presentation in court. In current systems, evidence passes through multiple authorities, increasing the risk of tampering.Traditionally, CoC details are recorded using paper or electronic forms. These forms usually include investigator names, evidence descriptions, and a hash code for verification[5]. Modern forensic forms include digital evidence submission forms, chain of custody logs, and electronic evidence transfer records. Forensic software enhances this process by providing detailed evidence descriptions, electronic user identification, digital signatures, and automated audit trails. However, there is still a significant gap between the capabilities of current CoC software and the specific needs of the judicial system. This gap affects various stakeholders, including first responders, court officers, police, forensic investigators, expert witnesses, prosecutors, and defendants [7].

1.1 Maintaining chain of custody

A. Lifecycle of Digital Evidence

The chain of custody involves detailed documentation and maintenance of evidence throughout the investigation process. It begins with evidence collection at the crime scene, followed by its transfer to the investigation unit. The initial responder then hands the evidence to the forensic investigator for analysis. The analyzed data is subsequently transferred to the prosecutor for court presentation. The defense team may also review this data. Finally, the evidence is presented in court for judicial proceedings.

B. Security Concerns in Chain of Custody

Digital evidence plays a vital role in the investigation and judicial processes. However, a significant challenge arises from security vulnerabilities in handling such evidence. Documentation and recording of interactions with evidence present a key issue within the Chain of Custody. Moreover, when multiple parties are involved in utilizing the evidence, there's an inherent risk of tampering. In legal proceedings, detailed and accurate logs are essential to support the investigation process. Maintaining the integrity of data stands as a major challenge within the Chain of Custody, ensuring that digital evidence remains complete and untampered. Verifying that parties interacting with and modifying evidence are authorized poses another significant issue.

C. Digital Evidence Framework

In the current system, digital evidence is often deemed unreliable by the court unless empirical testing validates the techniques used in its production. Documentation, including paperwork, is crucial for identifying various aspects of digital evidence.
When evidence is transferred between entities, detailed information about both the entity and the evidence is recorded on a document. This document is later appended to the investigation's chart-sheet. However, there is currently no standardized approach for acquiring evidence or tracing its current owner. Establishing a standard process for data acquisition and owner tracing would enhance the court's ability to assess the reliability of digital evidence.

D. Ingenuity of Evidence

The authenticity of evidence is upheld through its storage among all participants in the network. Instead of transmitting the actual data through the chain, only a hash value of the evidence is passed.

2. B-CoC Approach

So the B-COC which is Blockchain based chain of custody provide a proper solution to it, By using the features of Blockchain like immutability ,distributed ledger, concences and smart contracts ,we can maintain chain of custody in more secure and in untemperable way

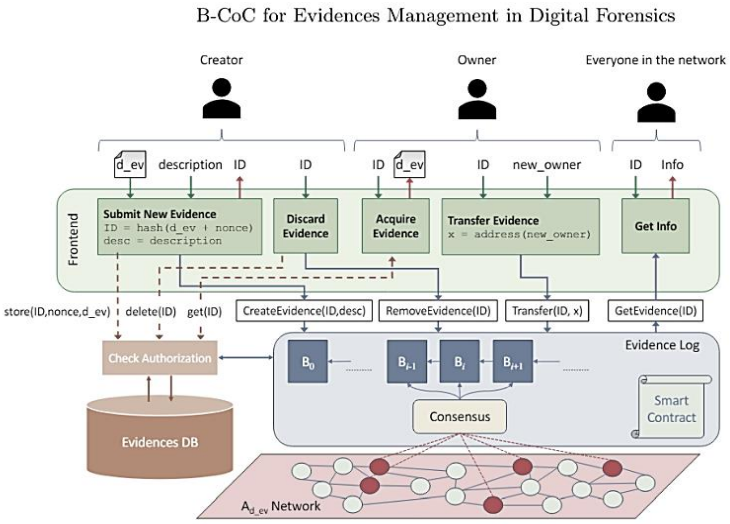

fig.3. B-COC Architecture [8]

2.1 B-COC Architecture

The Blockchain-based Chain of Custody (B-CoC) framework employs a private, permissioned blockchain to safeguard the security and integrity of digital evidence. This architecture ensures that only authorized and trusted parties can access and manage the evidence [8]. The system provides two distinct types of access: Automated access and Subsequent accesses, which will be elaborated on later in this paper [9].

As depicted in Figure 3, the B-CoC framework is comprised of three main components: **(i) the Evidence Database (Evidence DB), (ii) the Evidence Log, and (iii) the Frontend Interface**. The Evidence DB acts as a conventional database or file repository for storing digital evidence, whereas the Evidence Log, leveraging blockchain technology, records data related to the Chain of Custody (CoC). This distinction is crucial because evidence files are often too large to be stored directly on the blockchain and must be accessible only to authorized nodes [8].

A) Evidence DB: This component is a standard database or file repository designed to store original digital evidence. Each piece of evidence is assigned a unique identifier (ID), generated from a hash of the evidence combined with a nonce to ensure its uniqueness. Managed by trusted entities, access to this database is strictly controlled and limited to authorized personnel [8].

B) Evidence Log: Utilizing blockchain technology, the Evidence Log maintains records of the ID, description, submitter's identity (creator), and the chronological history of ownership changes for each piece of evidence. Although the actual evidence is not stored on the blockchain, the ID maintains the evidence's integrity through a robust cryptographic hash function. This log operates on a peer-to-peer network composed of authorized nodes, categorized into validator nodes and lightweight nodes. Validator nodes are responsible for storing the blockchain copy, validating transactions, and managing the blocks, while lightweight nodes generate transactions and rely on validators for validation [8].

The Evidence Log runs a smart contract that facilitates four operations:

1. **Create Evidence (ID, description):** Adds a new evidence entry with the specified ID and description, registering the submitter as the creator and current owner.
2. **Transfer (ID, new owner):** Transfers evidence ownership, recording the handover; fails if the issuer is not the current owner.
3. **Remove Evidence (ID):** Deletes an evidence entry; fails if the issuer is not the creator.
4. **Get Evidence (ID):** Retrieves information about the evidence, including ID, description, creator, and ownership history.

Evidence Log Implementation

The Evidence Log is a fundamental component of the Blockchain-based Chain of Custody (B-CoC) system, crucial for securely recording and managing digital evidence in forensic investigations. It meticulously documents evidence creation, ownership transfers, and deletions, ensuring transparency throughout the process. Implemented on a private blockchain network, it utilizes Geth, an Ethereum node implementation, enabling customization of consensus protocols and network configurations. The system operates on a Proof of Authority (PoA) consensus, specifically the IBFT protocol, ensuring reliability and integrity. Initialization of the private blockchain, network creation, and deployment of smart contracts are essential steps in its implementation, ensuring effective management of the Chain of Custody process.[8]

C) Frontend Interface: The frontend interface links users to the B-CoC system. Each node hosts a local instance of the frontend, facilitating interaction with both the Evidence DB and the Evidence Log. When authorized users upload new digital evidence, the frontend generates a unique identifier (ID) using a nonce. It then stores the evidence in the Evidence DB and triggers a Create Evidence transaction. The user who uploads the evidence is registered as its initial owner. Through the frontend, users can initiate operations such as evidence submission, ownership transfer, or deletion. These operations are authenticated by the frontend before updating the system records accordingly [8].

2.2 Workflow of B-CoC:

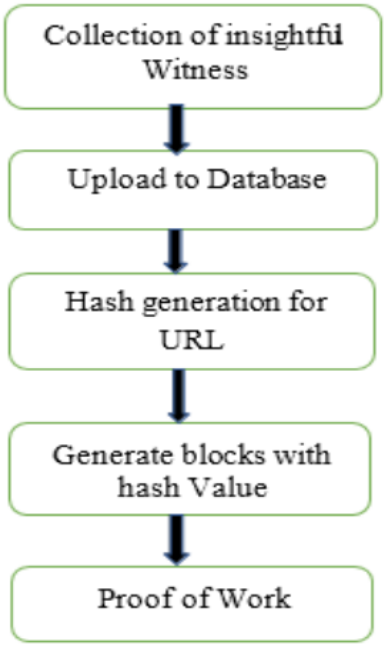

fig.4. Flow idea of B-coc [1]

Steps To Understand Workflow of B-CoC:

To ensure the Chain of Custody (CoC) remains as authentic as possible, the following steps must be undertaken [1]:

Step 1: Digital evidence is gathered from the crime scene or investigation site, comprising various types such as DNA analysis results, videos, audio recordings, text documents, images, or system logs. Each piece of evidence is assigned a timestamp to establish a chronological sequence.

Step 2: The collected evidence is then uploaded to a database that maintains detailed case information. A unique URL is generated for each uploaded item, which is subsequently used in the blockchain hashing process.

Step 3: The generated URL undergoes hashing as a string alongside its timestamp using a hash algorithm. This process produces a hash value that is stored within a blockchain block, thereby ensuring the evidence's integrity.

Step 4: A block is formed containing the timestamp, marking when the evidence was uploaded onto the blockchain. Any modification to the evidence would alter the timestamp, thereby disrupting the chain. A consistent chain confirms the block's integrity and unchanged state.

Step 5: Proof of Work (PoW) is employed to detect evidence tampering. This involves recalculating hashes of existing blocks and comparing them with current data to maintain coherence. Any disparity would signal potential tampering, preserving the integrity of the evidence chain.

2.3 An Application Oriented B-CoC

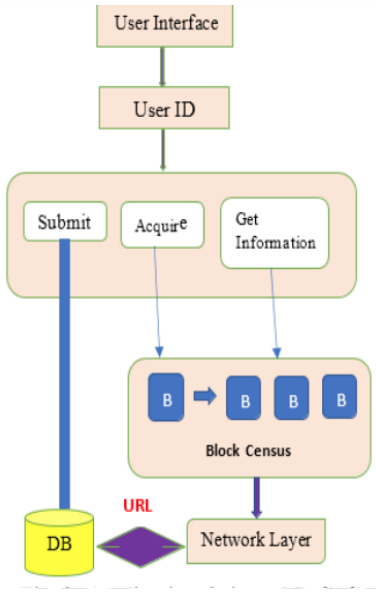

fig.5. Application Oriented B-coc [1]

Blockchain technology enables the robust implementation of Chain of Custody (CoC).. Upon block creation, it includes a hashed value, timestamp, and previous hash value, enabling seamless tracking of each block. This approach ensures accessibility, allowing anyone to view the details. It meets all CoC requirements by providing integrity and authenticity, assigning a user ID for database access, and securing the block through mining to prevent tampering. The suggested application leverages blockchain effectively to create a reliable and tamper-resistant chain of custody.. Figure 5 illustrates the operation of the Android application [1].

2.4 System Model For Digital Evidence Management in Forensic Investigations

A. Chain of Custody Model

The Chain of Custody (CoC) ensures the integrity of digital evidence from collection to court. Authorized entities (Ad_ev) like law enforcement and judges handle the evidence, each identified uniquely. Digital evidence (d_ev) has one owner at a time. Ownership transfers are formally requested, validated, and logged to maintain transparency and accountability.

B. Network Model

The efficacy of digital evidence management hinges on a robust network model that facilitates seamless communication and collaboration among authorized entities while safeguarding against unauthorized access and tampering. Within this model, each authorized entity is represented as a distinct process equipped with private-public key pairs for authentication and message signing.

Operating within a peer-to-peer network characterized by authenticated perfect links, these processes form the backbone of the digital evidence management ecosystem. Despite the inherent trust vested in authorized entities, the network architecture accommodates fault tolerance by tolerating up to a certain number of compromised entities, ensuring continuity and reliability in the face of adversarial scenarios.

2.5 Integration With B-COC:

The system model described here lays the groundwork for the adoption and integration of Blockchain-based Chain of Custody (B-CoC) solutions in forensic investigations. By aligning traditional CoC principles with the decentralized and immutable nature of blockchain technology, the integrity and accountability of digital evidence management can be further fortified, ushering in a new era of transparency and trust in legal proceedings [8].

IV. USING ETHEREUM BLOCKCHAIN FOR COC:

Ethereum is a Blockchain, featuring a built-in Turing-complete programming language, enables users to develop smart contracts and decentralized applications, setting their own arbitrary rules for ownership, transaction formats, and state transition functions [9].

By design, blockchain ensures transparency, authenticity, security, and auditability, making it highly suitable for maintaining and tracking the chain of custody in forensic applications.

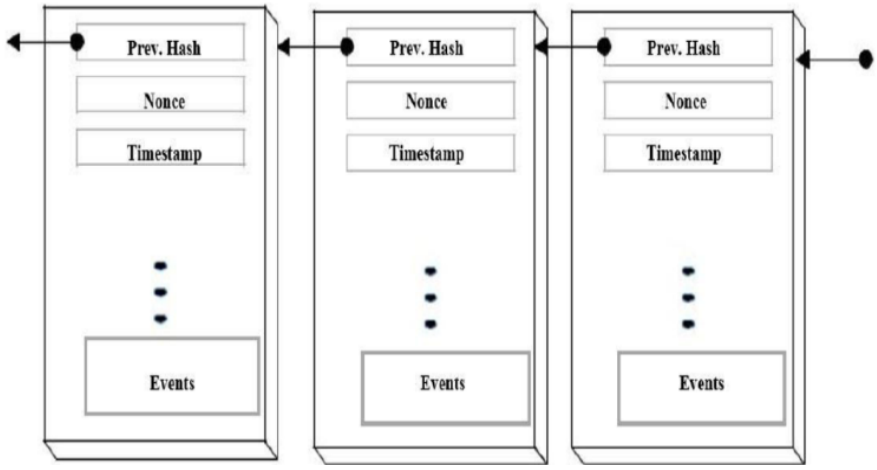

fig. 6. Blockchain and state[9]

1. Actual Implementation is as follows:

The initial implementation involves the blockchain's genesis block, which contains the initial hash of the data, including details such as the time, date, and location of the original acquisition.

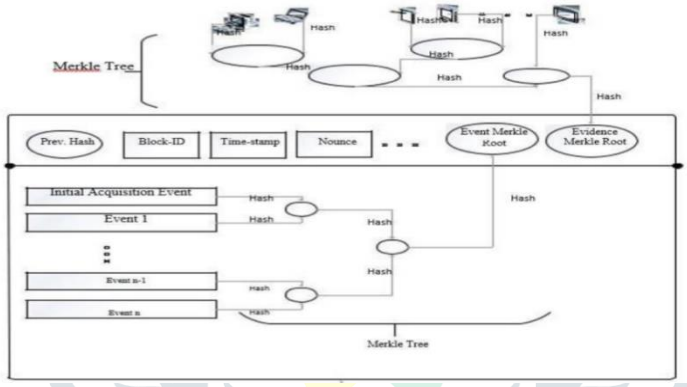

fig.7. Actual Implementation[9]

Provides two types of access namely:

A. Subsequent Accesses : This procedure is enabled by a specialized application, similar to those used for interpreting bitcoin blockchains, which creates new blockchain entries each time evidence is accessed or transferred. In simpler terms, whenever critical information is interacted with during subsequent accesses to the evidence, a new, non-repudiable, irreversible, cryptographically secure block is appended to the blockchain-based chain of custody[9], as depicted in the figure below.

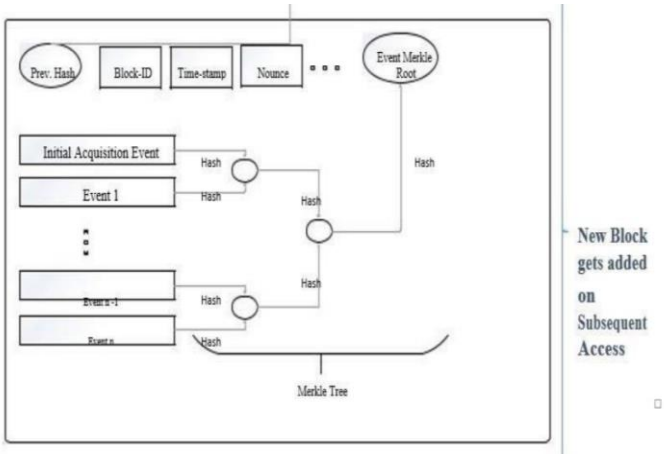

fig.8. Subsequent Accesses[9]

B. Automated Access: Automated access tracking via smart contracts will assist in identifying when evidence copies are being created and will document these actions in the blockchain. However, authorized copies or other routine record-keeping activities will be specifically logged into the blockchain-based chain of custody.

2. Benefits of Using Ethereum Blockchain:

The Forensic-Chain model offers significant advantages to forensic applications, enhancing the processes of evidence collection, preservation, and validation:[9]

1. **Strengthening Evidence Handling:** The utilization of Forensic-Chain enhances the collection, preservation, and validation of evidence, fortifying the integrity of forensic procedures.

2. **Traceability of Events**: Forensic-Chain enables the tracing of events or actions back to their origins within the investigative process, ensuring accountability and reliability.

3. **Enhanced Efficiency and Cost Reduction:** By increasing transparency and eliminating the need for trusted third parties in certain transactions, Forensic-Chain improves transactional efficiency and reduces associated costs, fostering consensus through a Proof of Trust mechanism.

4. **Fraud Mitigation:** The transparent audit trail provided by Forensic-Chain reduces the occurrence of fraud, bolstering the reliability and authenticity of forensic data.

5. **Embedded Verification:** Organizations can embed verification mechanisms directly within the evidence record, facilitating continuous access and verification of evidence authenticity.

6. **Accessible and Verifiable Evidence:** Forensic-Chain establishes a framework for ongoing evidence accessibility and verifiability, ensuring the reliability of forensic findings.

3. FORENSICS CHAIN IN ACTION

Forensic-Chain is activated by the First Responder, who takes a hash of the digital evidence and securely records it on the blockchain using a smart contract. Additional details such as location, time, and date of the crime scene are also logged on the blockchain. During the digital forensics investigation, any transfer of evidence is automatically recorded on the blockchain through smart contracts, including details like the recipient's address, the current state of the evidence, permission levels, date, and time. Moreover, subsequent access to digital evidence is securely logged on the blockchain through smart contracts activated by the respective forensic investigator[9].This process establishes a chain of trust by documenting every action related to the digital evidence.

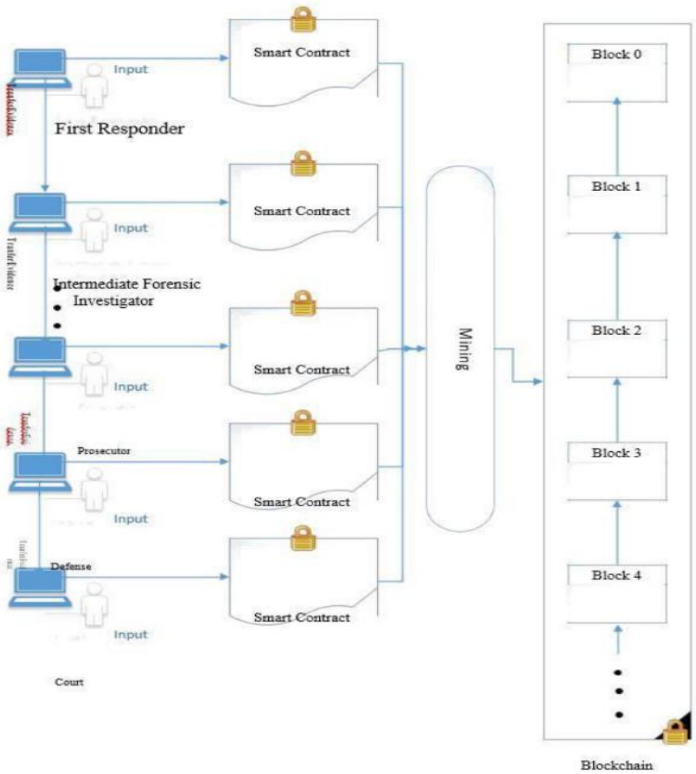

fig.8. Forensics chain in action[9]

V. CONCLUSION

Integrating blockchain technology into digital forensics through the Blockchain-based Chain of Custody (B-CoC) framework significantly enhances the management and security of digital evidence. Traditional methods often face challenges such as tampering and inconsistencies in documentation, which can compromise the integrity of the evidence. The B-CoC framework tackles these challenges by harnessing the immutability, transparency, and decentralized characteristics of blockchain technology[13].

The B-CoC framework is built on a private, permissioned blockchain using Ethereum's Geth client and employs a Proof of Authority (PoA) consensus mechanism, ensuring that only authorized nodes can participate and maintaining high levels of security and integrity. Smart contracts are used to automate critical operations such as creating evidence entries, transferring ownership, and retrieving information, making any tampering attempts easily detectable.

By providing a transparent log of evidence handling, the B-CoC framework enhances the reliability and admissibility of digital evidence in legal proceedings. Its primary benefits include improved security, transparency, and accountability, which can potentially reduce costs and increase efficiency.

In conclusion, the B-CoC framework demonstrates how blockchain technology can enhance the management of digital evidence by ensuring its integrity, authenticity, and reliability, thus fostering greater trust in legal proceedings and forensic investigations.

VI. REFERENCES

1] "Digital Forensics Using Blockchain" Dr.S. Harihara Gopalan, S. Akila Suba,C. AshmithashreeA Gayathri, V. Jebin Andrews
2]aws.amazon.com/what-is/blockchain
3] "The future of blockchain technology and cryptocurrencies (Doctoral dissertation)." Hreinsson, E. M., & Blöndal, S. P
4] "Chain of Custody" by Badiye A , Kapoor N ,Menezes RG
5]" Chain of custody and the handling of real evidence" by Paul C Giannelli
6]" Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer" by Auqib Hamid Lone, Roohie Naaz Mir
7]" Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems" by Giuliano Giova
8] B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics by Silvia Bonomi , Marco Casini , and Claudio Ciccotelli
9] "Forensic-chain: Ethereum blockchain based digital forensics chain of custody" by Auqib Hamid Lone, Roohie Naaz Mir Department of Computer Science and Engineering NIT Srinagar
10] K. Zatyko, "Improving cyber forensics cybersecurity through block chain technology with truth based systems," International Symposium on Forensic Science Error Management, July-23-2015
11] "The Application of Blockchain of Custody in Criminal Investigation Process Department of Criminal Investigation", Central Police University,2021
12] Du, X, Le-Khac N-A and Scanlon M. (2017) "Evaluation of digital forensic process models with respect to digital forensics as a service." arXiv preprint arXiv:170801730.
13] "Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review" by Danielle Batista 1ORCID,Ana Lara Mangeth 2ORCID,Isabella Frajhof 2,Paulo Henrique Alves 2,*ORCID,Rafael Nasser 2ORCID,Gustavo Robichez 2,Gil Marcio Silva 3 andFernando Pellon de Miranda 3ORCID