International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Comprehensive Survey of Blockchain Usage in Digital Evidence Handling

A. Y. V. Krishna[1], Naveen Chaudhary[2], Ajit Muzumdar[3]

Submitted: 30/12/2023 **Revised**: 04/02/2024 **Accepted**: 10/02/2024

Abstract Blockchain technology has emerged as a promising solution for enhancing security and trust in various domains, including digital evidence handling. The survey begins by providing an overview of blockchain technology, high- lighting its key components, such as implementation platforms, consensus mechanisms, types and smart contract. Through an analysis of existing re- search and real-world use cases, the survey showcases the potential benefits of blockchain in digital evidence handling. These benefits include increased trust and transparency, improved evidence integrity, efficient and auditable chain of custody processes, and enhanced stakeholder collaboration. How- ever, the survey also identifies several challenges and limitations of blockchain technology in this context. These challenges encompass scalability, privacy concerns, interoperability, legal and regulatory considerations, and standardized frameworks. Addressing these challenges is crucial for successfully adopting and implementing blockchain in digital evidence handling.

Keywords: *Blockchain, Consensus mechanism, Smart contract, Chain of Custody, Digital evidence handling.*

1. Introduction

Proper handling of evidence is a crucial step in digital forensics. During the entire process, from the evidence collection until its utilization in a legal court, multiple parties involved in the investigation may access the evidence and temporarily take its ownership [1]. The entire evidence handling, from Identification to Reporting, should have sequential documentation or trail that accounts for the seizure, custody, control, transfer and analysis sequence. This process is called the Chain of Custody (CoC).

Several indications have been identified that serve as potential indicators of problems in CoC management. Unlike physical evidence, which can be photo/video graphed for future reference, digital evidence cannot be seen, touched, or sketched as it is in binary form. As a result, during the lifespan of digital evidence, its integrity is constantly at risk. Generating massive amounts of data by billions of linked devices presents significant challenges in ensuring authenticity. The complexity and volatility of digital evidence, which may be inadvertently or incorrectly altered after acquisition, necessi tate a CoC that guarantees admissibility in court. The growing number of devices and software in the computer and information technology fields leads to difficulties for cybercrime investigators in processing large volumes of evidence. The critical issue of securing CoC documentation considering that digital evidence can be copied and transferred to other systems. The need for CoC adaptability and capacity is due to the increasing data produced by various emerging digital forensics technologies.

Blockchain technology consists of interconnected data structures known as blocks, which comprehensively record and track all activities within distributed systems on a peer-to-peer network. Each block is linked to the previous block through a unique hash pointer, creating a chain-like structure. This design establishes an immutable and irreversible history, forming an append-only system. Therefore, the blockchain is a distributed ledger technology in that any participant can verify the records by directly examining the data itself [2, 3].

The blockchain is the best option for maintaining and tracing the chain of custody in forensic applications because of its built-in properties that guarantee transparency, authenticity, security, and auditability [4, 5, 6]. Its authenticity protects the accuracy of the recorded information, while its transparency ensures that the entire process is visible and responsible. Furthermore, the blockchain's advanced security protocols guard against tampering and unauthorised changes. Last but not least, its auditability makes it simple to confirm the veracity and accuracy of the evidence trail. Over- all, the blockchain is well-suited for ensuring the integrity and reliability of the chain of custody in forensic applications. Therefore, blockchain is a promising technology that can help to address the CoC issues. In literature, blockchain-enabled CoC solutions have been reported. However, there is a need to investigate blockchain's feasibility in CoC.

This paper investigates different blockchain platforms with

[1] *National Forensic Sciences University, India. ayvkrishna@yahoo.com*
[2] *National Forensic Sciences University, India. naveen.chaudhary@nfsu.ac.in*
[3] *National Forensic Sciences University, India. ajit.muzumdar_goa@nfsu.ac.in*

consensus mechanisms and analyzes their feasibility for CoC. In addition, the existing efforts towards blockchain-enabled CoC are investigated with the research gaps. By considering the research gaps in the existing solutions, future re- search scope is presented, which will help the research community to fulfil the CoC requirements.

The rest of the paper is organized as follows: Section 2 provides a detailed discussion on the digital evidence handling, existing blockchain and consensus mechanisms. Section 3 explores the research efforts towards blockchain enabled CoC with the research gaps. Sections 4 presents the future research scope. Finally, section 5 concludes our findings with the references at the end.

2. Background

2.1. Digital Evidence Handling

The initial handling of digital evidence involves four distinct phases, depicted in Figure 1. The first phase is evidence identification, where investigator verify the nature of the cybercrime and identify potential sources of digital evidence. Investigators collect evidence from these sources using various cyber forensic tools as per standard operating procedures, record the seizure in the prescribed formats, and inform the judicial authority about the acquisitions. In the examination and Analysis phase, investigators make an image of the collected evidence and thoroughly examine the image of collected evidences to determine its relevance to the crime in hand. The investigators send the collected digital evidence to the designated Forensic Laboratory for an expert opinion/report before being presented to the court of law. In addition, it also maintains proper records of evidence handling. The entire evidence handling, from Identification to Reporting, should have sequential documentation or trail that accounts for the seizure, custody, control, transfer and analysis sequence. This process is called the Chain of Custody (CoC). [7, 8, 9].

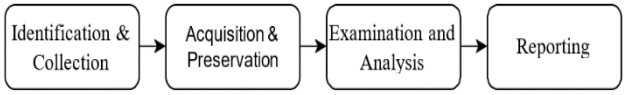

Fig 1: The process of digital evidence handling.

The CoC holds immense importance in evidence management and investigations [10]. It encompasses the systematic preservation and documentation of the chronological history of digital evidence. Forensic investigators need to comprehensively understand digital evidence's discovery, collection, tracking, handling, and protection, including the precise details of where, when and how it was obtained. A robust CoC should consist of meticulous documentation that covers all these aspects. Failure to address these inquiries compromises the CoC's reliability and trustworthiness. In addition, CoC should maintain the integrity of digital evidence. Ultimately, with a valid certificate of conformity, the evidentiary value and usefulness of the evidence will be maintained. In the realm of digital systems, the integrity of the digital evidence system can be compromised by data tampering, which involves unauthorized modifications or alterations to the evidence, as well as privacy breaches that expose and potentially misuse private information. Hence, we require CoC that offers integrity, trustworthy, authentication, Non-tampered, traceability, and verifiability. In addition, an architectural disconnect exists between the storage of digital evidence gathered by experts and the widespread implementation of standardized CoC mechanisms. These mechanisms enable other law enforcement personnel to access, maintain, and utilize a reliable and legally compliant chain of custody for digital evidence. This requires the utmost integrity and reliability throughout the process [11]. The existing chain of custody faces a scientific challenge as it is inherently impossible to prove that evidence has not been intentionally altered throughout all phases. The process of CoC encounters multiple challenges, including issues related to data integrity and the security of CoC documentation. Digital evidence possesses characteristics of complexity, diffusion, volatility, and susceptibility to change.

2.2. Blockchain Technology

Blockchain, also known as Distributed Ledger Technology (DLT), functions as a distributed database or ledger that possesses a remarkable quality of practical immutability. This technology operates through a decentralized Peer-to-Peer (P2P) network, leveraging consensus mechanisms, cryptography, and block referencing to order and authenticate transactions [2, 3] To ensure the integrity of participants' identities, each peer is assigned a cryptographic pseudonym, enabling them to initiate transactions securely. The transactions initiated by users are transparently visible to all peers and are grouped into blocks. These blocks of transactions undergo cryptographic verification by peer nodes based on distributed consensus. Once verified, the block is added to the chain maintained by each node, creating a virtually unalterable record. In the realm of blockchain, a smart contract refers to an agreement that binds participants according to predefined policies. It possesses its own private storage and is associated with preprogrammed executable code, which is triggered when a message is sent to its designated address. The common working of the bitcoin blockchain is depicted in Figure 2.

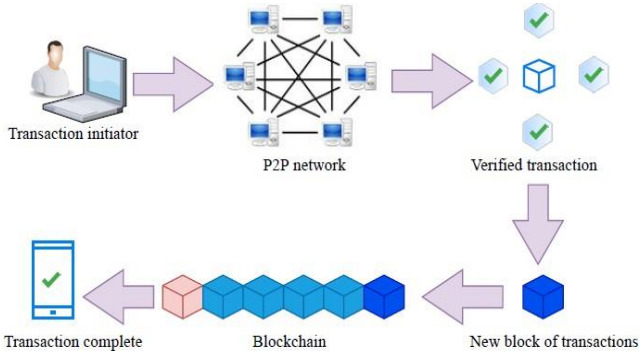

Fig 2: Common working of the blockchain.

Bitcoin, recognized as the pioneering implementation of blockchain [12], operates as a permissionless ledger that allows any node to join or leave the network. Primarily designed for financial transactions, it offers a decentralized platform. On the other hand, the Ethereum blockchain caters to business-to-consumer applications and introduces smart contracts to apply business logic. For rapid transaction validation, Ethereum adopts the Proof of Stake (PoS) consensus mechanism [13]. Hyperledger [14], in contrast, is a permissioned blockchain preferred for business-to-business applications. In this setup, a network is formed by a consortium of organizations, where each organization takes responsibility for creating the peers. Transaction requests are initiated by peers and forwarded to endorser peers. Only the endorser peer can execute the chain code (smart contract) and authorize the transaction. The client sends approved transactions to the orderer peer, which compiles them into a block and forwards it to the anchor node. The anchor node broadcasts the block to update the ledger on other peers. Corda [15], another permissioned blockchain platform, operates with a network operator issuing certificates to participants for network access. Each node maintains a separate list of transactions, referred to as facts associated with it. Corda introduces the concept of an immutable object called 'state,' which represents facts shared by nodes. The historical and current states are stored in a database called the Vault. Corda treats transactions as proposals to update the states and utilizes the UTXO model, supporting notary change transactions to modify the state. IOTA [16] employs a unique tangle data structure. Transactions are stored and distributed across IOTA nodes to ensure data integrity. Dedicated IRI nodes validate transactions and propagate them to other IRI nodes. Senders transmit data and IOTA tokens to receivers through IRI nodes, with the IOTA token serving as a record of ownership held by the IRI nodes.

A blockchain's scalability, throughput and fault tolerance depend on underlying consensus. Various consensus mechanisms exist within blockchain networks to facilitate secure block creation and maintain the integrity of the blockchain. The most well-known consensus mechanism is Proof of Work (PoW) [12], which requires miners to solve complex mathematical puzzles to append a block to the blockchain. This consensus offers high security but is energy inefficient, less scalable, and has limited throughput. Proof of Stake (PoS) selects a miner based on the age of the owned coins for new block creation. Delegated Proof of Stake (DPoS) [17] involves the election of delegates based on their stake or votes received from users. Delegates perform block creation and verification, with dishonest delegates subject to removal through voting. Intel introduced Proof of Elapsed Time (PoET) [18], designed to run on its trusted execution environment. PoET uses a lottery- based model where the next leader is randomly chosen to finalize the block. The validator with the shortest waiting time is elected for block creation. PoET is hardware-dependent. Proof of Burn (PoB) [19] requires miners to commit to burning coins to increase their chances of mining a new block. As miners mine new blocks, their power to burn coins diminishes. Proof of Stake Velocity (PoSV) [20] encourages both coin hoarding (stake) and coin spending (velocity) and incentivizes transaction verification. Proof of Authority (PoA) [21] is suitable for private blockchains, where a group of authorities holds special permission to control new block creation. In Proof of Capacity (PoC) [22], miners are granted mining rights based on their available storage space. Miners can pre-compute possible mining solutions and store them on their hard disks. Proof of Importance [23] determines block creation eligibility based on participants' importance scores. Participants with higher importance scores have a greater chance of mining new blocks, with importance scores influenced by vesting, transaction partners, and transaction size. Proof of Activity combines elements of PoW and PoS [24]. The first block (Genesis block) is created using PoW, and then validators can create a new block based on their stake. Proof of Reputation (PoR) [24] determines block creation chances based on participants' reputation, considering their assets and transaction activity.

Blockchain technology can be categorized into two types based on data access permissions: Permissionless and Permissioned. Permissionless blockchains, such as Bitcoin [25], are open to anyone who wants to participate and con- tribute to the network. They provide a decentralized and transparent plat- form for transactions. On the other hand, permissioned blockchains offer improved transaction processing speed and more controlled trust management. Access to a private blockchain is restricted to a specific group of participants who have been granted permission.

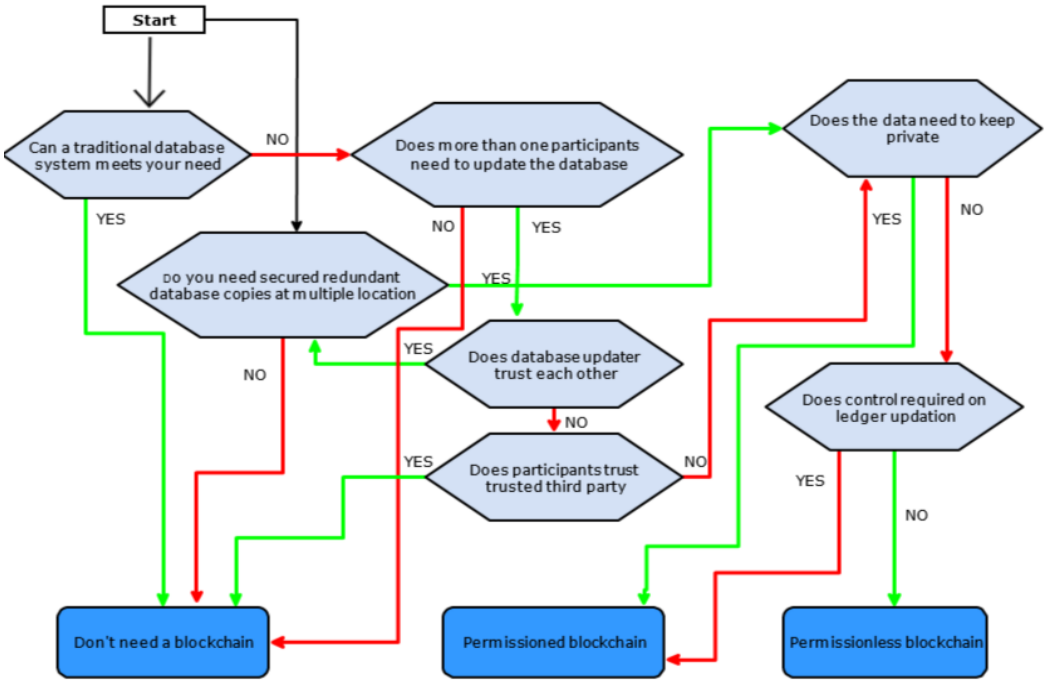

Fig 3: Blockchain feasibility decision tree.

Figure 3 depicts a blockchain feasibility decision tree. This tree helps determine whether and which blockchain suits the given use case. Utilizing Blockchain and Smart Contracts technologies offers significant advantages, particularly for applications that demand information security, immutability, and integrity in governmental and business contexts. While traditional systems provide relatively straightforward control, the decentralized nature of blockchain necessitates shifts in responsibilities and new governance approaches. Implementing blockchain without comprehensive changes may not fully realize all the associated benefits. The blockchain possesses fundamental attributes deeply embedded in its design, including transparency, authenticity, security, and auditability. These inherent characteristics make it an exceptional choice for maintaining and tracing the chain of custody in forensic applications.

3. Existing Digital Evidence Handling Approaches

Rasjid *et al.* [25] focused on the integrity of digital evidence. It relies on the most common approach *i.e.* cryptographic hashing function allows the fact-finder to verify that the evidence remains unchanged since its acquisition.

However, unless a secure tamper-evident mechanism is in place, there is nothing to prevent dishonest individuals from altering the digital evidence and its associated hash value at a later stage. The fact-finder's verification is limited to confirming that the evidence has not been tampered with since the hash value calculation. Notably, the hash itself does not contain temporal information, and timestamps associated with digital evidence can potentially be manipulated or backdated.

Cosic *et al.* [26] developed a dependable time stamping technique to safeguard digital evidence throughout the investigation process. This technique involved obtaining a timestamp from a secure third party to establish the exact date and time staff accessed the evidence. However, a significant challenge arises in ensuring the reliability of the time source, as it relies on the accurate setting of the clock responsible for generating the timestamp.

Saleem *et al.* [27] employed a range of security techniques to safeguard the integrity of digital evidence, which included the use of CRC, hash functions, and digital signatures. After conducting tests and evaluations, SHA-512 was selected as the integrity protection mechanism due to its fast computational performance and minimal susceptibility. However, it is essential to note that an individual could modify the original data, recalculate the hash, and substitute the original hash with the newly calculated one. This action would undermine the integrity service provided by the security measures.

Widatma *et al.* [28] applied the RC4 cryptography technique to encrypt the XML structure of the digital chain of custody data storage. One advantage of using XML is its simplicity, making it easily comprehensible even for non-professionals. Furthermore, XML does not require a specific database management system for access. However, a notable drawback is that the openness of XML raises concerns regarding the acceptance of digital evidence integrity in a court of law. Additionally, the RC4 encryption process tends to be slower when dealing with longer plaintext data.

Lone *et al.* [29] have proposed a blockchain based digital forensics CoC. The system focuses on bringing integrity

and tamper resistance to digital forensics CoC. The authors used Ethereum blockchain and proof of concept for the implementation. The performance of the proposed system is evaluated using the Hyperledger composer framework. However, the system suffers from low transaction throughput and high transaction latency.

Ahmed *et al.* [30] proposed blockchain-based CoC. The framework focuses on real-time tamper-proof evidence management. Ali *et al.* [31] combined fuzzy hash and blockchain technology for CoC in digital image forensics; this paradigm presents a promising solution for ensuring the integrity of digital evidence, particularly in the context of CoC documents. Utilizing fuzzy hash within the blockchain data structure empowers the framework to navigate the challenges posed by error-prone tools and uncertainties inherent in CoC documents, offering enhanced reliability and integrity.

Tian *et al.* [32] introduces the Block-DEF (Blockchain-based Digital Evidence Framework), which establishes a secure environment for managing digital evidence using blockchain technology. The framework utilizes a loose coupling structure, separating the evidence from its associated information. While the evidence information is stored on the blockchain, the actual evidence is securely stored on a trusted storage platform. The proposed system's blockchain framework is based on a practical Byzantine fault tolerance consensus mechanism.

Khan *et al*. [33] have used the Hyperledger sawtooth framework to establish a secure, transparent, and efficient CoC. In this proposed architecture, a consortium of participating stakeholders forms a private network, enabling seamless exchange and consensus on various investigation activities. These activities are then securely recorded on the blockchain. The proposed frame- work offers a robust mechanism for ensuring information integrity, tampering prevention, and evidence preservation.

Bonomi *et al.* [34] proposed a blockchain-based Chain of Custody (B- CoC), designed to streamline and enhance the CoC process. By leveraging blockchain technology, B-CoC offers a decentralized approach that ensures the auditable integrity of collected evidence and provides traceability of owners throughout the CoC. The proposed system is developed using the Ethereum blockchain implementation platform. However, the proposed system lacks multiple stakeholder management and struggles with anonymity.

Li *et al.* [35] have proposed an Ethereum blockchain-based legal evidence management system that oversees the entire flow of evidence and court data, from evidence collection and access during police investigations to jury voting in court trials. This system incorporates the use of short randomizable signatures to authenticate witnesses' identities anonymously, ensuring the protection of their privacy. However, this system suffers from poor transaction latency and throughput.

Zarpala *et al.* [36] proposed an Ethereum blockchain-based forensic model for financial embezzlement detection. The proposed system exhibits a forensically sound flow for investigating financial crimes, leveraging the Ethereum blockchain as its foundation. In addition, it utilizes the transparency and traceability features of the Ethereum blockchain.

Petroni *et al.* [37] proposed Ethereum blockchain-enabled storage and maintenance of digital CoC. This framework enables digital evidence storage and facilitates consultation by law enforcement personnel, maintenance staff, and individuals involved in legal proceedings, including lawyers, judges, and prosecutors.

Zhang *et al.* [38] proposed a solution for enhancing the trustworthiness of the chain of custody for cloud forensics is a blockchain-based process provenance. This approach offers proof of existence and privacy preservation for process records. By leveraging blockchain technology and group signatures, the scheme aims to prevent tampering and preserve privacy. However, a fundamental limitation of this scheme is its reliance on the honest performance of central nodes.

Burri *et al.* [39] proposed a blockchain-based verifiable e-CoC (electronic Chain of Custody) ledger with chronological independence. In this approach, each e-CoC record is stored within a block, and each block is linked to the preceding one through a hash value. Selected data is hosted on the blockchain to ensure privacy. Additionally, to demonstrate the e-CoC ledger's unaltered state, periodic information transmissions are made to a public blockchain, which guarantees integrity through its decentralized nature and the structure of its secure ledger. Not all blocks are sent to the public blockchain, allowing for varying levels of verification.

Elgohary et al. [40] addressed the uncertainty and trustworthiness of digital evidence with the help of the Ethereum blockchain-based framework. Framework relies on the fuzzy hash function to maintain the integrity of the digital evidence as the conventional hash method is inefficient at dealing with identical files that may arise from benign or malicious alteration of the digital evidence. However, the framework may suffer from scalability issues.

Yuni et al. [41] employed Blockchain technology to integrate the Digital Evidence Cabinet (DEC) architecture. The resulting prototype is known as B-DEC. B-DEC leverages data storage integrity to manage digital evidence associated with DEC, which is stored in XML format. However, the system requires secure digital evidence

storing ability. It is imperative to implement measures, such as encryption, to enhance the protection of digital evidence. Alruwaili [42] proposed a framework leveraging a private blockchain protocol and smart contracts to facilitate the control, transfer, analysis, preservation, and monitoring of digital evidence. The utilization of smart contracts in this model aims to augment the automation process, thereby enhancing evidence preservation and handling with improved security measures. The proposed framework emphasizes security when sharing forensic data by implementing stringent authorization protocols for all participating entities involved in data exchange and sharing. In addition, the framework ensures the secure storage of forensic data, minimizing the risk of attacks. This approach establishes an enhanced evidence preservation and handling methodology

that prioritizes improved security and reliability.

Hossain *et al.* [43] proposed a framework with a specific focus on detecting criminal incidents within the Internet of Things (IoT) and collecting communication details from various entities within the IoT ecosystem. The framework aims to model transaction interactions effectively. However, one notable drawback of this methodology is its inefficiency in collecting and analyzing data within large-scale IoT systems. This limitation hinders the framework's effectiveness in handling extensive data sets and conducting timely analysis, which is crucial for forensic investigations in such complex environments. Kumar et al. [44] proposed Internet-of-Forensics (IoF), a tailored blockchain based framework for digital forensics in the context of the Internet of Things (IoT). IoF offers a transparent view of the investigation process involving all stakeholders within a unified framework, including heterogeneous devices and cloud service providers. It leverages a blockchain-based case chain to manage the investigation process, encompassing chain-of-custody and evidence chain management. IoF utilizes a consensus mechanism within a consortium to address cross-border legalization challenges, ensuring transparency and ease of forensic reference.

Li et al. [45] proposed the IoT forensic chain (IoTFC), a blockchain enabled forensics framework explicitly designed for the Internet of Things (IoT). The IoTFC ensures that evidence items within the forensic investigation are traceable and possess a verifiable provenance. The framework records detailed information about evidence identification, preservation, analysis, and presentation within blocks of the blockchain. This approach strengthens the trust in both the evidence items and the examiners by offering transparency through an audit trail. The framework provides an immutable record of events, guaranteeing evidence's authenticity and traceability while establishing a distributed trust mechanism among all involved entities.

Singh et al. [46] proposed a framework to address the secure storage of digital evidence captured before and after an incident, with the goal of enabling reactive forensics. The model incorporates several key components: integrity checks, environment sandboxing, strong encryption, two-factor authentication, and unique random file naming. These elements are essential to ensure the security and reliability of the stored forensic artefacts. The results demonstrated that securing forensic artefacts can be achieved with minimal effort, as the model proved relatively inexpensive and reliable.

Cebe et al. [47] proposed forensic framework leverages permissioned blockchain technology, vehicular public key infrastructure integration, and fragmented ledger design to enable trustless, traceable, and privacy-aware post-accident analysis. The framework aims to optimize storage and processing overhead, providing an effective and secure solution for managing vehicle-related data.

Based on existing literature [48], we identified CoC requirements as: **R1**: No privilege escalation i.e. CoC framework should maintain access control strictly, **R2**: Non-repudiation i.e. forensic investigator should not deny evidence handling, **R3**: No single point of failure i.e. CoC ledger should be stored on distributed database, **R4**: Evidence immutability i.e. CoC ledger should be tamper-proof, **R5**: Evidence trustworthiness *i.e.* consensus mechanism should bring trust regarding CoC ledger updation, **R6**: Evidence traceability *i.e.* CoC ledger transactions history should be available to concerned authority, **R7**: Evidence provenance *i.e.* all CoC ledger records must be verified before CoC ledger updation, and **R8**: Evidence integrity *i.e.* CoC ledger should be tamper-proof. In addition, we have performed a requirement analysis of the existing blockchain enabled CoC approaches.

4. Future Directions

Blockchain technology can be a feasible solution to implement a secure and trustworthy chain of custody in digital forensics due to its outstanding features. The transparency of the blockchain ensures that the entire process is open and accountable, creating a sense of trust and reliability. The blockchain's robust cryptographic mechanisms protect the recorded data's confidentiality and integrity. Unauthorised modification or change becomes impossible once the transaction data is recorded on the blockchain. Therefore, the reliability and accuracy of the evidence trail are assured. The blockchain's decentralised architecture and cryptographic techniques provide a high level of security, making it difficult for nefarious parties to influence or tamper with the chain of custody. Additionally, the auditability of the blockchain enables

quick and simple confirmation of the accuracy and validity of the evidence trail. Participants can examine and confirm the records on their own. By leveraging these inherent attributes, the blockchain is a dependable and robust solution for maintaining the integrity and traceability of the chain of custody in forensic applications. It offers a transparent, secure, and auditable platform that enhances the trustworthiness and reliability of digital evidence. However, blockchain-based applications for securing the chain of custody in digital forensics introduce unique challenges. The CoC refers to the chronological documentation of the handling and transfer of digital evidence, ensuring its integrity and admissibility in legal proceedings. Here are some significant challenges and potential future research directions to address them:

4.1. Immutability and Integrity

Blockchain technology provides immutability, which is crucial for maintaining the integrity of digital evidence. However, ensuring that the evidence stored on the blockchain remains tamper-proof throughout its lifecycle is a challenge. Future research can focus on developing robust cryptographic techniques, including digital signatures and hash functions, to enhance the immutability and integrity of the evidence stored on the blockchain.

Table 1: A summary of the existing CoC frameworks in terms of fulfilling the requirements.

Sr. No.	Author/Year	Approach/ System	DLT	Limitation	CoC Requirements							
					R1	R2	R3	R4	R5	R6	R7	R8
1	Rasjit *et al.* [25]/ 2017	Hash function based Digital forensics	NA	Lack of temporal information and timestamp based hash	✗	✓	✗	✗	✓	✗	✗	✓
2	Cosic *et al.* [26]/ 2010	Time stamp based CoC	NA	Reliability depends on clock synchronization	✗	✓	✗	✗	✓	✗	✓	✓
3	Saleem *et al.* [27]/ 2011	Ensuringdigital evidence integrity	NA	Undermine the integrity of the digital evidence	✗	✓	✗	✗	✓	✗	✗	✓
4	Widatma *et al.* [28]/ 2018	RC4 based secured digital CoC	NA	Slow hash processing	✗	✓	✗	✗	✗	✗	✗	✓
5	Lone *et al.* [29]/ 2019	Blockchain based digital CoC	Ethereum	suffers from poor transaction latency and throughput	✗	✓	✓	✓	✓	✓	✗	✓
6	Ahmed *et al.*[30] / 2020	Blockchain based CoC	Ethereum	Low transaction throughput and less transparency	✗	✓	✓	✓	✓	✓	✗	✓
7	Ali *et al.*[31] / 2020	Blockchain and grey hash based digital image forensics	Hyperledger fabric	Computational overhead	✓	✓	✓	✓	✓	✗	✗	✓
8	Tian *et al.*[32] / 2019	Secure digital evidence framework	ONPBFT based permissioned blockchain	Depends on trusted storage platform	✓	✓	✗	✓	✓	✗	✗	✓
9	Khan *et al.*[33] / 2021	Multimedia CoC forensic investigation architecture	Hyperledger sawtooth	Exponentially increasing transaction count	✓	✓	✗	✓	✓	✗	✗	✓
10	Bonomi *et al.*[34] / 2018	Blockchain based evidence management	Ethereum	Lacks multiple stakeholder management and struggles with anonymity	✗	✓	✓	✓	✓	✓	✗	✓
11	Li *et al.*[35] / 2021	Lechain	Ethereum	Struggles with security, privacy, and transparency issues	✗	✓	✗	✓	✗	✓	✗	✗
12	Zarpala *et al.*[36] / 2021	Blockchain based forensic model	Ethereum	Struggles with financial digital investigation	✗	✓	✓	✓	✗	✓	✗	✗
13	Petroni *et al.*[37] /	Blockchain based digital evidence maintainance	Ethereum	Risk of intentional manipulation of data	✗	✓	✓	✗	✗	✓	✗	✗

Sr. No.	Author/Year	Approach/ System	DLT	Limitation	CoC Requirements							
					R1	R2	R3	R4	R5	R6	R7	R8
	2020											
14	Zhang *et al.*[38] / 2017	Blockchain based process provenance for cloud forensics	Hyperledger fabric	Existence of central management nodes	✓	✓	✗	✓	✓	✗	✗	✓
15	Burri *et al.*[39] / 2020	Verifible CoC using blockchain	Hyperledger composer	Not fault tolerant	✗	✓	✓	✗	✓	✓	✗	✓
16	Elgohary *et al.*[40] / 2022	Improved uncertainty in CoC for image forensics	Permissioned blockchain with fuzzy hash	Struggles with privacy	✗	✓	✓	✗	✗	✗	✗	✓
17	Yuni *et al.*[41] / 2019	Blockchain for evidence management	Ethereum	suffers from poor transaction latency and throughput	✗	✓	✓	✗	✗	✓	✗	✗
18	Alruwaili *et al.*[42] / 2021	Custodyblock	Hyperledger fabric	Computational overhead	✓	✓	✗	✓	✓	✗	✗	✓
19	Hossain *et al.*[43] / 2018	Forensic investigation frameworkfor IoT using blockchain	Permissioned blockchain	Struggles with transparency	✗	✓	✓	✗	✗	✗	✗	✓
20	Kumar *et al.*[44] / 2021	Blockchain based IoT forensic investigation	Ethereum	Low transaction throughput and less transparency	✗	✓	✓	✓	✓	✓	✗	✓
21	Li *et al.*[45] / 2019	Blockhain based IoT and social system digital forensic	Permissioned blockchain	Struggles with transparency	✓	✓	✓	✗	✗	✗	✗	✓
22	Singh *et al.*[46] / 2018	Secure storage model for digital forensics	NA	May be vulnerable to single point of failure	✗	✓	✗	✗	✓	✗	✗	✓
23	Cebe *et al.*[47] / 2017	Lightweight blockchain model for forensic applica-tion	Permissioned blockchain	Struggles with transparency	✓	✓	✗	✗	✓	✗	✗	✓

(✓: Fulfilled, ✗: Not Fulfilled)

4.2. Authenticity and Non-repudiation

Establishing the authenticity and non-repudiation of digital evidence is essential in legal proceedings. Blockchain can provide a decentralized and transparent framework to verify the authenticity of evidence and ensure non-repudiation. Future research can explore the integration of digital sig- natures, timestamping mechanisms, and secure communication protocols to strengthen the authenticity and non-repudiation aspects of the blockchain- based chain of custody systems.

4.3. Privacy and Confidentiality

Protecting the privacy and confidentiality of sensitive information during the chain of custody process is crucial. While blockchain offers transparency, it may expose sensitive details to all participants. Future research can fo-cus on incorporating privacy-enhancing techniques, such as zero-knowledge proofs or selective disclosure mechanisms, to ensure that only authorized parties can access specific information while preserving the transparency and integrity of the chain of custody.

4.4. Standardization and Interoperability

Achieving interoperability between digital forensic tools and blockchain platforms is vital for seamless integration and widespread adoption. Future research can explore the development of standardized data formats, proto- cols, and interoperability frameworks to enable efficient and secure data ex- change between digital forensic tools and blockchain-based chain of custody systems.

4.5. Scalability and Performance

Digital forensics involves processing and storing large volumes of data. Blockchain scalability becomes a challenge when considering digital evidence's transaction throughput and storage requirements. Future research can focus on developing scalable blockchain architectures, including off-chain storage solutions, sidechains, or layer-two protocols, to enhance the scalability and performance

of blockchain-based chain of custody systems.

4.6. Trust and Governance

Establishing trust among participants in the chain of custody process is crucial. Future research can explore integrating decentralized identity management systems, reputation mechanisms, and smart contracts to ensure individuals' trustworthiness in handling digital evidence. Additionally, research efforts can focus on developing governance models that provide transparency, accountability, and fairness in the chain of custody process.

4.7. Usability and Adoption

Digital forensic professionals should find it simple and easy to employ blockchain-based CoC systems. Future research might create user-friendly user interfaces, training courses, and educational materials to improve the usability and adoption of a blockchain-based CoC in digital forensics.

Collaboration between researchers, experts in digital forensics, lawyers, and blockchain engineers is necessary to overcome these obstacles. By solving these difficulties, blockchain-based applications can increase the safety, reliability, and admissibility of digital evidence in court, enhancing the general efficiency and dependability of the digital forensic process.

5. Conclusion

Digital evidence handling must address trust, transparency, evidence integrity, efficient and auditable chain of custody processes, and enhanced stakeholder collaboration. This paper highlights the significant potential and challenges of applying blockchain technology in handling digital evidence. Blockchain has the potential to revolutionize digital evidence handling by providing enhanced security, trust, and efficiency. In addition, blockchain offers immutability, transparency, decentralization, and cryptographic security, which can improve the security, integrity, and efficiency of the digital evidence handling process. As blockchain technology continues to evolve and mature, it is expected to play a significant role in strengthening the digital forensic process, combating cybercrime, and ensuring the integrity of digital evidence in the future.

The survey demonstrates that the use of blockchain in managing digital evidence, including securing the CoC, confirming the veracity of digital evidence, locating and tracing illegal transactions, and maintaining the integrity of forensic data, has been successful. The existing blockchain-enabled applications have shown promising improvements in the accuracy and dependability of digital forensic techniques and the ability to conduct more efficient investigations and support the admissibility of evidence in court cases. However, also point up several issues and possible directions for fur- their study. Scalability, privacy, interoperability, legal and regulatory issues, and standardized frameworks are some of these difficulties. Researchers, law enforcement agencies, lawyers, and technological specialists must work together across disciplines to overcome these obstacles.

Future research directions in this field should focus on addressing the scalability limitations of blockchain, developing privacy-preserving mechanisms, establishing interoperability standards, managing legal and regulatory concerns surrounding blockchain based evidence, and enhancing user-friendliness and adoption of blockchain technology in digital evidence handling.

References

[1] S. Nair, J. L. de la Vara, M. Sabetzadeh, D. Falessi, Evidence manage- ment for compliance of critical systems with safety standards: A survey on the state of practice, Information and Software Technology 60 (2015) 1–15.

[2] A. Muzumdar, C. Modi, M. G.M., C. Vyjayanthi, A trustworthy and incentivized smart grid energy trading framework using distributed ledger and smart contracts, Journal of Network and Computer Applications 183-184 (2021) 103074.

[3] A. Muzumdar, C. Modi, C. Vyjayanthi, A permissioned blockchain enabled trustworthy and incentivized emission trading system, Journal of Cleaner Production 349 (2022) 131274.

[4] F. C. Tsai, The application of blockchain of custody in criminal investigation process, Procedia Computer Science 192 (2021) 2779–2788. Knowledge-Based and Intelligent Information and Engineering Systems: Proceedings of the 25th International Conference KES2021.

[5] H. Al-Khateeb, G. Epiphaniou, H. Daly, Blockchain for Modern Digital Forensics: The Chain-of-Custody as a Distributed Ledger, Springer International Publishing, pp. 149–168.

[6] M. Chopade, S. Khan, U. Shaikh, R. Pawar, Digital forensics: Maintaining chain of custody using blockchain, in: 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 744–747.

[7] P. C. Giannelli, Chain of custody and the handling of real evidence, Am. Crim. L. Rev. 20 (1982) 527–568.

[8] M. M. Evans, P. A. Stagner, Maintaining the chain of custody evidence handling in forensic cases, AORN Journal 78 (2003) 563–569.

[9] L. E. Cartier, S. H. Ali, M. S. Krzemnicki,

Blockchain, chain of custody and trace elements: An overview of tracking and traceability opportunities in the gem industry., Journal of Gemmology 36 (2018).

[10] A. Tanner, J. Bruno, Timely: A chain of custody data visualizer, in: 2019 SoutheastCon, pp. 1–5.

[11] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, E. K. Markakis, A survey on the internet of things (iot) forensics: Chal- lenges, approaches, and open issues, IEEE Communications Surveys and Tutorials 22 (2020) 1191–1221.

[12] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Decentralized business review (2008) 21260–21269.

[13] M. Pustiˇsek, A. Kos, Approaches to front-end iot application development for the ethereum blockchain, Procedia Computer Science 129 (2018) 410–419.

[14] Hyperledger, Hyperledger fabric, https://www.hyperledger.org/use/ fabric, 2017.

[15] Corda, Corda master documentation, https://docs.corda.net/, 2016.

[16] IOTA, The next generation of distributed ledger technology iota, https://www.iota.org/, 2015.

[17] B. Group, Proof of stake versus proof of work, https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf, 2015.

[18] POET, Sawtooth v1.1.2 documentation, https://sawtooth.hyper ledger.org/docs/core/releases/latest/architecture/poet.html, 2018.

[19] P4Titan, Slimcoin: A peer-to-peer crypto-currency with proof-of-burn, http://www.slimcoin.club/whitepaper.pdf, 2019.

[20] PoSV, Proof of stake velocity: Building the social currency of the digital age - reddcoin, https://reddcoin.com/proof-of-stake-velocity/, 2016.

[21] S. Angelis, Pbft vs proof of authority and applying the cap theorem to permissioned blockchain, http://ceur-ws.org/Vol-2058/paper-06.pdf, 2016.

[22] PoC, Proof of capacity, https://www.investopedia.com/terms/ p/proof- capacity-cryptocurrency.asp, 2010.

[23] NEM, Nem technical reference, https://nemplatform.com/wp-content/uploads/2020/05/NEM techRef.pdf, 2015.

[24] A. Bentov, Rosenfeld, Proof of activity: Extending bitcoin's proof of work via proof of stake, SIGMETRICS Perform. Eval. Rev. 42 (2014) 34–37.

[25] G. W. E. A. Zulfany Rasjid, Benfano Soewito, A review of collisions in cryptographic hash function used in digital forensic tools, Procedia Computer Science 116 (2017) 381–392.

[26] J. C´osi´c, M. Baˇca, (im)proving chain of custody and digital evidence integrity with time stamp, in: The 33rd International Convention MIPRO, pp. 1226–1230.

[27] S. Saleem, O. Popov, R. Dahman, Evaluation of security methods for ensuring the integrity of digital evidence, in: 2011 International Conference on Innovations in Information Technology, pp. 220–225.

[28] K. Widatama, Y. Prayudi, B. Sugiantoro, Application of rc4 cryptography method to support xml security on digital chain of custody data storage, International Journal of Cyber-Security and Digital Forensics 7 (2018) 230–238.

[29] A. H. Lone, R. N. Mir, Forensic-chain: Blockchain based digital forensics chain of custody with poc in hyperledger composer, Digital Investigation 28 (2019) 44–55.

[30] L. Ahmad, S. Khanji, F. Iqbal, F. Kamoun, Blockchain based chain of custody towards real time tamper-proof evidence management, in: Proceedings of the 15th International Conference on Availability, Reliability and Security, ARES '20.

[31] M. Ali, A. Ismail, H. Elgohary, S. Darwish, S. Mesbah, A procedure for tracing chain of custody in digital image forensics: A paradigm based on grey hash and blockchain, Symmetry 14 (2022).

[32] Z. Tian, M. Li, M. Qiu, Y. Sun, S. Su, Block-def: A secure digital evidence framework using blockchain, Information Sciences 491 (2019) 151–165.

[33] A. A. Khan, M. Uddin, A. A. Shaikh, A. A. Laghari, A. E. Rajput, Mf-ledger: Blockchain hyperledger sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture, IEEE Access 9 (2021) 103637–103650.

[34] S. Bonomi, M. Casini, C. Ciccotelli, B-coc: A blockchain-based chain of custody for evidences management in digital forensics, arXiv preprint arXiv:1807.10359 (2018).

[35] M. Li, C. Lal, M. Conti, D. Hu, Lechain: A blockchain-based lawful evidence management scheme for digital forensics, Future Generation Computer Systems 115 (2021) 406–420.

[36] L. Zarpala, F. Casino, A blockchain-based forensic model for financial crime investigation: the embezzlement scenario, Digital Finance 3 (2021) 301–332.

[37] B. C. Aparecido Petroni, R. F. Gon¸calves, P. S´ergio de Arruda Ign´acio, J. Z. Reis, G. J. Dolce Uzum Martins, Smart contracts applied to a functional architecture for storage and maintenance of digital chain of custody using blockchain, Forensic Science International: Digital Investigation 34 (2020) 300985.

[38] Y. Zhang, S. Wu, B. Jin, J. Du, A blockchain-based process provenance for cloud forensics, in: 2017 3rd IEEE International Conference on Computer and Communications (ICCC), pp. 2470–2473.

[39] X. Burri, E. Casey, T. Boll´e, D.-O. Jaquet-Chiffelle, Chronological independently verifiable electronic chain of custody ledger using blockchain technology, Forensic Science International: Digital Investigation 33 (2020) 300976.

[40] H. M. Elgohary, S. M. Darwish, S. M. Elkaffas, Improving uncertainty in chain of custody for image forensics investigation applications, IEEE Access 10 (2022) 14669–14679.

[41] E. Yunianto, Y. Prayudi, B. Sugiantoro, B-dec: Digital evidence cabinet based on blockchain for evidence management, Int. J. Comput. Appl 181 (2019) 22–29.

[42] F. F. Alruwaili, Custodyblock: A distributed chain of custody evidence framework, Information 12 (2021) 88.

[43] M. Hossain, Y. Karim, R. Hasan, Fif-iot: A forensic investigation frame- work for iot using a public digital ledger, in: 2018 IEEE International Congress on Internet of Things (ICIOT), pp. 33–40.

[44] G. Kumar, R. Saha, C. Lal, M. Conti, Internet-of-forensic (iof): A blockchain based digital forensics framework for iot applications, Future Generation Computer Systems 120 (2021) 13–25.

[45] S. Li, T. Qin, G. Min, Blockchain based digital forensics investigation framework in the internet of things and social systems, IEEE Transactions on Computational Social Systems 6 (2019) 1433–1441.

[46] A. Singh, R. A. Ikuesan, H. Venter, Secure storage model for digital forensic readiness, IEEE Access 10 (2022) 19469–19480.

[47] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, S. Uluagac, Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles, IEEE Communications Magazine 56 (2018) 50–57.

[48] D. A. Flores, A. Jhumka, Implementing chain of custody requirements in database audit records for forensic purposes, in: 2017 IEEE Trust-com/BigDataSE/ICESS, pp. 675–682.