A Bibliometric Analysis and Systematic Review of a Blockchain-Based Chain of Custody for Digital Evidence

Belinda I. Onyeashie(✉), Petra Leimich, Sean McKeown, and Gordon Russell

Edinburgh Napier University, Edinburgh, Scotland
belinda.onyeashie@napier.ac.uk

Abstract. The effective management of digital evidence is critical to modern forensic investigations. However, traditional evidence management approaches are often prone to security and integrity issues. In recent years, the use of blockchain technology has emerged as a promising solution to enhance the security, transparency, and integrity of digital evidence. This systematic review critically evaluates the current state of research on blockchain-based chain of custody for digital evidence and its potential to transform the digital forensic community. By analysing papers from major databases, this study provides a bibliometric analysis of the research trends and opportunities for blockchain-based evidence management since 2015. The review highlights the benefits of blockchain technology in providing an immutable and decentralised structure for documenting and auditing evidence trails. Additionally, this research identifies the challenges and limitations of implementing a blockchain-based chain of custody and presents practical and scalable solutions for overcoming these challenges at Big Data scale.

Keywords: Bibliometric Analysis · Big Data · Chain of Custody · Digital Evidence · Digital Forensic

1 Introduction

There are challenges associated with the storage and sharing of digital evidence during an investigation. These challenges may include concerns about authenticity, integrity, privacy, and security, as well as difficulties with storing and sharing evidence. There have been significant delays for investigations involving digital evidence. Some cases may take up to six years to coordinate the handling and processing, and law enforcement personnel may be required to travel up to 4,500 times every week to physically obtain digital evidence [1]. Another significant challenge the police force is facing is how to securely store and share digital evidence during an investigation [2]. The volume of data generated and stored electronically is expanding at an exponential rate [3]; therefore, a secure and efficient method for storing and sharing evidence is required. However, the current procedures for storing and sharing digital evidence are inadequate and prone to errors [2] and threats, such as concerns about insider threats. This may compromise the integrity of the evidence and delay the investigation process.

Z. Tan et al. (Eds.): BDTA 2023, LNICST 555, pp. 112–131, 2024.
https://doi.org/10.1007/978-3-031-52265-9_8

Additionally, digital evidence monitoring, and documentation are still done manually, on paper, which is error-prone and time consuming [4]. Chain of custody is often a problem when dealing with digital evidence. The chain of custody plays a crucial role in digital forensic investigations by keeping track of every detail of digital evidence as it passes through different organisational levels [5]. Metadata on the method, time, place, and people who handled the data during its acquisition, processing, storage, and eventual use in investigations are all recorded by chain of custody. However, chain of custody is vulnerable to compromise if data is not retained and maintained during the life cycle of digitally recorded evidence, making it difficult to prove any situation relating to cybercrime in a court of law [6].

Digital evidence integrity relies on maintaining a verifiable chain of custody throughout an investigation. Furthermore, a chain of custody is incomplete if the evidence storage is inconsistent and unaccounted for [7]. Current systems inadequately track evidence trail and handling in a tamper-proof manner. Centralised evidence storage also poses risks of security breaches and system failures. This review examines the use of blockchain technology to strengthen the evidence chain of custody and interoperate with decentralised storage.

Research has demonstrated that blockchain can offer chain of custody immutability, and auditability [8–12]. A blockchain is a distributed database that creates a digital ledger (record) of timestamped transactions that is visible to everyone on a network [13]. Data on a blockchain are saved on a block and each block on a blockchain are linked to the previous block by the hash value. As a result of the unique feature of blockchain, application and research on blockchain is growing at an exponential rate.

Bibliometric analysis is a statistical method used to track research trends and measure academic output [14]. It was introduced by Garfield in 2007 and is used to assess the impact of research in various fields [15–17]. However, it has not yet been applied to blockchain for digital evidence chain of custody.

This paper provides a bibliometric analysis and literature review of blockchain's use in managing digital evidence chain of custody. It examines how blockchain technology can strengthen the evidential chain of custody and interoperate with actual evidence storage. The goal is to survey implementations that use blockchain to provide tamper-proof custody records and enable decentralised, verified evidence storage. The review also assesses current research, identifies gaps in knowledge, and provides direction for future research.

A literature search was conducted using Scopus, Google Scholar, and Web of Science, followed by a bibliometric analysis to investigate the relationship between article weight, content, co-occurrence, and search terms in the relevant publications. Subsequently, 58 most relevant articles were included in the systematic literature review. The study is structured into four main sections: Section 2 presents the Literature Search and Bibliometric Analysis, Sect. 3 provides a Systematic Review of the selected studies on blockchain-based chain of custody for digital evidence management, and Sect. 4 concludes the paper by summarising key findings and proposing future research directions.

2 Literature Search and Bibliometric Network

This section will introduce the literature search and bibliometric network related to the blockchain-based chain of custody. It aims to outline the research methodology and provide an overview of the interconnections and patterns within the existing body of literature in this field.

2.1 Literature Search

A review of the literature on blockchain-based chain of custody for digital evidence was conducted to answer the following research question: What is the current research on blockchain-based chain of custody for digital evidence? To find an answer, the scientific databases and search engines Scopus, Web of Science, and Google Scholar were used below. All three databases were subject to a time constraint from 2015 to the present. It was our goal to utilise both title, abstract, and keyword search queries in all three databases; however, this wasn't always feasible. It was not possible to do an abstract search on Google Scholar. Similarly, exporting search results from Google Scholar will require saving each search string individually before exporting. Also, the research results from google scholar overlapped search results already exported from Scopus and Web of Science. Therefore, we used Scopus and Web of Science to export the entire search string. Both databases required an exact-spelling search to avoid returning too many irrelevant papers. The search query returned a total of 104,324 articles from the three databases and search engines (below). The records from Scopus and Web of Science were imported into Mendeley.

Duplicates were excluded, leaving 10,134 articles to evaluate for title-based relevance. Following this preliminary screening, the remaining 2,440 articles were extracted and exported to VOSviewer for bibliometric analysis with author, title, abstract, source title, year, and volume.

2.2 Bibliometric Analysis

The bibliometric method was utilised in this study because it can objectively map out how a field's canon of literature has developed over time [18]. According to Khanra, et al. [15] a bibliometric technique is a multidisciplinary strategy for accurately charting the paths taken and areas researched as a field of study evolved. VOSviewer, an opensource tool to visualise bibliometric networks, was used to build and visualise co-occurrence networks of extracted terms from the literature. Research has shown that network visualisation is an efficient tool for analysing diverse bibliometric networks [19]; hence, it was utilised in this study.

There have been many innovative studies published because of the growing interest in blockchain technology. Numerous studies on blockchain have included a bibliometric examination of the data and trend. Zeng, et al. [20] conducted a bibliographic evaluation of blockchain-related studies between January 2011 and September 2017. Consequently, Dabbagh, et al. [21] used a bibliometric analysis to study the evolution of blockchain from 2013 to 2018. Numerous studies have also incorporated bibliometric analysis and a comprehensive literature assessment [17, 22, 23]. The bibliometric analysis in this study

combines co-occurrence, and network analysis. We developed network visualisation to analyse the links between the search phrases' co-occurrence networks [19]. The overlay visualisation was also developed for the purpose of illustrating the frequency with which a particular keyword appears in the literature (Table 1).

Table 1. The number of articles based on search terms found in each database.

Keywords	Google Scholar	Scopus	Web of Science
Blockchain-based	30,700	8,865	11,528
Blockchain and Digital Forensic	7,740	205	132
Blockchain and Digital Evidence	28,200	344	337
Blockchain Chain of Custody	6,730	78	107
Blockchain Chain of Custody Evidence	4,780	34	29
Blockchain Chain of Custody Digital Evidence	4,448	31	24
Total Number of Articles	82,610	9,557	12,157

2.3 Blockchain and Digital Forensic Bibliometric Network

The total link strength represents the number of occurrences of a set of keywords in publications [24]. If two keywords are connected, it means they appear frequently together. The numerical value of each keyword indicates the relative importance of the link between two keywords. The relatedness of keywords is determined by how close they occur together. This network of associated keywords was constructed by calculating the frequency with which related publications contain the same keywords. As a result, the proximity of two terms indicates the degree to which they are related to one another. Clusters of highly related keywords are represented in the network by a variety of colours.

The visual representation of contents' co-occurrence networks is shown in Fig. 1. Each circle in the diagram signifies a different keyword. The greater the size of a circle, the greater the number of articles that include the matching term in their keywords. Words that appear together frequently are clustered in close proximity. The keywords were categorised, and the size of the group including the word "Blockchain" was exceptionally large. The red cluster encompasses blockchain, the light green cluster is comprised of digital forensics, chain of custody, cloud forensics, electronic crime countermeasures and investigative processes. The leaf-green cluster consists of big data, GDPR, privacy, and review, while the purple cluster contains several keywords related to digital storage, security, computer crime, and decentralisation.

The network contains 347 items and 8 clusters. The total link strength is 19591. Blockchain is the largest component in the network, with a total of 346 links, 4347 strong links, and 861 occurrences, indicating that it appeared at least once in every paper analysed, making it the keyword with the most occurrences in the network. Digital forensics consists of 204 links, 902 total link strengths, and 110 occurrences. Digital storage contained 118 links, 367 total strengths, and 47 occurrences, while chain of custody contained 94 links, 241 total link strengths, and 34 occurrences.

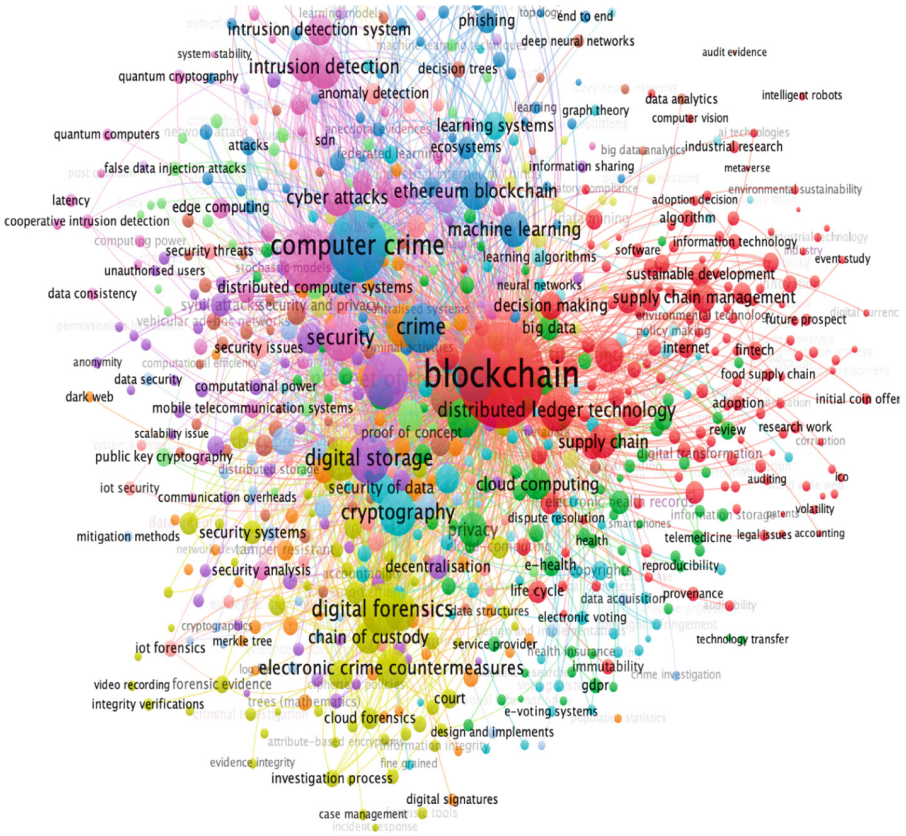

Fig. 1. Network visualisation of Blockchain for Digital Forensic.

Publication Year: The first article addressing the use of blockchain in digital evidence chain of custody was published in 2016, and the number of such publications has progressively increased since then, reaching a peak in 2021 with a total of thirty-four articles. The total number of articles published since 2016 is one hundred and three (Fig. 2).

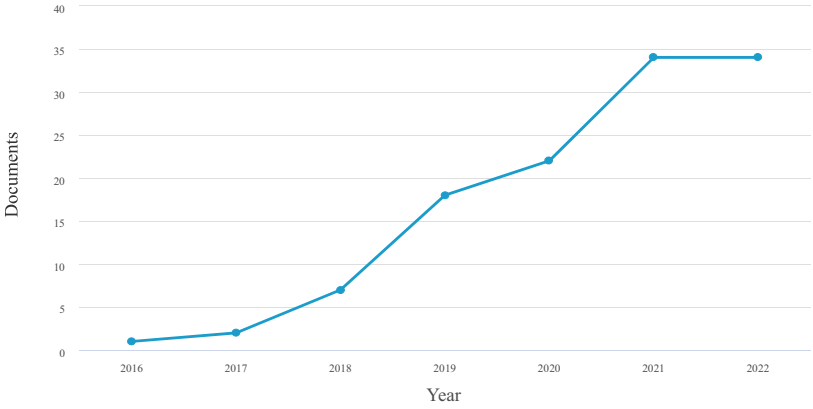

Fig. 2. Article Publication Year

Publication by Country: The paper counts from the Scopus dataset are displayed in Fig. 3, which ranks the top thirteen countries worldwide. The diversity of the countries represented on this graph demonstrates that blockchain-based chain of custody is an emerging, promising topic that is garnering interest from researchers all over the world.

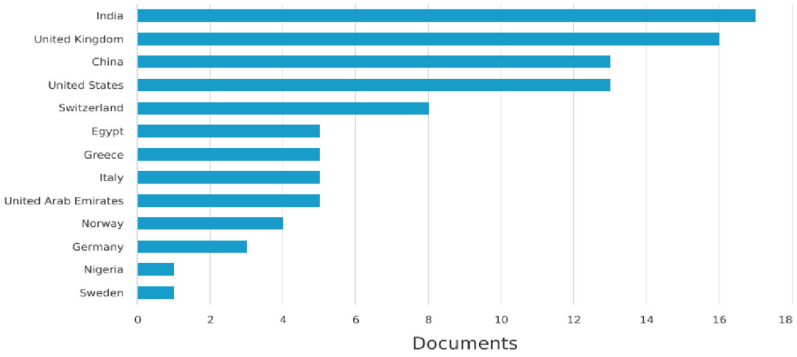

Fig. 3. Article Publication by Country

Document by Type: There have been 344 documents published for blockchain and digital evidence. 42.4% of the documents are articles. 41.5% are conference paper 4.2% are conference reviews and 8.5% are book chapters and 2.5% are review papers and one erratum paper (Fig. 4).

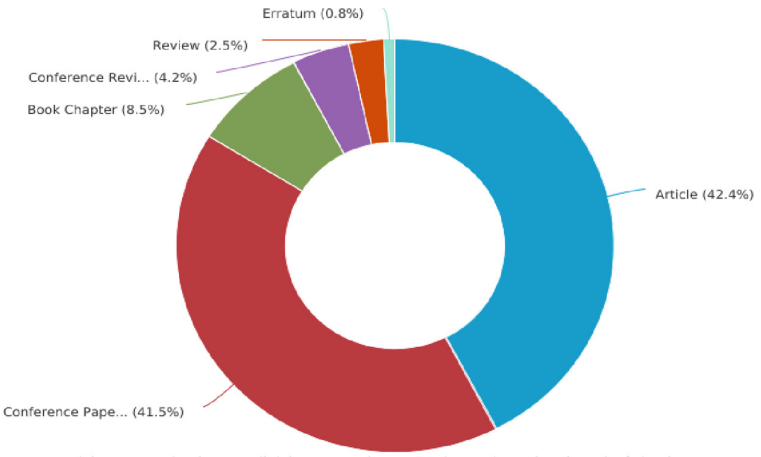

Fig. 4. Documents by source.

3 Systematic Review

Following the bibliometric analysis, the papers were reviewed in their entirety, including the abstract, method, results, and conclusion, and using the following selection criteria:

- Is there a connection between the subject of the article and the chain of custody for digital evidence?
- Is there any mention of the search phrases in the article?
- Is the study comprehensive?
- Does the study propose a blockchain-based solution for the chain of custody of digital evidence?

The final exclusion step resulted in a significant reduction of relevant articles for systematic review. Following these procedures, 58 articles were found to be applicable to the systematic review of this study.

3.1 Digital Evidence

Digital evidence encompasses any data in binary form that can serve as proof in an investigative or legal context [25, 26]. However, establishing the integrity and authenticity of digital evidence presents numerous challenges. Due to its latent and inherently volatile nature, digital evidence is susceptible to unintentional or deliberate alteration and degradation over time as technology evolves [26]. This poses threats to the reliability and admissibility of evidence.

To be admissible in court, digital evidence must be properly managed and preserved throughout its lifecycle, from initial acquisition to final disposal or destruction [27]. The digital evidence lifecycle contains various phases, including acquisition, analysis, and reporting [27, 28].

Maintaining a clear, comprehensive chain of custody is essential to verify the integrity of digital evidence as it moves between parties during an investigation [4]. Digital evidence is often handled by multiple departments and personnel, including first responders, forensic investigators, expert witnesses, law enforcement, and others [26]. The exchanges between these participants create vulnerabilities where the evidence could be unintentionally or deliberately compromised [29]. Meticulous documentation of custody transfers is therefore critical to ensure admissibility and reliability [29, 30].

Furthermore, the ephemeral properties of digital evidence raise concerns regarding integrity, authenticity, prevention of degradation, and assurance of chain of custody (Fig. 5).

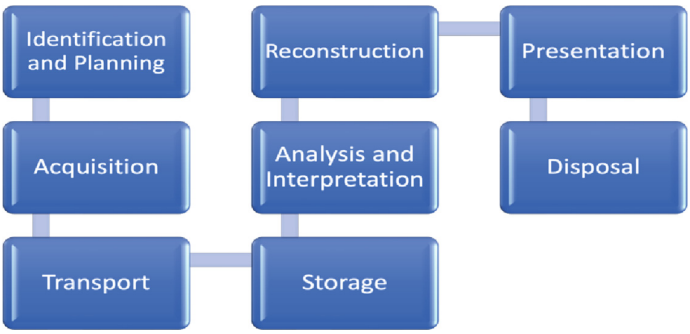

Fig. 5. Digital evidence processes [53]

3.2 Chain of Custody

Chain of custody sometimes referred to as (CoC) is a document that records sequential trail of evidence in each stage of an investigation evidence to establish provenance and authenticity [29]. For digital evidence, the chain of custody involves meticulously recording its complete lifecycle [4]. Comprehensive logs are necessary to ascertain integrity and enable admissibility. Unlike physical evidence, establishing chain of custody for inherently volatile digital artifacts presents unique challenges [30]. Phases must be comprehensively documented, incorporating, metadata and concerns about access control and security [7]. A break in the chain of custody or any questions about the authenticity or integrity of the evidence can weaken its value as evidence in a legal proceeding.

Cosic and Baca [31] proposed a digital evidence Management framework (DEMF) which aims to enhance the chain of custody of digital evidence throughout the entire process of a digital investigation. Their proposed framework made use of the SHA-2 hash function to create a digital fingerprint of the evidence, biometric traits to verify and identify the person who managed the scientific proof, a digital trusted timestamp to pinpoint the exact moment the evidence was found or was accessed, and global positioning system coordinates to pinpoint its location. Their framework comprises Five W's (and one H) in which five W represents What, Who, When, Where, Why and How.

To guarantee that digital evidence will be approved by the court, all these aspects must be used in the appropriate way to establish a safe and secure chain of custody.

The "where" of the five W's refers to the storage architecture involve in the investigation process. The storage system represents a crucial element in the effective management of digital evidence, particularly considering the voluminous nature of big data. Similar to the influence of the human factor, the storage architecture plays a crucial role in guaranteeing the security and accessibility of evidence as well as preserving the integrity of the chain of custody. As a result of this, it is imperative to improve storage systems as a preventative measure against potential threats that may inadvertently or deliberately impede the progress of an investigation.

3.3 Storage Architectures

Digital evidence storage architecture consists of technology, software, and methods for storing and managing digital evidence. The storage of digital evidence needs to be designed with the investigators' time and ability to work without being hindered by their location in mind [7]. The storage architecture for digital evidence encompasses the underlying technology, software, and protocols used to store and manage evidentiary data [32]. Digital evidence storage architectures exist across a spectrum from centralised servers to fully decentralised distributed networks. Centralised repositories simplify access control and oversight but concentrate risk in single points of failure [33, 34]. Decentralised systems enhance security through distribution but can impede holistic chain of custody views [35]. Hybrid models attempt to balance both approaches [34].

However, limitations remain with current standards alone for robust evidence custody. Centralised servers have inherent vulnerabilities while decentralised networks struggle to provide complete audit trails. This has driven interest in blockchain's tamper-proof ledgers for evidence custody management [33]. However, blockchain itself lacks native storage capacity for large evidence volumes.

An emerging solution proposes integrating decentralised storage backends with blockchain custody ledgers [35]. This allows distributing evidence across nodes for security while maintaining an immutable record of chain of custody events. This is important in evidence management, where the volume and range of digital evidence are rapidly growing, necessitating the use of flexible, scalable, and cost-effective storage systems. Decentralised storage and blockchain may fully address digital evidence security, integrity, resilience, and auditability challenges in a holistic architecture.

Subsequent sections present an overview on blockchain, blockchain's intersection with digital forensics, and a systematic review on blockchain in chain of custody for digital evidence. The literature review examines current research and open issues in unifying decentralised storage systems with blockchain for comprehensive digital evidence custody. A critical analysis of current research and implementations will reveal remaining gaps and opportunities to realise this promising convergence.

3.4 Blockchain Technology: Key Principles and Characteristics

Blockchain is a distributed ledger technology (DLT) that allows for synchronised sharing of data across multiple nodes [13]. This decentralised network reduces reliance on a

single authoritative entity and increases data availability and resilience against single points of failure [36, 37].

One of the key features of blockchain is its ability to ensure data immutability. Once transactions are added to the chain through consensus, it becomes nearly impossible to alter their contents due to the cryptographic chaining of blocks [38]. This immutability provides a transparent and auditable transaction history.

Consensus algorithms, such as Proof-of-Work, Proof-of-Stake, etc., drive transaction validation and block creation within the blockchain [39]. These mechanisms ensure agreement among network nodes on the validity of transactions and prevent double-spending attacks. A network that is based on consensus ensures that every node has access to the same information. A consensus algorithm performs two functions: it ensures that the data on the ledger is the same for all the nodes in the network, which, in turn, prevents malevolent actors from manipulating the data; and it reaches a conclusion about what the data should be [13]. This precludes manipulation or unauthorised alteration of the blockchain, as any changes to the data would require consensus from the network. Guo, et al. [40] framework is grounded in post-Quantum theory, which protects the blockchain against outside attacks while also preserving its verifiability. The authors also used pre-image sampling process to produce secret keys that can be used to select a random value and sign the message. In addition, the consensus process can contribute to the blockchain's transparency and auditability by maintaining an immutable ledger of all transactions. This is particularly useful in the context of digital evidence chain of custody because it allows for straightforward tracking and tracing of the evidence's movement and management.

Consensus algorithm differs depending on the implementation of the blockchain being used [39] and the choice of consensus algorithm used will rely on the system's requirements, including security, efficiency, scalability, and cost. An analysis on consensus algorithms and their differences were highlighted in [39]. Proof of Work is the algorithm used in Bitcoin to achieve a consensus on the blockchain. However, other blockchain technologies use a wide variety of consensus algorithms [39], such as Proof of Stake, Proof of Burn, Practical Byzantine Fault Tolerance (PBFT), Proof of Elapsed Time, and a great number of others, depending on the specific requirements that they have.

Blockchain's versatility also includes the use of smart contracts, self-executing agreements with terms written directly into code. These digital protocols increase efficiency by automatically triggering actions when predefined conditions are met, eliminating the need for intermediaries [41]. Smart contracts operate on the simple rules "if, when, and then…" phrases that are encoded in the blockchain. Before smart contracts can be executed on the blockchain, they must be written with specific needs and specifications, including code, rules, objects, and data models [42]. A network of computers performs the actions at the time when pre-agreed conditions and rules have been verified and accomplished. These conditions and rules might comprise transfer of digital evidence to relevant participants, notification sending, and/or transfer of evidence ownership. Once a smart contract has been activated and carried out, the contract itself cannot be cancelled or erased from the blockchain once it has been recorded there [42]. Smart contracts will run, authenticate, and construct calls accordingly in the decentralised records without

altering or amending the transactions itself. The blockchain is automatically updated whenever a transaction is successfully completed, and the participants will also be able to exchange, visualise data, information, and interact automatically without the need for an intermediary or time loss and the results of the implementation can be checked by authorised participant in the blockchain network (Table 2).

Table 2. Categories of Blockchain [36, 43]

Category	Definition
Public Blockchain	Anyone in the network can contribute and access information
Private Blockchain	Only one person or organisation has access to it
Consortium Blockchain	Only accessible to specified groups of people inside an organisation and, allows only authorised users to access the network and view data based on predefined permissions

Blockchain Frameworks, Features and Suitability for Chain of Custody: Public blockchains like Ethereum allow transparency and immutable custody records viewable by all participants [9]. Ethereum's native support for self-executing smart contracts enables reliable evidence handling rules and audit trails across open decentralised networks. However, public chains lack access controls and mechanisms to restrict sensitive forensic data, which could impede adoption.

Private blockchain architectures address these gaps through permissions and selective data sharing. Hyperledger Fabric utilises private channels, modular consensus, and membership services to conduct confidential custody transactions between authorised participants via chaincode contracts [37, 44]. Similarly, Corda propagates evidence exchange only between parties with a need to know [37].

Multichain facilitates interoperability between multiple private chains, allowing segmented custody trails across entities while preventing unauthorised access. These capabilities enhance privacy, throughput, and governance compared to fully public chains [45].

Hybrid approaches like Kadena bridge public verifiability and private data management [46]. The public chain provides transparent immutable records while its Kuro chain enables private smart contracts and restricted evidence access. Its partitioned architectures allow customisable security and performance based on use case needs [46].

In conclusion, the blockchain framework chosen for chain of custody should ensure privacy and non-repudiation while seamlessly interoperating with existing storage architectures that constitute the complete digital forensic processes for evidence management.

3.5 Blockchain's Intersection with Digital Forensics

This subsection highlights the potential synergistic alignment of blockchain technology with digital forensics, focusing on how blockchain's salient characteristics may engender a paradigm shift in current methodologies and offer cogent solutions to existing digital forensic challenges especially with digital evidence management.

Digital forensics involves identifying, extracting, and analysing digital evidence from electronic devices and systems for legal or investigative purposes [47]. It plays a critical role in law enforcement and cybersecurity, allowing organisations to identify and prosecute cybercriminals and protect against security threats [11]. The field has evolved rapidly with the widespread use of electronic devices [6, 48]. A key challenge is ensuring the integrity and authenticity of digital evidence, which can be volatile and easily altered [33, 49]. Stakeholders must follow established protocols to properly collect, preserve, and analyse evidence while being aware of legal and ethical considerations [7, 50]. In lieu of this, a system that guarantees accuracy, accessibility, privacy, and integrity of digital evidence is needed.

Blockchain's immutability generates a permanent record of digital evidence trails, ensuring authenticity from acquisition to its final disposition [33]. Integration of smart contracts can transform process automation, improving efficiency and reliability [51]. Blockchain's inherent transparency can bolster traceability of digital evidence, allowing authorised participants to audit interactions and validate evidence authenticity [38].

3.6 Blockchain in Chain of Custody for Digital Evidence

Blockchain is a focal solution where trust is lacking due to its transparency and traceability feature. Areas that have been researched includes Governance, finance sector, health, supply chains management, and digital forensics [52–54]. A blockchain-based evidence log keeps track of information such as the description of the evidence, its identification, the names of the creators, and the ownership history of the evidence [9]. The majority of previous research and studies on blockchain-based chain of custody propose a chain of custody system in which the evidence metadata is stored on the blockchain while the actual evidence is held on a different medium and is accessible to only permissioned participants [9, 33, 34, 55]. This is primarily because the evidence may be too large to be stored efficiently on a blockchain. The authors Bonomi, et al. [9] also explained that if the evidence is stored on a blockchain it will make it accessible to every node on the Blockchain. The sensitivity of chain of custody data restricts its disclosure to the public (unauthorised individuals), as doing so would compromise the confidentiality and privacy attributes that evidence data and trails should hold.

Research from Bonomi, et al. [9] and Lone and Mir [56] presented a chain of custody system based on a public Ethereum. In addition to the fact that creating a system on a public blockchain is costly, there is also the absence of privacy and confidentiality. Public blockchains are open and transparent, allowing anybody with an internet connection to access the blockchain's transactions. This may not be suitable for sensitive and confidential data, such as a digital evidence trail, as it may expose sensitive information to unauthorised individuals.

The authors [56] proposed another blockchain based chain of custody solution "Forensic-Chain" [33] based on permissioned Hyperledger Composer. In their system, system allows members' identities and roles to be known to other network members and is controlled by a consensus mechanism and a peer-to-peer network. The framework is made up of three components: a digital witness, a digital custodian, and a law enforcement organisation. A consensus mechanism is established to guard against system sabotage, and public-key cryptography is employed to uniquely identify all entities within the framework.

Ahmad, et al. [12] took the research a step further by proposing a prototype based on private Ethereum and introduced the concept of smart lock to link and secure access to the location of the physical evidence. Their framework uses predefined smart contracts to activate the smart locks in order to restrict and grant access to evidence. Tian, et al. [34] propose a blockchain-based digital evidence framework (Block-DEF) against file tampering. Their paper focuses on digital evidence security against file tampering that uses a multi-signature method that includes non-random and certificated key pairs for submitting and retrieving evidence. As opposed to the evidence framework proposed by Bonomi, et al. [9] the evidence in Block-DEF [34] must first be temporarily stored with its name and public key before establishing its validity.

Li, et al. [57] proposed LeChain, a system based on Ethereum blockchains and Proof of Authority as the consensus mechanism to record evidence trails and voting system to keep the jury anonymous. The system is intended to ensure the traceability of evidence while also protecting identities of witnesses and jurors. The authors employed Ciphertext Policy-Based Encryption (CP-ABE) to authenticate evidence access. CPABE is a form of encryption that enables users to selectively encrypt data depending on a set of predetermined policies [58]. These regulations specify who has access to encrypted data and under what circumstances. Furthermore, Lechain [57] used a short randomizable signature to authenticate the witness's identity. Additionally, their prototype aimed to address the issue of insider threats by invoking the access permissions of identified malicious participants.

Burri, et al. [59] study builds on their previous work [60] which used a trusted entity to improve e-Chain of Custody and public blockchain to safeguard specific blocks. They recommend that a private ledger be used to track chain of custody data, and the state of the private e-CoC ledger is frequently updated into a public blockchain. This according to the authors was to secure the trusted entity and ensure integrity of the data. Burri, et al. [59] framework for implementing a private blockchain hosted by a trusted institution is identical to the framework proposed by Ahmad, et al. [12] except that Ahmad, et al. [12] also propose installing smart locks to authenticate and authorise access for a requesting participant.

Khan, et al. [44] proposed the MF-Ledger, based on the Hyperledger Sawtooth framework, to form a private network for participants to communicate and decide on investigative activities before storing evidence metadata on a blockchain. The system incorporated smart contracts to authenticate access and focused on tracking and managing multimedia evidence. In a subsequent research [61], they designed a wireless

IoT-blockchain-enabled video surveillance chain of custody and evidence storage system, built on Hyperledger Sawtooth, that proposed storing actual evidence in IPFS, a decentralised storage system.

3.7 Existing Frameworks and Methodology

This subsection provides an overview of the blockchain frameworks, consensus mechanisms, and storage architectures employed in the existing literature on blockchain-based chain of custody. It aims to highlight the current methodologies and technologies used, thereby offering a comprehensive understanding of the prevailing trends and potential gaps in this research area.

Blockchain Frameworks Utilised: The surveyed literature employed a variety of blockchain frameworks, including permissioned, private, and consortium blockchains. Ethereum was used in 35% of the papers for experimental and analytical purposes. Despite the cost associated with using public Ethereum for experimentation, its ease of use justifies the expense. However, this necessitates a consideration of the trade-off between privacy and ease of use (Table 3).

Table 3. Blockchain frameworks

Framework	Reference	Year Framework was Introduced
DigiByte	[60]	2013
Ethereum (Private/Public)	[8, 9, 12, 56, 57, 62, 63]	2015
Hyperledger Composer	[33, 64]	2015 but declared end of life by August 2019
Hyperledger Sawtooth	[44, 61]	2015
Undisclosed Hyperledger Project	[65]	N/A
Unspecified	[10, 11, 30, 55, 59, 66, 67]	N/A

Consensus Mechanisms Utilised: The choice of consensus mechanism is largely contingent on the blockchain framework employed. Much of the current research on blockchain for digital evidence chain of custody is theoretical rather than experimental. As result, nearly half of the studies reviewed did not specify which consensus mechanisms they employed. Further practical testing is needed to evaluate different consensus algorithms within blockchain frameworks for digital evidence CoC and management. Identifying optimal mechanisms tailored to forensic needs will strengthen these conceptual models as they transition to implementation (Table 4).

Table 4. Consensus Mechanisms

Consensus Mechanism	Reference
Practical Byzantine Fault Tolerance (PBFT)	[9, 44]
Proof-of-Authority (PoA)	[57]
Proof of Work (PoW)	[60–62, 66]
Raft	[12]
Zero-Knowledge Proof (ZKP)	[63]
Unspecified	[8, 10, 11, 30, 33, 55, 56, 59, 64, 65, 67]

Storage Architectures Utilised: While blockchain technology has been proposed as a potential solution for storing evidence metadata and tracking chain of custody, the majority of research has not addressed the method for the actual storage of the evidence. The digital evidence management's storage architecture is a critical area needing more focus and presents a clear opportunity for future research. The chain of custody is intrinsically linked to this storage architecture, and its comprehensiveness can only be asserted when this connection is established.

Digital forensics processes play a crucial role in managing digital evidence. Standard procedures for collection, analysis, and preservation of digital evidence are paramount to ensure its authenticity and admissibility. Strict adherence to forensic best practices is essential, as any deviation could potentially undermine the admissibility and credibility of the evidence (Table 5).

Table 5. Storage Architectures

Storage Architecture	Reference	Paper year of publication
Filecoin	[44]	2021
Google Storage Codeline	[63]	2023
IPFS	[61, 62]	2021, 2022
Undisclosed Decentralised system	[57]	2021
Unspecified	[8–12, 30, 33, 55, 56, 59, 60, 64–67]	N/A

3.8 Open-Ended Issues

Blockchain technology is a relatively new field, and literature and research on blockchain-based chains of custody are still in their early stages, with gaps and room for future work. The papers evaluated above utilised various blockchain solutions available at the time to create a path for future research into digital evidence chain of custody and blockchain.

Digital forensics relies on the integrity of digital evidence, which is safeguarded by the method of chain of custody. The complexity and volume of digital evidence have further exacerbated the challenges of chain of custody management.

The surveyed papers propose various blockchain architectures and protocols to log custody transactions, verify integrity, and ensure provenance of digital evidence [10, 30, 33]. Key functionalities include cryptographic hashing for tamper-proofing, timestamping events, and enabling decentralised access control and verification. Both public and private blockchain configurations have been considered.

However, a clear approach for evidentiary file storage, either on-chain or off-chain, is not consistently defined. A few studies hint at using the InterPlanetary File System (IPFS) for distributed storage [61, 62] without offering in-depth implementation specifics. The choice of storage mechanisms directly affects scalability, privacy, and associated costs.

A few studies have provided more specifics on storage. For instance, Burri, et al. [59] propose storing hashed metadata on-chain while keeping the data files off-chain. Tian, et al. [34] describe a dual-chain architecture with a public chain storing hashes and permissions and a private chain holding the evidence. However, even in these cases, the exact storage systems and infrastructure are ambiguous.

Future studies should explore user perceptions and acceptance of blockchain-based digital evidence management systems and strive to establish a standardised regulatory framework and best practices in compliance with existing law. A thorough understanding of constraints and potential solutions for storage interoperability, privacy, system scalability, and performance are essential. Addressing these challenges successfully could significantly improve the usefulness of blockchain technology in managing digital evidence.

4 Conclusion

This research emphasises the crucial role of chain of custody in preserving the integrity of digital evidence in digital forensics. Current systems face challenges due to the high volume of digital evidence, insider threats, and security vulnerabilities.

This study's bibliometric analysis indicates that blockchain technology may offer a promising solution. The systematic review further highlights its potential for creating an auditable, and transparent ledger system for managing digital evidence. However, further research is needed to address the challenges and limitations of blockchain-based chain of custody, including the development of practical and scalable solutions for blockchain interoperability with existing storage architectures.

Additionally, more research is required to ensure that the storage architecture holding evidence is properly integrated into the blockchain-based chain of custody, covering the entire lifecycle of evidence.

References

1. Business-Wire: UK's Cleveland Police Selects NICE Investigate for Digital Evidence Management Process Transformation in the Cloud. https://www.businesswire.com/news/home/20201014005424/en/UK%E2%80%99s-Cleveland-Police-Selects-NICE-Investigate-for-Digital-Evidence-Management-Process-Transformation-in-the-Cloud. Accessed

2. Rao, S., Fernandes, S., Raorane, S., Syed, S.: A novel approach for digital evidence management using blockchain (2020)
3. Granja, F.M., Rafael, G.D.R.: The preservation of digital evidence and its admissibility in the court. Int. J. Electron. Secur. Digit. Forensics **9**(1), 1–18 (2017)
4. Sadiku, M.N.O., Shadare, A.E., Musa, S.M.: Digital chain of custody. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **7**(7), 117 (2017)
5. Ali, M., Ismail, A., Elgohary, H., Darwish, S., Mesbah, S.: A procedure for tracing chain of custody in digital image forensics: a paradigm based on grey hash and blockchain. Symmetry **14**(2) (2022)
6. Losavio, M.M., et al.: The juridical spheres for digital forensics and electronic evidence in the insecure electronic world. Wiley Interdisc. Rev. Forensic Sci. **1**(5), e1337 (2019)
7. Prayudi, Y., Ashari, A., Priyambodo, T.K.: The framework to support the digital evidence handling. J. Cases Inf. Technol. **22**(3) (2020)
8. Tsai, F.-C.: The application of blockchain of custody in criminal investigation process. Procedia Comput. Sci. **192**, 2779–2788 (2021)
9. Bonomi, S., Casini, M., Ciccotelli, C.: B-CoC: a blockchain-based chain of custody for evidences management in digital forensics (2018)
10. Yan, W., Shen, J., Cao, Z., Dong, X.: Blockchain based digital evidence chain of custody. Presented at the Proceedings of the 2020 The 2nd International Conference on Blockchain Technology (2020)
11. Al-Khateeb, H., Epiphaniou, G., Daly, H.: Blockchain for modern digital forensics: the chain-of-custody as a distributed ledger. In: Jahankhani, H., Kendzierskyj, S., Jamal, A., Epiphaniou, G., Al-Khateeb, H. (eds.) Blockchain and Clinical Trial. ASTSA, pp. 149–168. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-11289-9_7
12. Ahmad, L., Khanji, S., Iqbal, F., Kamoun, F.: Blockchain-based chain of custody: towards real-time tamper-proof evidence management. In: Proceedings of the 15th International Conference on Availability, Reliability and Security (2020)
13. Sheth, H., Dattani, J.: Overview of blockchain technology. Asian J. Convergence Technol. (AJCT) (2019). ISSN-2350-1146
14. Iqbal, W., Qadir, J., Tyson, G., Mian, A.N., Hassan, S.-U., Crowcroft, J.: A bibliometric analysis of publications in computer networking research. Scientometrics **119**, 1121–1155 (2019)
15. Khanra, S., Dhir, A., Mäntymäki, M.: Big data analytics and enterprises: a bibliometric synthesis of the literature. Enterp. Inf. Syst. **14**(6), 737–768 (2020)
16. Tandon, A., Kaur, P., Mäntymäki, M., Dhir, A.: Blockchain applications in management: a bibliometric analysis and literature review. Technol. Forecast. Soc. Change **166** (2021)
17. Lawal, I.A., Klink, M., Ndungu, P., Moodley, B.: Brief bibliometric analysis of "ionic liquid" applications and its review as a substitute for common adsorbent modifier for the adsorption of organic pollutants. Environ. Res. **175**, 34–51 (2019)
18. Xue, X., Wang, L., Yang, R.J.: Exploring the science of resilience: critical review and bibliometric analysis. Nat. Hazards **90**, 477–510 (2018)
19. Tran, B.X., et al.: The current research landscape of the application of artificial intelligence in managing cerebrovascular and heart diseases: a bibliometric and content analysis. Int. J. Environ. Res. Public Health **16**(15) (2019)
20. Zeng, S., Ni, X., Yuan, Y., Wang, F.-Y.: A bibliometric analysis of blockchain research, pp. 102–107. IEEE (2018)
21. Dabbagh, M., Sookhak, M., Safa, N.S.: The evolution of blockchain: a bibliometric study. IEEE Access **7**, 19212–19221 (2019)
22. Ante, L.: Smart contracts on the blockchain–a bibliometric analysis and review. Telematics Inform. **57**, 101519 (2021)

23. Bertoglio, R., Corbo, C., Renga, F.M., Matteucci, M.: The digital agricultural revolution: a bibliometric analysis literature review. IEEE Access **9** (2021)
24. Guo, Y.-M., Huang, Z.-L., Guo, J., Li, H., Guo, X.-R., Nkeli, M.J.: Bibliometric analysis on smart cities research. Sustainability **11**(13) (2019)
25. Swgde, I.: Digital evidence: standards and principles. Forensic science. Digital Evidence: Standards and Principles. Forensic Science Communications, A—pill (2000). https://www.swgde.org/home
26. Horsman, G.: ACPO principles for digital evidence: time for an update? Forensic Sci. Int. Rep. **2** (2020)
27. Berghs, S., Morrison, G.S., Goemans-Dorny, C.: Electronic evidence: challenges and opportunities for law enforcement. In: Biasiotti, M.A., Mifsud Bonnici, J.P., Cannataci, J., Turchi, F. (eds.) Handling and Exchanging Electronic Evidence Across Europe. LGTS, vol. 39, pp. 75–123. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-74872-6_6
28. Biasiotti, M.A.: A proposed electronic evidence exchange across the European Union. Digit. Evid. Elec. Signature L. Rev. **14**, 1 (2017)
29. Shah, M., Saleem, S., Zulqarnain, R.: Protecting digital evidence integrity and preserving chain of custody. J. Digit. Forensics Secur. Law (2017)
30. Chopade, M., Khan, S., Shaikh, U., Pawar, R.: Digital forensics: maintaining chain of custody using blockchain, pp. 744–747. IEEE (2019)
31. Cosic, J., Baca, M.: A framework to (Im) Prove "Chain of Custody" in digital investigation process. In: Central European Conference on Information and Intelligent Systems 2010, p. 435. Faculty of Organization and Informatics Varazdin (2010)
32. Prayudi, Y., Ashari, A., Priyambodo, T.K.: Digital evidence cabinets: a proposed framework for handling digital chain of custody. Int. J. Comput. Appl. **107**(9) (2014)
33. Lone, A.H., Mir, R.N.: Forensic-chain: blockchain based digital forensics chain of custody with PoC in Hyperledger composer. Digit. Investig. **28**, 44–55 (2019)
34. Tian, Z., Li, M., Qiu, M., Sun, Y., Su, S.: Block-DEF: a secure digital evidence framework using blockchain. Inf. Sci. **491**, 151–165 (2019)
35. Kumar, R., Tripathi, R.: Implementation of distributed file storage and access framework using IPFS and blockchain. In: Fifth International Conference on Image Information Processing (ICIIP), pp. 246–251. IEEE (2019)
36. Yaga, D., Mell, P., Roby, N., Scarfone, K.: Blockchain technology overview (NISTIR-8202), NIST: National Institute of Standards and Technology (2018)
37. Ramadoss, R.: Blockchain technology: an overview. IEEE Potentials **41**(6), 6–12 (2022)
38. Comert, O.: Blockchain revolution: how the technology behind bitcoin and other cryptocurrencies is changing the world (2020)
39. Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., Qijun, C.: A review on consensus algorithm of blockchain (2017)
40. Guo, R., Shi, H., Zhao, Q., Zheng, D.: Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. IEEE Access **6** (2018)
41. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the internet of things. IEEE Access **4** (2016)
42. Hewa, T., Ylianttila, M., Liyanage, M.: Survey on blockchain based smart contracts: applications, opportunities and challenges. J. Netw. Comput. Appl. **177** (2021)
43. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: architecture, consensus, and future trends (2017)
44. Khan, A.A., Uddin, M., Shaikh, A.A., Laghari, A.A., Rajput, A.E.: MF-ledger: blockchain hyperledger sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture. IEEE Access **9** (2021)
45. Ismail, S., Reza, H., Zadeh, H.K., Vasefi, F.: A blockchain-based IoT security solution using multichain (2023)

46. Martino, W.: The first scalable, high performance private blockchain. Revision v1. 0 (2016)
47. Alruwaili, F.F.: CustodyBlock: a distributed chain of custody evidence framework. Information (2021)
48. Reedy, P.: Interpol review of digital evidence 2016–2019. Forensic Sci. Int. Synerg. **2** (2020)
49. Arshad, H., Jantan, A.B., Abiodun, O.I.: Digital forensics: review of issues in scientific validation of digital evidence. J. Inf. Process. Syst. (2018)
50. Watney, M.M.: Cross-border law enforcement: Gathering of stored electronic evidence. J. Inf. Warfare (2016)
51. Mougayar, W.: The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley (2016)
52. Baldi, A.M., Celestrini, J.R., Andreão, R.V., Mota, V.F.S., Santos, C.A.S.: A blockchain approach for eHealth situation-aware data processing (2022)
53. Caro, M.P., Ali, M.S., Vecchio, M., Giaffreda, R.: Blockchain-based traceability in Agri-Food supply chain management: a practical implementation. Presented at the 2018 IoT Vertical and Topical Summit on Agriculture - Tuscany (IOT Tuscany) (2018)
54. Chakrabarti, A., Chaudhuri, A.K.: Blockchain and its scope in retail. Int. Res. J. Eng. Technol. (2017)
55. Xiong, Y., Du, J.: Electronic evidence preservation model based on blockchain. Presented at the Proceedings of the 3rd International Conference on Cryptography, Security and Privacy - ICCSP 2019 (2019)
56. Lone, A.H., Mir, R.N.: Forensic-chain: Ethereum blockchain based digital forensics chain of custody. Sci. Pract. Cyber Secur. J. (2018)
57. Li, M., Lal, C., Conti, M., Hu, D.: LEChain: a blockchain-based lawful evidence management scheme for digital forensics. Futur. Gener. Comput. Syst. **115**, 406–420 (2021)
58. Zhang, S., Li, L., Chang, L., Gu, T., Liu, H.: A ciphertext-policy attribute-based encryption based on multi-valued decision diagram. In: Intelligent Information Processing IX: 10th IFIP TC 12 International Conference, IIP (2018)
59. Burri, X., Casey, E., Bollé, T., Jaquet-Chiffelle, D.-O.: Chronological independently verifiable electronic chain of custody ledger using blockchain technology. Forensic Sci. Int. Digit. Investig. **33** (2020)
60. Jaquet-Chiffelle, D.-O., Casey, E., Bourquenoud, J.: Tamperproof timestamped provenance ledger using blockchain technology. Forensic Sci. Int. Digit. Invest. **33** (2020)
61. Khan, A.A., Shaikh, A.A., Laghari, A.A.: IoT with multimedia investigation: a secure process of digital forensics chain-of-custody using blockchain hyperledger sawtooth. Arab. J. Sci. Eng., 1–16 (2022)
62. Durga, S., Daniel, E., Deepakanmani, S., Neeba, T.M., Ravi, V.: Blockchain-based privacy preservation technique for digital forensics records. In: Artificial Intelligence and Blockchain in Digital Forensics, pp. 211–229. River Publishers (2023)
63. Santamaría, P., Tobarra, L., Pastor-Vargas, R., Robles-Gómez, A.: Smart contracts for managing the chain-of-custody of digital evidence: a practical case of study. Smart Cities **6**(2), 709–727 (2023)
64. Rajasekar, V., Sathya, K., Velliangiri, S., Karthikeyan, P.: Blockchain-based identity management systems in digital forensics. In: Artificial Intelligence and Blockchain in Digital Forensics, pp. 241–259. River Publishers (2023)
65. López-Aguilar, P., Solanas, A.: An effective approach to the cross-border exchange of digital evidence using blockchain. In: Saponara, S., De Gloria, A. (eds.) Applications in Electronics Pervading Industry, Environment and Society. LNEE, vol. 866, pp. 132–138. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-95498-7_19

66. Chougule, H., Dhadiwal, S., Lokhande, M., Naikade, R., Patil, R.: Digital evidence management system for cybercrime investigation using proxy re-encryption and blockchain. Procedia Comput. Sci. **215**, 71–77 (2022)
67. Akhtar, M.S., Feng, T.: Using blockchain to ensure the integrity of digital forensic evidence in an IoT environment. EAI Endorsed Trans. Creative Technol. **9**(31), e2 (2022)