electronics

MDPI

*Review*

# Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions

**Hany F. Atlam [1,*], Ndifon Ekuri [2], Muhammad Ajmal Azad [3] and Harjinder Singh Lallie [1]**

[1] Cyber Security Centre, WMG, University of Warwick, Coventry CV4 7AL, UK; hl@warwick.ac.uk
[2] School of Computing and Engineering, University of Derby, Derby DE22 3AW, UK; ekurindifon@gmail.com
[3] School of Computing, Birmingham City University, SteamHouse, Belmont Row, Birmingham B4 7RQ, UK; muhammadajmal.azad@bcu.ac.uk
* Correspondence: hany.atlam@warwick.ac.uk

**Abstract:** Blockchain technology has gained significant attention in recent years for its potential to revolutionize various sectors, including finance, supply chain management, and digital forensics. While blockchain's decentralization enhances security, it complicates the identification and tracking of illegal activities, making it challenging to link blockchain addresses to real-world identities. Also, although immutability protects against tampering, it introduces challenges for forensic investigations as it prevents the modification or deletion of evidence, even if it is fraudulent. Hence, this paper provides a systematic literature review and examination of state-of-the-art studies in blockchain forensics to offer a comprehensive understanding of the topic. This paper provides a comprehensive investigation of the fundamental principles of blockchain forensics, exploring various techniques and applications for conducting digital forensic investigations in blockchain. Based on the selected search strategy, 46 articles (out of 672) were chosen for closer examination. The contributions of these articles were discussed and summarized, highlighting their strengths and limitations. This paper examines the selected papers to identify diverse digital forensic frameworks and methodologies used in blockchain forensics, as well as how blockchain-based forensic solutions have enhanced forensic investigations. In addition, this paper discusses the common applications of blockchain-based forensic frameworks and examines the associated legal and regulatory challenges encountered in conducting a forensic investigation within blockchain systems. Open issues and future research directions of blockchain forensics were also discussed. This paper provides significant value for researchers, digital forensic practitioners, and investigators by providing a comprehensive and up-to-date review of existing research and identifying key challenges and opportunities related to blockchain forensics.

**Keywords:** blockchain; digital forensics; blockchain forensics; blockchain-based forensic framework; systematic literature review

check for updates

**Citation:** Atlam, H.F.; Ekuri, N.; Azad, M.A.; Lallie, H.S. Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions. *Electronics* **2024**, *13*, 3568. https://doi.org/10.3390/electronics13173568

Academic Editors: Dimitrios G. Kogias, Panagiotis A. Karkazis and Michael G. Xevgenis

Received: 22 July 2024
Revised: 4 September 2024
Accepted: 6 September 2024
Published: 8 September 2024

## 1. Introduction

Blockchain has emerged as one of the most revolutionary advancements of the digital age, transforming a multitude of domains with its unique attributes of decentralization, immutability, and transparency. It was originally regarded as the underlying technology for Bitcoin; however, blockchain has rapidly expanded beyond cryptocurrencies to impact industries such as finance, supply chain management, healthcare, and many others [1]. Its ability to create secure and tamper-proof ledgers ensures data integrity and trust without the need for intermediaries, which reduces costs and increases efficiency. As a foundational technology, blockchain's influence is expanding, promising to redefine trust, security, and efficiency in the digital age [2].

While blockchain offers numerous advantages across various domains, it brings security and forensic challenges. The anonymous nature of blockchain transactions complicates the identification of individuals involved in illegal activities. The decentralized and immutable characteristics of blockchain also make it difficult to alter or remove fraudulent or malicious transactions once they are recorded, posing a unique set of challenges for investigators attempting to trace and rectify such actions [3]. Furthermore, the global and borderless nature of blockchain networks means that illegal activities can span multiple jurisdictions, complicating legal processes and international cooperation. The complexity of blockchain protocols and the rapid development of new blockchain-based technologies, such as privacy coins and Decentralized Finance (DeFi) platforms, introduce additional layers of difficulty in monitoring and investigating suspicious activities [4].

Traditional digital forensic frameworks are inadequate for handling blockchain investigations due to the distinct challenges posed by blockchain. Unlike conventional systems where data can be centrally accessed and manipulated, blockchain's decentralized nature means that data are distributed across a vast network of nodes, making it difficult to isolate and analyse. The anonymity of blockchain transactions further complicates the identification of individuals involved in illegal activities, as addresses and transactions do not inherently link to real-world identities [5]. Also, the immutable characteristic of blockchain poses a challenge for forensic investigators adapted to the possibility of recovering deleted files or analysing logs for traces of manipulation. Additionally, the rapid evolution of blockchain protocols and the emergence of complex features like smart contracts and privacy coins add another layer of complexity, requiring specialized tools and expertise that traditional frameworks lack [6].

Blockchain forensics is a critical field that addresses the unique challenges posed by blockchain in digital forensic investigations. The decentralized, immutable, and anonymous nature of blockchain transactions makes traditional forensic techniques inadequate for tracing illegitimate activities and securing digital evidence. To combat these challenges, effective frameworks that utilize blockchain-based forensic solutions should be used. These solutions offer significant benefits in the digital forensic investigation of various domains by leveraging the inherent strengths of blockchain technology, such as transparency, immutability, and decentralization. These solutions enhance the integrity and reliability of digital evidence by ensuring that once data are recorded on the blockchain, it cannot be altered or deleted, thereby preserving a tamper-proof chain of custody. This immutability is crucial for maintaining the credibility of evidence in legal proceedings. Additionally, the transparent nature of blockchain allows for real-time verification and auditing of transactions, making it easier to trace and link illegal activities across different platforms [7,8].

This paper aims to provide a comprehensive systematic literature review that follows the PRISMA 2020 protocol designed by Page et al. [9], which investigates and evaluates state-of-the-art studies in blockchain forensics, a crucial field in digital forensics that addresses the unique challenges posed by blockchain. The primary objective of this paper is to systematically identify, evaluate, and summarize the current state of research in blockchain forensics. This involves a thorough review of the literature to capture recent advancements, methodologies, and frameworks used in the field. By synthesizing findings from various studies, this paper aims to provide a comprehensive overview of how blockchain forensics has evolved and the contributions of different research efforts. Another key objective is to assess the various digital forensic frameworks and methodologies employed specifically in blockchain contexts, as well as evaluate the impact of blockchain-based forensic solutions on digital forensic investigations. Based on the selected search strategy, 46 articles (out of 672) were chosen for closer examination. The contributions of these articles were discussed and summarized, highlighting their strengths and limitations. This paper conducts a comprehensive review of selected literature to identify various digital forensic frameworks and methodologies employed in blockchain forensics. It also assesses how blockchain-based forensic solutions have contributed to the advancement of digital forensic investigations. Furthermore, this paper highlights the common applications of blockchain-based forensic frameworks and explores the legal and regulatory challenges encountered in conducting forensic investigations within blockchain systems. Open issues and future research directions of blockchain forensics are also discussed.

The contribution of this paper can be summarized as follows:

- Investigating and reviewing recent and state-of-the-art studies on blockchain forensics by highlighting the merits and limitations of each study.
- Identifying diverse digital forensic investigation frameworks and methodologies used in blockchain forensics.
- Determining common applications of blockchain-based digital forensic investigation frameworks across various domains.
- Identifying legal and regulatory challenges encountered in conducting forensic investigations on blockchain systems.
- Presenting open issues and future research directions of blockchain forensics.

The rest of this paper is organised as follows. Section 2 presents an overview of blockchain forensics; Section 3 describes the research methodology used to produce this systematic literature review; Section 4 describes the analysis of the data; Section 5 describes how this systematic review answers the research questions; Section 6 presents open issues and future research directions; and Section 7 is the conclusion.

## 2. An Overview of Blockchain Forensics

This section provides an overview of blockchain forensics. It starts by presenting the fundamentals of blockchain technology and its main components, then discusses digital forensics and the investigation lifecycle, and finally, discusses blockchain forensics and its investigation lifecycle.

### *2.1. Blockchain Technology*

Blockchain technology has emerged as a transformative force across various industries, revolutionising how data is stored, managed, and shared. Blockchain is a decentralized and distributed ledger system that enables the secure and transparent recording of transactions across a network of workstations/nodes. It is a revolutionary concept that has gained significant attention in recent years. It essentially functions as a decentralized and distributed ledger, enabling secure and transparent recording of transactions across a network of workstations/nodes. Imagine a digital record-keeping system where information is shared and replicated across multiple nodes, making it virtually impossible to tamper with or alter [4]. This distributed nature eliminates the need for a central authority, advancing trust and transparency. Blockchain uses cryptography to secure transactions, ensuring their authenticity and integrity. Each transaction is grouped into blocks, which are then linked together in a chronological chain. This chain is continuously growing, with each new block adding to the record. The immutability of the blockchain makes it an ideal platform for various applications, including cryptocurrency, supply chain management, and healthcare [10].

As shown in Figure 1, blockchain comprises several key components that work together to create a secure, decentralized, and transparent digital ledger system. One of the fundamental components is the node, which refers to any computer that participates in the blockchain network. Nodes maintain copies of the blockchain, validate and propagate transactions, and ensure the network's integrity. They can be full nodes, which store the entire blockchain, or lightweight nodes, which only store a subset of the data [11]. Transactions are the basic units of data in a blockchain, representing the transfer of value or information between parties. Each transaction is digitally signed by the sender using cryptographic techniques to ensure authenticity and integrity [12,13].

These transactions are grouped into blocks, each of which contains a list of transactions, a timestamp, a nonce, and the hash of the previous block. The hash serves as a unique identifier, linking each block to its predecessor and forming a continuous chain, which enhances security and immutability. The process of adding transactions to the blockchain involves miners, who are specialized nodes that validate and record transactions by solving complex cryptographic puzzles. This process, known as mining, requires significant computational power and is integral to maintaining the blockchain's security. In return, miners are rewarded with cryptocurrency tokens [14].

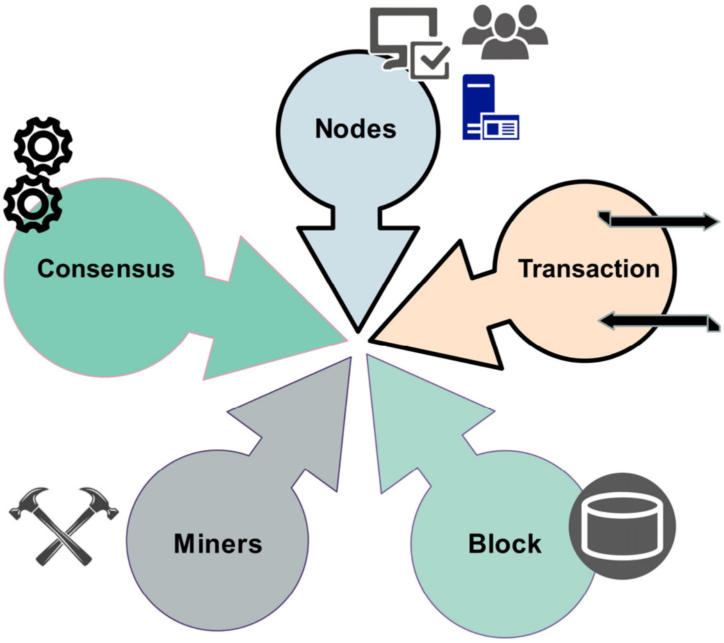

**Figure 1.** Main component of blockchain.

The integrity and consistency of the blockchain are maintained through consensus algorithms, which are protocols that nodes follow to agree on the validity of transactions and the state of the blockchain. The most well-known consensus algorithm is Proof of Work (PoW), used by Bitcoin, where miners compete to solve a mathematical problem, and the first to solve it gets to add a new block to the blockchain. Another popular consensus mechanism is Proof of Stake (PoS), used by Ethereum 2.0, where validators are chosen based on the number of tokens they hold and are willing to “stake” as collateral. These consensus algorithms prevent double-spending, ensure network security, and maintain decentralization [15].

### *2.2. Digital Forensics*

Digital forensics focuses on the recovery, analysis, and presentation of data from digital devices. As technology has advanced, the scale and complexity of digital forensics have expanded, encompassing a broad range of devices, from traditional computers and smartphones to modern IoT devices and cloud services [16]. Digital forensics offers massive benefits across various domains. It enables the investigation of cybercrimes, such as hacking, online fraud, and identity theft, by uncovering critical evidence that might otherwise remain hidden. It also can assist in responding to data breaches, internal misconduct, and intellectual property theft, helping organizations to understand the scope of an incident and mitigate future risks. Additionally, it supports the resolution of disputes involving digital evidence, such as contract breaches or intellectual property cases. Beyond legal and corporate contexts, digital forensics plays a role in safeguarding personal privacy and security by identifying and addressing unauthorized access or misuse of personal data. As the digital landscape continues to evolve, digital forensics remains a vital discipline, providing essential tools and methodologies to navigate the complexities of modern technology and ensuring accountability in an increasingly digital world [17].

In digital forensics, the investigative process is structured into six distinct phases to ensure the detailed handling and management of digital evidence [18], as shown in Figure 2. These six phases include the following:

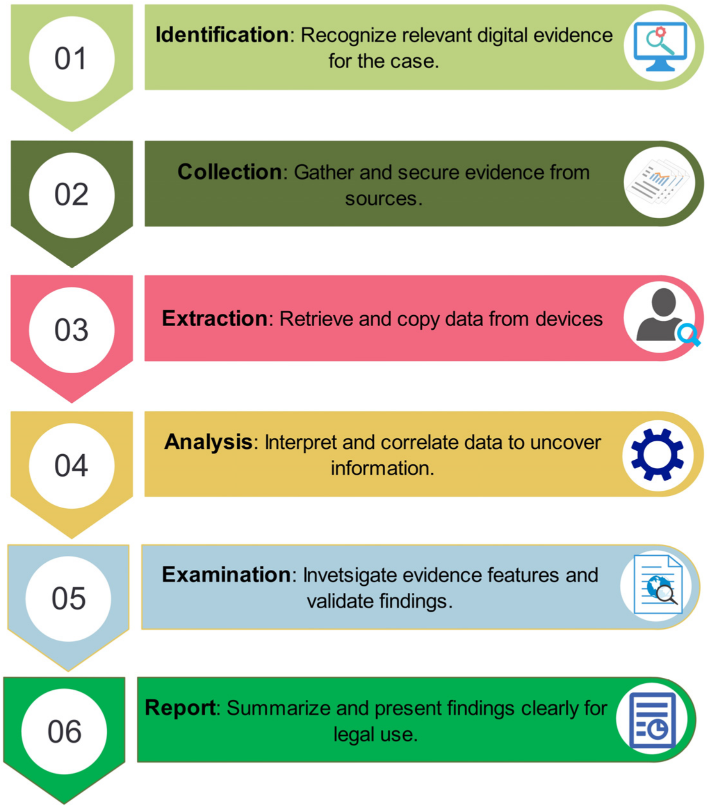
01
**Identification**: Recognize relevant digital evidence for the case.
02
**Collection**: Gather and secure evidence from sources.
03
**Extraction**: Retrieve and copy data from devices
04
**Analysis**: Interpret and correlate data to uncover information.
05
**Examination**: Invetsigate evidence features and validate findings.
06
**Report**: Summarize and present findings clearly for legal use.

**Figure 2.** Digital forensic investigation lifecycle.

- Identification: This initial phase involves recognizing and determining the specific types of digital evidence relevant to the investigation. It requires a detailed understanding of the case to identify relevant digital artefacts, which may include files, metadata, logs, or communication records.
- Collection: Once the evidence has been identified, the collection phase focuses on the systematic gathering of digital evidence from the crime scene or relevant sources. This involves securing and documenting the devices or media, such as computers, smartphones, or servers, to ensure that no data are altered or lost during the process. Proper procedures, including using write-blockers and ensuring chain-of-custody documentation, are crucial to maintaining the integrity of the evidence.
- Extraction: During the extraction phase, the digital investigator retrieves the data from the identified devices. This may involve creating forensic images or copies of hard drives, memory cards, or other storage media. The aim is to extract relevant data while preserving the original evidence intact. Extraction often requires specialized tools and techniques to handle encrypted or damaged files and to ensure that all potentially relevant information is obtained.
- Analysis: In the analysis phase, the extracted data are examined in detail to uncover meaningful information. This involves interpreting file structures, recovering deleted files, analysing log entries, and correlating data across different sources. The goal is to identify patterns, connections, and anomalies that can support or disprove the claims made in the investigation. This phase often requires deep technical expertise and may involve reconstructing events or understanding complex data relationships.
- Examination: The examination phase is where the investigator carefully scrutinizes the features of the digital evidence. This involves verifying the authenticity of the data, validating findings through repeated tests, and ensuring that all aspects of the evidence are thoroughly explored. The examination phase aims to provide a detailed and accurate representation of the evidence, ensuring that all relevant details are considered.

- Report: The final phase involves compiling and presenting the findings in a comprehensive report. This report summarizes the investigative process, methodologies employed, and the conclusions drawn from the analysis and examination. It must be clear, detailed, and structured in a way that is understandable to non-technical audiences, including legal professionals and court personnel. The report plays a critical role in legal proceedings, providing evidence that is both admissible and persuasive in court.

### *2.3. Blockchain Forensics*

Blockchain forensics is an emerging field within digital forensics that focuses on the investigation of blockchain-based activities. The unique properties of blockchain technology present both opportunities and challenges for forensic investigators. Blockchain forensics involves the systematic examination of blockchain data to uncover evidence of illegal activities, such as fraud, money laundering, and cybercrimes, which are increasingly facilitated through cryptocurrencies and decentralized platforms. The decentralized and anonymous nature of blockchain transactions adds complexity to these investigations, necessitating specialized tools and techniques to correlate on-chain data with off-chain information [6,19].

The need for investigating blockchain arises from the rapid adoption of blockchain technology across various industries and the corresponding rise in blockchain-related crimes. Cryptocurrencies, which are built on blockchain technology, have become a popular medium for transactions due to their anonymous nature and ease of cross-border transfers. This has made them attractive for criminal activities, including ransomware attacks, illegal trade on dark web marketplaces, and terrorist financing. Investigating these activities requires a deep understanding of how blockchain networks operate and how data can be traced and analysed within these systems [14]. In addition, blockchain forensics is invaluable for businesses and individuals who engage in cryptocurrency transactions. It helps in verifying the legitimacy of transactions, identifying potential security breaches, and recovering lost or stolen assets. As the blockchain ecosystem continues to expand, the importance of blockchain forensics will only increase. The ability to analyse and interpret blockchain data accurately and efficiently is critical for maintaining trust and security within this innovative space. Thus, blockchain forensics not only aids in the detection and prevention of criminal activities but also enhances the overall reliability and transparency of blockchain technologies [7].

One of the significant aspects related to blockchain forensics is node-level backups, which play a crucial role in maintaining the integrity and reliability of blockchain data. Each node in a blockchain network keeps a complete copy of the blockchain ledger, ensuring data redundancy across multiple nodes. This distributed storage is essential for forensic investigations because it prevents data loss and allows access to the complete transaction history, even if some nodes fail or become compromised. The redundancy provided by node-level backups helps ensure that forensic analysts can retrieve and examine accurate blockchain records, contributing to the overall robustness of the forensic process [20]. Node-level backups also facilitate tamper detection and data validation. As each node independently verifies the blockchain's state against its copy, discrepancies between nodes can signal tampering or errors. This feature allows forensic investigators to cross-check data across multiple nodes, enhancing the ability to detect fraudulent activities and confirm the integrity of the blockchain ledger. The distributed verification process provided by these backups is crucial for ensuring the reliability of forensic findings and supports the accuracy of investigations into blockchain transactions [21].

Furthermore, the resilience and reliability of the blockchain network are significantly bolstered by node-level backups. By decentralizing data storage and ensuring that each node maintains a complete and up-to-date copy of the blockchain, the network becomes more resistant to failures and attacks. This resilience ensures that data remain accessible and intact even during adverse conditions, such as network breaches or node malfunctions [22].

However, there are challenges associated with maintaining node-level backups. Ensuring that all nodes are properly synchronized can be difficult, particularly in large or rapidly evolving networks. Inconsistent backups can lead to discrepancies that complicate forensic analysis. Additionally, the storage and computational resources required for maintaining complete copies of the blockchain can strain system performance and scalability. Security and access control are also critical, as breaches at the node level can compromise the integrity of the backup copies and affect the reliability of forensic evidence. Effective management of these challenges is essential to maintaining the robustness of forensic practices and ensuring the accuracy and reliability of blockchain investigations.

Applying the digital forensic investigation lifecycle discussed earlier in the context of blockchain can describe the lifecycle of blockchain forensics, as shown in Figure 3, to ensure that evidence is accurately collected, analysed, and presented while maintaining the integrity of the blockchain data as follows:

- Identification: The first step in a blockchain forensic investigation is identifying the relevant data that needs to be examined. This involves determining the specific blockchain platform involved (e.g., Bitcoin and Ethereum), identifying relevant addresses, transactions, and smart contracts, and understanding the nature of the suspected illegal activity. The goal is to identify the exact data on the blockchain that is relevant to the investigation. For instance, studies have shown the importance of identifying specific addresses and transactions linked to criminal activities such as money laundering or ransomware payments.
- Collection: In the collection phase, investigators gather the identified data from the blockchain. This includes downloading the entire blockchain or extracting specific blocks, transactions, or addresses of interest. Given the public nature of most blockchains, these data are typically accessible without a warrant. However, the process must ensure that data are collected in a manner that preserves its integrity and authenticity. Advanced tools and techniques, such as blockchain explorers and forensic software, are often used to facilitate this process.
- Preservation: Preservation involves maintaining the integrity of the collected data to ensure they remain unchanged and reliable throughout the investigation. This includes creating cryptographic hashes of the data and securely storing them in a manner that prevents tampering. Blockchain's inherent immutability aids in this process, but proper handling and documentation are still essential to uphold evidentiary standards in legal contexts.
- Analysis: The analysis phase is where investigators explore the collected data to uncover meaningful patterns, relationships, and anomalies. This may involve tracking the flow of cryptocurrencies, analysing transaction histories, and identifying links between blockchain addresses and real-world identities. Sophisticated analytical tools and techniques, such as clustering algorithms and graph analysis, are employed to make sense of the complex and often pseudonymous data on the blockchain.
- Examination: During this phase, investigators contextualize their findings within the broader scope of the investigation. This includes correlating blockchain data with external sources of information, such as IP logs, email records, or traditional financial records. The goal is to build a coherent narrative that explains how the blockchain data fit into the overall case and supports the allegations being investigated.
- Report: The final phase involves compiling the analysis and interpretation into a comprehensive report that can be presented in legal or regulatory settings. This report must clearly explain the methods used, the findings, and their significance, making it understandable for non-technical stakeholders such as lawyers, judges, and juries. Proper documentation and expert testimony are often required to validate the findings and ensure their admissibility in court.

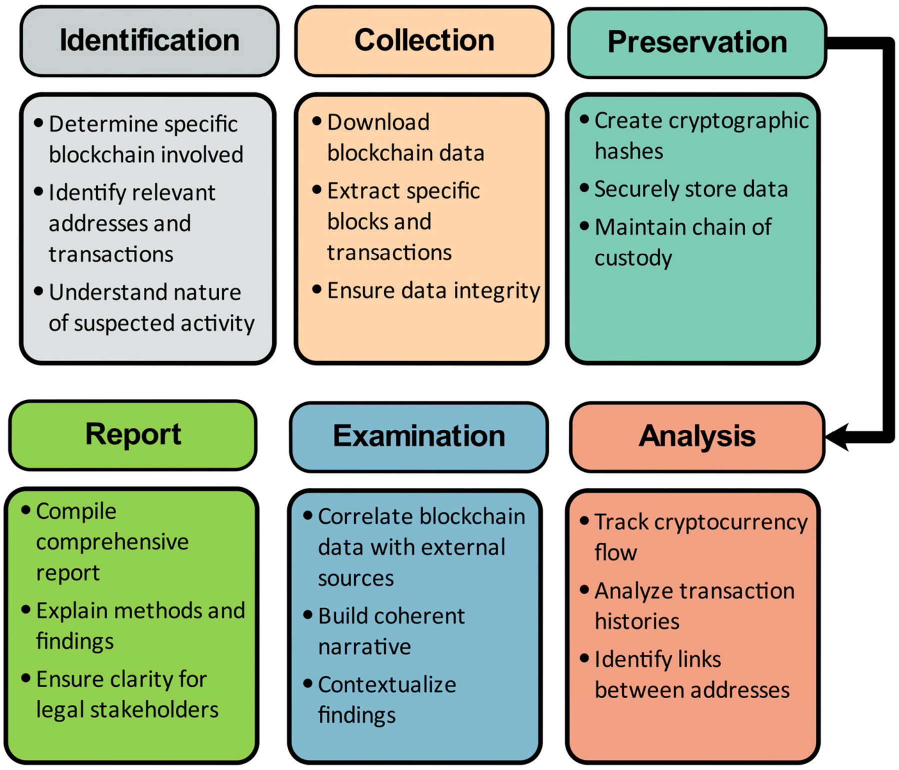
Identification
Determine specific blockchain involved
Identify relevant addresses and transactions
Understand nature of suspected activity
Collection
Download blockchain data
Extract specific blocks and transactions
Ensure data integrity
Preservation
Create cryptographic hashes
Securely store data
Maintain chain of custody
Analysis
Track cryptocurrency flow
Analyze transaction histories
Identify links between addresses
Examination
Correlate blockchain data with external sources
Build coherent narrative
Contextualize findings
Report
Compile comprehensive report
Explain methods and findings
Ensure clarity for legal stakeholders

**Figure 3.** Blockchain digital forensic lifecycle.

## 3. Research Methodology

The purpose of a systematic literature review is to define, analyse, and interpret all available research relevant to a research topic, a specific subject, or a set of interesting occurrences. While blockchain forensics has gained significant attention, the complexity and evolving nature of blockchain necessitates an in-depth review of current research. This systematic literature review examines existing blockchain forensic techniques and methodologies, as well as various studies presented by researchers employing different blockchain-based solutions in the forensic process and their conclusions.

To provide a transparent, reproducible, and scientific systematic literature review, the new version of the PRISMA 2020 protocol that was developed by Page et al. [9] was considered. The PRISMA or Preferred Reporting Items for Systematic Reviews and Meta-Analyses, which was first published in 2009, was designed to help systematic reviewers transparently report why the review was conducted, what the authors did, and what they found. We chose PRISMA over other existing protocols because of its comprehensiveness, its use in several disciplines worldwide, and its potential to increase consistency across reviews [9,23]. The PRISMA protocol for conducting a systematic literature review involves five stages, as shown in Figure 4. The first stage aims to formulate the research questions that this review will address. This is followed by determining the inclusion and exclusion criteria to ensure that the selected articles are the most relevant and pertinent to the research objectives and questions. The third stage specifies which research databases will be searched to find relevant articles. In the fourth stage, the findings are analysed, and in the fifth stage, the outcomes of each study topic are discussed.

This methodology was utilized to provide readers with a clear understanding of the systematic process used to complete this literature review. Before beginning to evaluate numerous sources, we defined our research questions to ensure a focused review. Next, selection criteria were used to narrow down the retrieved publications to those relevant to the study's objectives. The digital libraries utilized to compile these articles are also provided as data sources. Article selection based on relevance was also covered. The presented methodology offers various benefits, illustrating the steps taken by researchers to achieve their study's intended results.

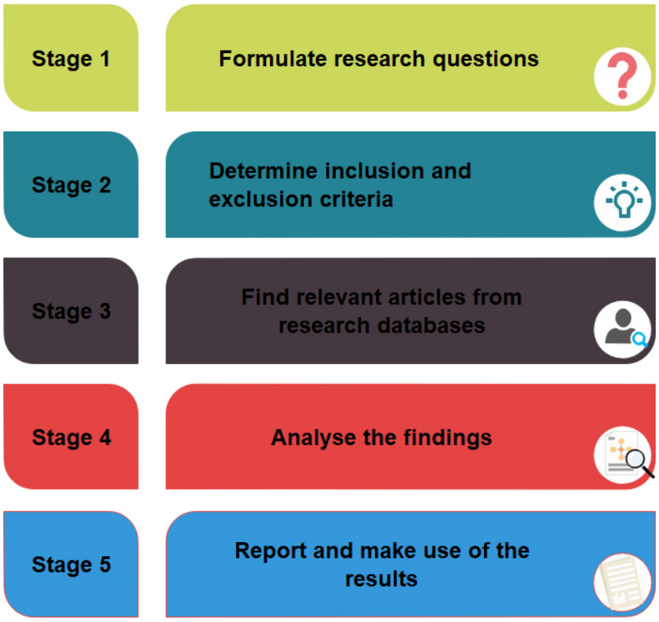
Stage 1
Formulate research questions
Stage 2
Determine inclusion and exclusion criteria
Stage 3
Find relevant articles from research databases
Stage 4
Analyse the findings
Stage 5
Report and make use of the results

**Figure 4.** Stages of conducting a systematic literature review.

Although this methodology has been employed in several systematic literature studies, there are some limitations, including the fact that it narrows the focus of the review and, hence, may not provide readers with all the facts needed to fully understand the subject matter. Additionally, data collection was limited to only a few sources for collecting relevant publications in our study, which could limit the number of publications reviewed. While these sources are considered the most reliable in various systematic literature studies, this limitation could result in the exclusion of pertinent articles related to the study objectives. In addition, the study selection process, although systematic, is subject to potential bias. The inclusion and exclusion of studies were based on specific research questions and criteria, which, despite our best efforts to remain objective, could have introduced selection bias. This bias may result from subjective interpretations of study relevance, potentially leading to the inadvertent exclusion of significant research that might have influenced our conclusions. Also, our review did not include a meta-analysis or other forms of statistical synthesis, as well as a formal quality assessment of the included studies was not conducted.

Moreover, our review exclusively included studies published in English, which introduces a potential language bias. This limitation could result in the exclusion of relevant studies published in other languages, thereby narrowing the scope of our review and possibly overlooking critical research findings. The reliance on English-language publications may have skewed the perspective of the review, particularly in a field as globally relevant as blockchain forensics.

These limitations may have implications for the interpretation and generalizability of the findings. The selection criteria, which were designed to ensure relevance and quality, may have introduced bias into the review process. Despite our efforts to maintain objectivity, the reliance on predetermined inclusion and exclusion criteria, as well as the subjective nature of interpreting study relevance, could have inadvertently excluded studies that might have significantly influenced the overall conclusions. This selection bias raises concerns about the potential for important findings to be overlooked, which may skew the review's results. Furthermore, by excluding non-English publications, the review introduces a language bias, potentially omitting significant research conducted in non-English speaking regions. This exclusion not only narrows the geographic and cultural scope of the review but also risks disregarding relevant studies that could provide critical insights, thereby affecting the global applicability of the findings.

### *3.1. Research Questions*

This paper seeks to address the following research questions:

- RQ1: What are the state-of-the-art studies related to blockchain forensics and blockchain-based solutions for digital forensics?
- RQ2: How can blockchain technology enhance digital forensic investigations?
- RQ3: What are the digital forensic frameworks and methodologies used in blockchain forensics?
- RQ4: What are the common applications of blockchain-based digital forensic investigation frameworks?
- RQ5: What are the legal and regulatory challenges in conducting a forensic investigation on blockchain systems?

### *3.2. Inclusion and Exclusion Criteria*

Inclusion and exclusion criteria were employed to select the relevant research. The primary purpose of these criteria was to answer the research questions and ensure the creation of a comprehensive literature review.

The inclusion criteria were as follows:

- Peer-reviewed journals and conference articles to ensure high-quality and credible sources;
- Relevant to the specific research questions;
- Topic mainly on blockchain forensics and blockchain-based forensic solutions;
- Full and available articles to allow for a comprehensive review of the content;
- English-language articles to maintain consistency in analysis.

The exclusion criteria were as follows:

- Articles concerning all other security aspects of blockchain apart from digital forensic investigations;
- Articles not focused on blockchain forensics or significantly deviating from the primary research questions;
- Unpublished articles, non-peer-reviewed articles, and editorial articles to ensure credibility;
- Articles that are not fully available;
- Non-English articles to avoid translation issues and maintain analysis consistency;
- Duplicates of already included articles to avoid redundancy.

### *3.3. Data Sources*

Recent studies have highlighted the growing importance of digital libraries in conducting comprehensive searches for systematic literature reviews. These electronic databases, selected based on their relevance and widespread recognition in current research, were instrumental in ensuring a thorough examination of the available literature. The digital libraries utilized in this SLR were chosen to align with the latest academic standards and recommendations [24–27]. Specifically, the electronic databases considered included the following:

- IEEE Xplore;
- PubMed;
- Elsevier ScienceDirect;
- Google Scholar;
- ACM Digital Library;
- SpringerLink.

A keyword-based search was conducted to gather articles pertinent to the topic and research questions. The primary keywords used included the following:

- Blockchain forensic investigation;
- Blockchain forensics;
- Digital forensics in blockchain;
- Cryptocurrency forensics;
- Forensic techniques in blockchain;
- Investigating blockchain transactions;
- Blockchain tracing;
- Blockchain evidence collection;
- Forensic challenges in blockchain;
- Legal aspects of blockchain forensics;
- Blockchain forensic tools;
- Cryptocurrency crime investigation;
- Blockchain fraud detection.

### *3.4. Selection of Relevant Articles*

This step involved choosing relevant and recent studies on blockchain forensics from the 672 articles gathered from various online digital libraries. The process of selecting relevant publications was divided into three phases:

- Phase 1: Publications found during the search and those already in the collection were sorted using the inclusion and exclusion criteria. The scope of the search was narrowed to include only articles published recently and consider the topic of blockchain forensics.
- Phase 2: The titles and abstracts of the articles collected from several digital libraries were reviewed to determine how well they addressed the topic and the questions posed in this research work.
- Phase 3: During this stage, we focused on eliminating duplicates among the six digital libraries used for our publication collection.

## **4. Analysis of Results**

The inclusion and exclusion criteria were applied to the collected publications in three phases, according to the PRISMA 2020 statement [9]. In the first phase, a total of 672 articles were identified from six different databases: Google Scholar (421), IEEE Explore (153), PubMed (6), Elsevier ScienceDirect (27), ACM Digital Library (31), and SpringerLink (34). Then, in phase 2, the collected articles were screened based on the research questions where the articles that did not align with the research questions were out of scope or did not meet the inclusion criteria were excluded. This resulted in excluding 301 articles and 71 articles moving forward. In phase 3, 25 duplicate articles were identified and removed from the 71 articles, leaving 46 articles that were included in this review. The flow diagram of the PRISMA process and the number of articles at each stage is shown in Figure 5.

The search that was executed in six different well-known online databases enabled us to collect most of the publications that are relevant to blockchain forensics. The results of the collected publications from each online database and the resultant number of publications after applying the three selection phases are shown in Table 1. The results show that Google Scholar and IEEE are the richest data sources of publications related to blockchain forensics.

Additionally, the number of publications related to blockchain forensics per year is shown in Figure 6. The data indicate that this is a dynamic field that has experienced rapid growth. The increase in publications from 2018 to 2021 reflects the increasing recognition of the need for robust blockchain forensics in response to the proliferation of blockchain technology and its applications. The peak in 2021 could be associated with significant milestones, such as regulatory developments, high-profile criminal investigations, or technological advancements that prompted extensive research and publications. The increase in publication again in 2023 and 2024 suggests a resilient field that continues to evolve and adapt to new challenges and opportunities.

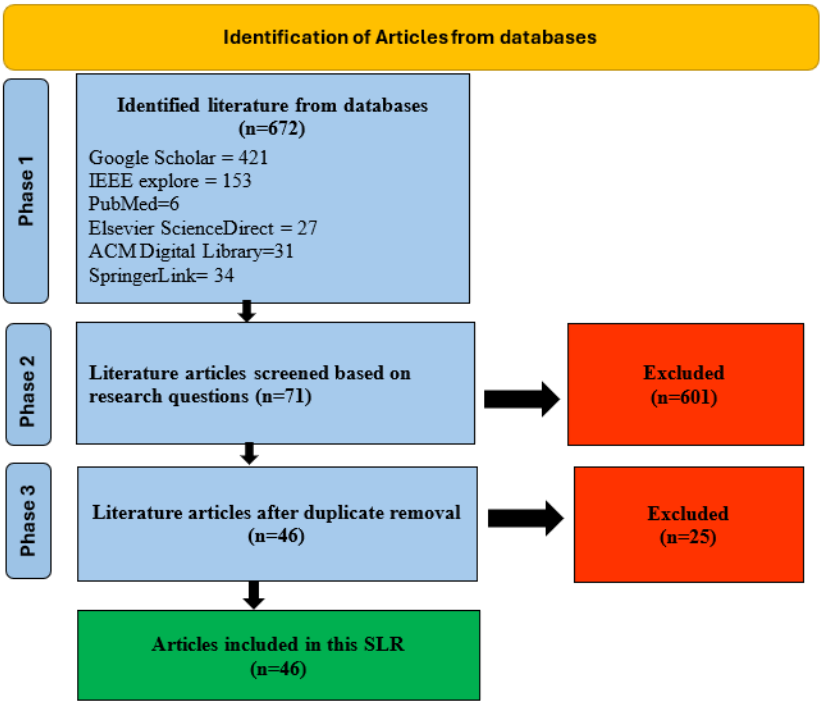
Identification of Articles from databases
Phase 1
Identified literature from databases (n=672)
Google Scholar = 421
IEEE explore = 153
PubMed=6
Elsevier ScienceDirect = 27
ACM Digital Library=31
SpringerLink= 34
Phase 2
Literature articles screened based on research questions (n=71)
Excluded (n=601)
Phase 3
Literature articles after duplicate removal (n=46)
Excluded (n=25)
Articles included in this SLR (n=46)

**Figure 5.** Flow diagram of the PRISMA process employed in this review.

**Table 1.** Number of search results per database after applying the three selection phases.

| Data Source | Phase 1 | Phase 2 | Phase 3 |
|---|---|---|---|
| Google Scholar | 421 | 27 | 18 |
| IEEE explore | 153 | 12 | 8 |
| PubMed | 6 | 2 | 1 |
| Elsevier ScienceDirect | 27 | 13 | 9 |
| ACM Digital Library | 31 | 9 | 5 |
| SpringerLink | 34 | 8 | 5 |
| Total | 672 | 71 | 46 |

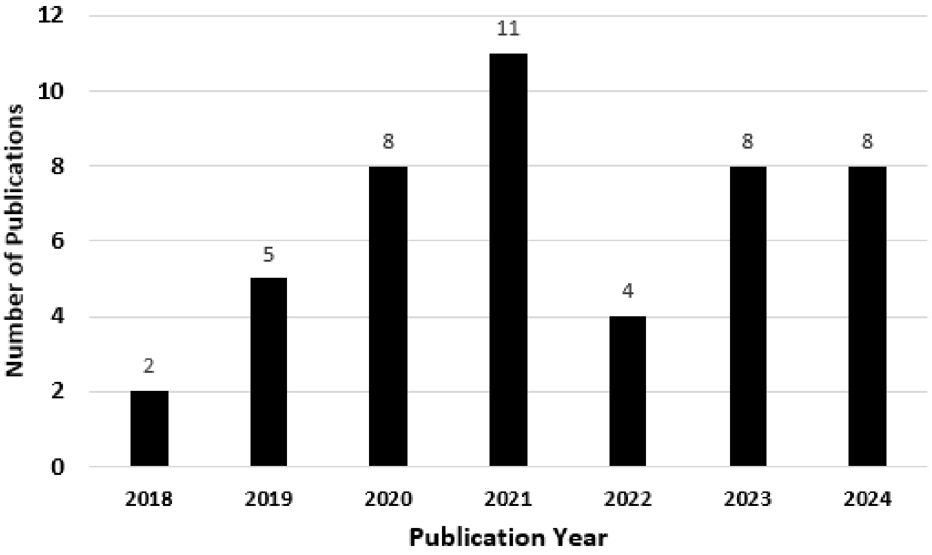

**Figure 6.** Number of publications per year.

## 5. Results and Discussion

The growing interest in blockchain forensics is driven by the increasing frequency of cybercrimes and the need for robust forensic solutions. As digital transactions and activities proliferate, the volume of digital evidence generated is immense. Traditional forensic methods struggle to cope with this scale, making the scalability and efficiency of blockchain-based solutions particularly appealing. Researchers are, therefore, keen to develop and refine blockchain forensic frameworks that can handle large volumes of data while maintaining high standards of security and integrity.

The reviewed studies collectively explore the integration of blockchain technology into various aspects of digital forensics, showcasing its potential to enhance evidence integrity, traceability, and transparency. Many studies propose innovative frameworks that leverage blockchain to secure digital evidence, manage the chain of custody, and address challenges in IoT, cryptocurrency, and vehicular forensics. However, a recurring limitation across these studies is the lack of detailed technical implementation and real-world evaluation, which raises concerns about the practical applicability of the proposed solutions. Many papers focus on conceptual designs without providing sufficient empirical data or performance analysis, which weakens the reliability of their findings. Additionally, issues such as scalability, privacy concerns, legal and regulatory implications, and integration with existing systems are often underexplored, further impacting the robustness of the proposed frameworks. While the potential of blockchain in digital forensics is evident, the absence of comprehensive evaluations and discussions on real-world challenges suggests that further research is needed to fully realize its benefits and address the practical limitations identified in these studies.

This section presents a comprehensive and detailed analysis to answer the research questions by integrating insights and contributions from various papers.

**RQ1: What are the state-of-the-art studies related to blockchain forensics and blockchain-based solutions for digital forensics?**

To answer this research question, the retrieved/analysed publications from this systematic literature review will be discussed by highlighting the contribution of each paper and their limitations, as shown in Table 2.

**Table 2.** Summary of recent studies related to blockchain forensics and blockchain-based forensics and their limitations.

| Citation | Summary of Contribution | Limitations |
|---|---|---|
| Ahmad et al. [28] | This paper proposes a blockchain-based chain of custody framework to ensure tamper-proof evidence management. The framework uses a private Ethereum blockchain to securely record evidence metadata while storing physical evidence in a reliable medium locked with smart locks. This approach aims to provide authenticated access, maintaining evidence integrity and admissibility among multiple stakeholders. | The scalability issues inherent in private blockchains and the need for smooth integration with existing digital evidence systems. Also, it does not discuss or address the challenges of managing large volumes of evidence and their associated costs. |
| Akinbi et al. [24] | This paper presents a comprehensive review of blockchain-based IoT forensic investigation models. It systematically reviews how blockchain is used to securely improve forensic investigations and discusses the efficiency of these models. This paper highlights the challenges, open issues, and future research directions of blockchain in IoT forensic investigations. | This paper does not provide a detailed analysis of the different techniques and methodologies used, and it does not discuss the legal and ethical implications of using blockchain in IoT forensic investigations. |

**Table 2.** *Cont.*

| Citation | Summary of Contribution | Limitations |
|---|---|---|
| Siaam et al. [29] | This paper proposes Probe-IoT, a forensic investigation framework for IoT systems that uses a public digital ledger to identify facts in IoT crime cases. It addresses the challenges of evidence spoliation and lack of transparency in IoT environments by recording interactions between IoT devices, users, and cloud services on a blockchain. The framework allows investigators to trace the flow of data and identify potential perpetrators. | This paper lacks a detailed implementation and evaluation of the proposed framework. In addition, the dependence on a public blockchain could raise privacy and legal concerns for users, as their interactions and communications are publicly accessible. |
| Billard [30] | This paper proposes a framework for building a fact-based confidence rating of digital evidence. It uses a blockchain-based Digital Evidence Inventory (DEI) to ensure immutability and traceability, categorizes digital evidence into data types with associated confidence ratings, and creates a Global Digital Timeline (GDT) to order evidence through time. | The confidence rating system needs to be refined by incorporating error rate probabilities and relevance measures. This paper also relies on expert's judgment for data categorization and rating, which adds subjectivity to the process. |
| Cebe et al. [1] | This paper proposes a blockchain-based framework called Block4Forensic (B4F) for vehicular forensics. B4F provides a secure, trustworthy, and comprehensive platform for collecting and analysing vehicle data. It integrates vehicular public key infrastructure for membership establishment and privacy and utilizes a fragmented ledger to store detailed vehicle information. B4F enables trustless, traceable, and privacy-aware post-accident analysis, facilitating dispute resolution and identifying faulty parties. | This paper lacks implementation details and performance evaluation. This paper also does not address the practical challenges of integrating B4F with existing vehicular systems. Also, this paper does not discuss potential security vulnerabilities of the proposed framework. |
| Chopade et al. [31] | This paper proposes a blockchain-based model for maintaining the chain of custody in digital forensics. The model utilizes a distributed ledger to record and track the transfer of digital evidence between various participants in an investigation to ensure its integrity and authenticity. The model employs Base64 encryption to generate a hash of the evidence, which is then transferred instead of the original data, preventing tampering and providing a verifiable record of ownership. | This paper lacks implementation and evaluation of the proposed model. It also does not discuss integrating the model with existing digital forensic frameworks and does not consider potential security vulnerabilities of using Base64 for evidence hashing, which could be vulnerable to certain attacks. |
| Dasaklis et al. [8] | This paper provides a comprehensive overview and classification of blockchain-based digital forensic tools to analyse their main features, benefits, and challenges. It examines the potential of blockchain to enhance digital forensics by addressing issues including evidence immutability, transparency, and auditability. | This paper does not discuss the legal, regulatory, and ethical implications of using blockchain in digital forensic investigations, which are crucial considerations for real-world applications. |
| Floride et al. [32] | This paper explores the application of blockchain in digital forensics, particularly focusing on its use in threat hunting and evidence management. It highlights the benefits of blockchain in ensuring evidence integrity, traceability, and immutability. This paper also examines the use of deep learning models for detecting vulnerabilities in smart contracts on the Ethereum blockchain. | This paper does not consider the practical challenges of implementing blockchain-based digital forensic systems in real-world applications. This paper also lacks empirical research to validate the effectiveness of the framework. |

**Table 2.** *Cont.*

| Citation | Summary of Contribution | Limitations |
|---|---|---|
| Frowis et al. [33] | This paper investigates the legal and technical aspects of forensic cryptocurrency investigations. It identifies key legal requirements for safeguarding the evidential value of such investigations, including lawfulness, authenticity, reliability, qualification, verifiability, chain of evidence, and the right to inspect records. This paper then translates these requirements into a data-sharing framework for law enforcement agencies to promote efficient and effective investigations while protecting individuals' privacy. | This paper lacks an in-depth analysis of blockchain forensic tools and techniques and does not provide a complete evaluation of the effectiveness of the proposed technique. This paper also does not discuss the complex legal implications of processing publicly available data for law enforcement purposes. |
| Hsu et al. [34] | This paper proposes an autonomous log storage management protocol for IoT environments that incorporates blockchain mechanisms and access control. Integrating blockchain and a novel "signature chain" concept provides robust identity verification, data integrity, non-repudiation, tamper resistance, and evidence legality, making it suitable for digital forensic investigations. | The performance of the proposed protocol in large-scale IoT deployments with high data volumes needs to be discussed. This paper does not discuss potential scalability issues associated with blockchain, particularly in terms of transaction throughput and latency. |
| Jin et al. [35] | This paper proposes a methodology for tracing operators of illegal dark websites through cryptocurrency transactions. It highlights the importance of tracking the flow of funds on the blockchain to link Bitcoin addresses to real-world bank accounts and use it in digital forensic investigations. This paper provides valuable insights into identifying perpetrators by analysing cryptocurrency transactions, despite the anonymity provided by cryptocurrencies. | This paper focuses only on publicly available information, neglecting the complexities of cryptocurrency and dynamic Bitcoin addresses. Also, this paper relies on POW consensus, which introduces latency and energy inefficiency, impacting real-time forensic analysis. |
| Khan et al. [36] | This paper proposes MF-Ledger, a blockchain-based architecture for multimedia digital forensic investigations using Hyperledger Sawtooth. MF-Ledger provides secure evidence integrity, preservation, transparency, and resistance to tampering by leveraging a permissioned blockchain network. It addresses the challenges of traditional digital forensics by offering a secure and transparent process for collecting, storing, analysing, and interpreting digital evidence. The architecture utilizes smart contracts to manage the chain of custody events and ensures privacy protection for evidence stored in an encrypted ledger. | This paper does not consider the challenges of implementing the proposed method in the real world. The proposed architecture is only simulated using sequence diagrams; however, it lacks validation and evaluation in a real-world forensic environment. Furthermore, this paper does not address the legal and regulatory challenges associated with using blockchain in forensic investigations. |
| Khanji et al. [37] | This paper presents a systematic review of the readiness of blockchain integration in IoT forensics. It analyses the literature to review the deployment of Blockchain to resolve various challenges presented in IoT forensics. | This paper does not provide a detailed analysis of the efficiency of the different models and frameworks reviewed in the literature. |

**Table 2.** *Cont.*

| Citation | Summary of Contribution | Limitations |
|---|---|---|
| Li et al. [38] | This paper proposes LEChain, a blockchain-based lawful evidence management scheme for digital forensics that addresses the entire lifecycle of evidence, from collection to court trial and sentencing. LEChain utilizes short randomizable signatures for anonymous witness authentication, fine-grained access control based on CP-ABE for evidence access, and secure voting to protect juror privacy. The system is built on a consortium blockchain to ensure transparency, immutability, and auditability of evidence transactions. | The proposed method was implemented on a consortium blockchain, which may not be suitable for all digital forensic scenarios. In addition, the evaluation of the proposed technique is based on a local Ethereum test network, which may not accurately reflect the performance of the system in a real-world setting. |
| Li et al. [7] | This paper proposes a blockchain-based digital forensic framework for the IoT, called IoT Forensic-Chain (IoTFC). IoTFC records all examination operations, including evidence identification, preservation, analysis, and presentation, in a chain of blocks. | This paper does not discuss potential privacy concerns associated with storing sensitive evidence on a public blockchain. |
| Mahrous et al. [39] | This paper proposes a blockchain-based IoT digital forensic architecture that incorporates fuzzy hashing into the blockchain's Merkle tree. This approach enhances the ability to identify potentially incriminating evidence that may have undergone benign or malicious alterations, which traditional hashing methods struggle to detect. By comparing blocks/files to all nodes in the blockchain network using fuzzy hash similarity, digital forensic investigators can verify their authenticity. | This paper does not discuss the challenges of integrating fuzzy hashing into existing blockchain platforms or discuss the potential performance overhead associated with fuzzy hash computations. Also, this paper lacks a detailed analysis of the security implications of using fuzzy hashing in a blockchain context. |
| Muyambo et al. [40] | This paper presents a systematic review of blockchain-based digital forensics in Internet voting systems. This paper also proposes a blockchain-based digital forensic-ready internet voting system called DFRMIV, which addresses issues of transparency, privacy, integrity, confidentiality, and auditability in online voting systems. | This paper does not discuss detailed information and technical details on how the proposed DFRMIV system would work in practice and how it would address challenges related to blockchain forensics. |
| Patil et al. [41] | This paper explores the potential of blockchain to improve the chain of custody in forensic investigations. It highlights how blockchain's decentralized, immutable, and transparent nature can address challenges like evidence tampering, excessive paperwork, and difficulty in tracking evidence interactions. The authors also propose a framework where evidence details are recorded on a blockchain, creating a tamper-proof and auditable record. | This paper lacks real implementation details and analysis of the practical challenges of blockchain in the chain of custody. This paper also lacks a detailed discussion on the legal and ethical implications of using blockchain in forensic investigations. |
| Ryu et al. [42] | This paper proposes a blockchain-based framework for digital forensics in the IoT. The framework utilizes blockchain to store all communications of IoT devices as transactions to ensure data integrity and simplify the chain of custody process. This decentralized approach enhances security, transparency, and reliability. | This paper does not discuss the technical details of implementing the proposed framework, such as the specific blockchain platform used or the methods for verifying digital signatures. |

**Table 2.** *Cont.*

| Citation | Summary of Contribution | Limitations |
|---|---|---|
| Sheelvanth et al. [43] | This paper proposes a blockchain-based forensic evidence management system to address vulnerabilities in traditional systems. It utilizes blockchain's decentralized and immutable nature to ensure data integrity, automate the chain of custody, and enhance transparency and accountability. | This paper only focuses on the conceptual design and lacks a detailed technical implementation, such as the specific blockchain platform used or the cryptographic algorithms employed. |
| Xiao et al. [6] | This paper proposes a blockchain-based digital forensic framework for IIoT environments. It utilizes a decentralized blockchain storage mechanism to ensure tamper-proof and permanent storage of digital evidence. The framework utilizes smart contracts for efficient evidence retrieval and tracing, and a token mechanism for access control. | This paper does not discuss the potential privacy risks associated with storing sensitive IIoT data on a public blockchain. Also, this paper does not explore the scalability of the proposed framework for handling large volumes of data generated by IIoT systems. |
| Zarpala and Casino [44] | This paper proposes a blockchain-based forensic model for financial crime investigations. The model uses blockchain's immutability and verifiability to create a tamper-proof audit trail to ensure the integrity of evidence and facilitate the chain of custody. | This paper focuses only on the embezzlement scenario, which limits its generalizability to other financial crimes. |
| Sakshi et al. [45] | This paper provides a review of research trends and challenges related to blockchain-based IoT forensic evidence preservation. It analyses the integration of blockchain with IoT forensics and discusses various blockchain platforms and tools. | This paper lacks technical details on implementing blockchain solutions for evidence preservation. It also does not discuss legal and regulatory aspects. |
| Alqahtany and Syed [46] | This paper proposes a framework for integrating blockchain technology into digital forensics, encompassing data preservation, acquisition, analysis, and documentation. The framework utilizes smart contracts and APIs to record every forensic transaction on the blockchain to ensure transparency, immutability, and authenticity of the evidence. | This paper focuses only on the conceptual design and theoretical aspects of the framework. It lacks detailed implementation and evaluation of the proposed solution on a real-world blockchain platform. |
| Onyeashie et al. [47] | This paper provides a systematic review of blockchain applications in the chain of custody. It examines how blockchain can strengthen the evidential chain of custody and interoperate with actual evidence storage. This paper highlights the benefits of blockchain in providing an immutable and decentralized structure for documenting and auditing evidence trails. | This paper does not discuss the implementation details of the system and real-world applications. This paper also does not discuss the technical challenges of integrating blockchain with existing forensic tools. |
| Kumar et al. [19] | This paper proposes a blockchain-based digital forensics framework called Internet-of-Forensics (IoF) for the IoT. IoF addresses the lack of transparency and heterogeneity in IoT using a consortium blockchain to manage evidence and ensure the chain of custody. It uses lattice-based cryptography for low complexity and post-quantum security, making it suitable for resource-constrained devices. | This paper does not discuss the practical challenges of integrating the proposed framework with existing forensic tools. Also, this paper does not evaluate the performance of the proposed framework in real-world scenarios. |
| Goyal [48] | This paper provides a review of blockchain in forensic science by highlighting the potential of blockchain to enhance privacy, authenticity, reliability, and evidence management in forensic investigations. | This paper does not discuss technical details, novel forensic frameworks, or considerations and evaluation related to real-world implementation. |

**Table 2.** *Cont.*

| Citation | Summary of Contribution | Limitations |
|---|---|---|
| Jacob and Kumar [49] | This paper proposes a framework for digital forensics using blockchain to secure digital data. The framework uses blockchain's immutability and transparency to ensure the integrity and authenticity of digital evidence. | The proposed framework is only conceptual and does not address practical challenges such as scalability, interoperability, and legal considerations. |
| Akbarfam et al. [50] | This paper presents ForensiBlock, a private blockchain framework designed for digital forensics provenance. ForensiBlock ensures secure data access, traces data origins, preserves records, and expedites provenance extraction, offering a secure, efficient, and reliable solution for handling digital forensic data. | This paper does not provide a detailed analysis of the performance of ForensiBlock in real-world scenarios. It also does not discuss the scalability of the proposed framework. |
| Masud et al. [51] | This paper reviews existing research on digital forensics frameworks for blockchain and cryptocurrency. It highlights the challenges and opportunities in applying digital forensic techniques to the unique characteristics of blockchain. | This paper does not discuss methods for evidence preservation in blockchain, which is a critical aspect for ensuring the admissibility of digital evidence. |
| Almutairi and Moulahi [52] | This paper proposes a framework for digital forensics in IoT that combines blockchain and federated learning. The blockchain is used to store the trained models from the federated learning process to ensure data integrity and traceability. The federated learning is used to address privacy concerns associated with data sharing. | This paper does not discuss the potential for blockchain attacks, such as 51% attacks, which could compromise the integrity of the evidence stored on the blockchain. |
| Cong et al. [53] | This paper explores various criminal activities related to cryptocurrencies, including investment scams, Ponzi schemes, rug pulls, ransomware attacks, money laundering, and darknet markets. It discusses how blockchain forensic techniques can be used to investigate and limit some of these cybercrimes. | This paper lacks a detailed technical analysis and implementation of blockchain forensic techniques and methods and their application in real-world investigations. |
| Alqahtany and Syed [54] | This paper proposes a framework for mobile VPN forensics by integrating blockchain with deep learning models. The blockchain acts as a secure and tamper-proof ledger for recording VPN transactions to enhance the integrity and admissibility of forensic evidence. | This paper does not discuss potential challenges related to blockchain scalability, transaction costs, or privacy concerns associated with storing sensitive VPN data on a public blockchain. |
| Srivasthav et al. [55] | This paper provides a survey of blockchain forensics and analytics tools, categorizing them based on their key features and comparing them across three practical parameters: cryptocurrency support, feature availability, and ease of access. | This paper focuses on only a limited number of tools and does not consider the rapidly evolving landscape of blockchain forensics. |
| Khan et al. [56] | This paper proposes an IoT-blockchain architecture for multimedia forensics investigations. The proposed system utilizes a private permissioned network to facilitate secure collaboration among stakeholders, including the exchange of video surveillance data and chain-of-custody details. Smart contracts automate ledger verification and validation, ensuring immutability and transparency in the investigation process. | This paper lacks a detailed analysis of the performance impact of smart contracts on the blockchain network. In addition, this paper does not discuss the scalability challenges of the proposed system when handling a large volume of multimedia data. |

**Table 2.** *Cont.*

| Citation | Summary of Contribution | Limitations |
|---|---|---|
| Al-Khateeb et al. [57] | This paper surveys the potential of blockchain to enhance digital forensics and incident response. It argues that blockchain can improve the implementation of digital investigation models by automating the identification and preservation phases. | This paper lacks technical details and implementation strategies for integrating blockchain into existing digital investigation frameworks. |
| Ragu and S. [58] | This paper proposes a blockchain-based cloud forensics architecture for privacy leakage prediction using SDN and blockchain to address the challenges of evidence integrity and centralized evidence collection in cloud environments. | This paper focuses only on the conceptual design and lacks technical details and evaluation of the proposed system in a real-world scenario. |
| Brotsis et al. [59] | This paper reviews recent blockchain-enabled forensics frameworks and extracts best practices for integrating blockchain into the process. It then presents a novel blockchain-enabled platform for IoT forensics, implemented with Hyperledger Fabric and evaluated on a virtualized testbed. | This paper focuses only on a specific blockchain platform (Hyperledger Fabric) and a limited number of attack scenarios. It also does not discuss the privacy implications of the proposed system. |
| Bonomi et al. [60] | This paper proposes a blockchain-based chain of custody (B-CoC) for managing digital evidence in digital forensics. B-CoC utilizes a private permissioned blockchain to ensure the integrity, traceability, authentication, and verifiability of digital evidence throughout its lifecycle. | This paper does not discuss the legal and practical implications of the proposed system. This paper also does not discuss the potential challenges of integrating B-CoC with existing legal frameworks. |
| Tian et al. [61] | This paper proposes a secure digital evidence framework using blockchain (Block-DEF) for blockchain forensics. Block-DEF employs a mixed block structure and a name-based consensus mechanism to address blockchain scalability issues. | This paper does not discuss the security implications of the Block-DEF and does not discuss the challenges of integrating Block-DEF with existing frameworks. |
| Lusetti et al. [62] | This paper proposes a blockchain-based solution called Custody Chain (CC) for the secure storage and sharing of digital forensic medical evidence. CC uses a hybrid platform that encrypts digital evidence and stores it in a redundant online file storage system, while using a private Hyperledger Fabric blockchain to record file properties, access history, and user permissions. | The proposed solution is mainly based on a private and permissioned blockchain, which limits the potential for wider adoption and interoperability with other forensic systems. |
| Verma et al. [63] | This paper proposes a blockchain-based electronic law record management scheme called NyaYa, which utilizes a public blockchain with off-chain storage in IPFS to maintain ELRs to ensure scalability and security. It also incorporates smart contracts for case closure and financial settlements. | This paper does not provide a detailed analysis of the security of the proposed scheme against existing blockchain forensic attacks. |
| Chen et al. [64] | This paper reviews the application of blockchain in generating electronic evidence for judicial proceedings, specifically focusing on its benefits in ensuring immutability, traceability, and independence of evidence. This paper proposes a consortium blockchain-based system for electronic evidence generation, enabling judicial bodies to verify evidence legitimacy and improve the reliability of evidence. | This paper lacks a discussion of specific forensic techniques and tools used for evidence analysis on the blockchain. This paper focuses on a single case study, which limits its generalizability to other types of cases and blockchain platforms. |

**Table 2.** *Cont.*

| Citation | Summary of Contribution | Limitations |
|---|---|---|
| Awuson-David et al. [65] | This paper proposes a Blockchain Cloud Forensic Logging (BCFL) framework that uses a permissioned blockchain to maintain tamper-proof logs within the cloud ecosystem. BCFL integrates a permissioned blockchain into the cloud, enabling evidence acquisition that enhances GDPR compliance and maintains a secured chain of custody. | This paper focuses only on a single case study, which may not be generalizable to other cloud environments. This paper also does not discuss potential scalability issues of the BCFL framework. |
| Olukoya et al. [66] | This paper proposes a framework for distilling blockchain requirements for security incident response platforms (SIRPs) to enhance auditability and integrity. The framework extracts actions, audit records, and relevant metadata from the SIRP, then designs payloads for these actions and defines a blockchain structure for storing the transactions. | This paper lacks a comprehensive evaluation of the proposed framework's performance and scalability. This paper also does not address the potential challenges of integrating the proposed blockchain system with existing SIRPs. |
| Burri et al. [67] | This paper proposes a blockchain-based solution for maintaining a chronological and independently verifiable electronic chain of custody (e-CoC) ledger for digital evidence using a private blockchain managed by a trusted entity, with periodic updates to a public blockchain for enhanced security. | The proposed solution relies on the integrity of the trusted entity and does not fully address the decentralized nature of blockchain technology. |

Examining the selected papers from the literature reveals diverse perspectives and innovative contributions towards integrating blockchain into digital forensics. There are several studies investigated the possibility of integrating blockchain in digital forensic investigations. These studies explore various aspects and methodologies for utilizing blockchain to improve evidence management, integrity, transparency, and security in forensic investigations. They investigate blockchain's potential to address traditional challenges in digital forensics, such as tampering, chain of custody, scalability, and interoperability. While each paper proposes different frameworks, models, and use cases, they all emphasize blockchain's immutable and decentralized nature as the key for advancing the reliability and efficacy of digital forensic investigations.

Although most of the selected papers have many common aspects in exploring the applicability of blockchain in digital forensic investigations, there are some major differences among these papers that lie in their specific focus areas, proposed frameworks, and the unique challenges they address within digital forensics. For instance, Ahmad et al. [28], Chopade et al. [31], Patil et al. [41], and Bonomi et al. [60] focus on ensuring the integrity and authenticity of the chain of custody in digital forensics. They propose frameworks that leverage blockchain to maintain tamper-proof records of evidence handling, although they have major differences in their implementation details and the specific aspects of custody they address. In contrast, Akinbi et al. [24], Siaam et al. [29], and Hsu et al. [34] focus on IoT forensic investigations. These papers examine how blockchain can be integrated into IoT environments to enhance the security, transparency, and reliability of forensic data. Their proposed frameworks are tailored to address the unique challenges posed by the dynamic and decentralized nature of IoT systems.

Similarly, the work by Jin et al. [35] and Cong et al. [53] is centred around cryptocurrency-related crimes, a growing area of concern in digital forensics. These papers explore how blockchain forensic techniques can be employed to trace illicit activities, such as dark web transactions and various cybercrimes. Despite the inherent anonymity provided by cryptocurrencies, these studies propose methods for tracking transactions to uncover criminal activities. Jin et al. [35] focus on algorithmic approaches for de-anonymizing transactions, while Cong et al. [53] concentrate on legal frameworks for using such evidence in court. Together, these papers provide a comprehensive view of how blockchain can be harnessed to tackle the challenges of cryptocurrency forensics. Additionally, Alqahtany and Syed [54] propose a novel integration of blockchain with deep learning models for mobile VPN forensics, highlighting how blockchain can secure and validate VPN transactions in mobile environments. This approach could be particularly valuable when combined with other blockchain-based forensic frameworks that focus on different aspects of digital forensics, such as evidence integrity or IoT forensics, thereby creating a multi-layered defense against forensic tampering and fraud. Muyambo et al. [40] and Ragu and S. [58] explore blockchain applications in internet voting and cloud forensics, respectively.

Despite the contributions provided by these researchers, these studies highlight common limitations such as scalability, integration challenges, privacy concerns, and the need for detailed implementation and performance evaluations. Scalability remains a significant concern, as the storage and processing requirements of blockchain can become difficult with large volumes of evidence data. Integration challenges with existing forensic systems pose technical and operational hurdles that need to be addressed for practical adoption. Privacy concerns, particularly in the context of public blockchains, require careful consideration and the development of mechanisms to protect sensitive information. Moreover, the lack of detailed implementation and performance evaluations in many of proposed frameworks limits the understanding of their practical applicability and effectiveness in various real-world investigation scenarios. Future research should focus on addressing these limitations, exploring practical applications, and balancing transparency with privacy to ensure the effective deployment of blockchain technology in digital forensic investigations.

**RQ2: How can blockchain technology enhance digital forensics investigations?**

Blockchain technology has emerged as a promising tool to enhance digital forensic investigations across various domains by addressing critical challenges related to evidence integrity, transparency, and security. The selected papers showcase a range of innovative applications where blockchain is leveraged to transform traditional forensic practices. Ahmad et al. [28], Chopade et al. [31], Li et al. [38], and Mahrous et al. [39] focus on evidence integrity in digital forensics, proposing blockchain-based frameworks to ensure the tamper-proof management of evidence. These frameworks utilize distributed ledgers to record and track the transfer of digital evidence securely. By employing cryptographic techniques and smart contracts, they establish a transparent and immutable record of custody, thereby reducing the risk of evidence tampering and ensuring its admissibility in court. This approach not only enhances the reliability of evidence but also streamlines the documentation and audit processes involved in forensic investigations.

One of the primary benefits of blockchain in digital forensics is its ability to ensure evidence immutability. Papers by Ahmad et al. [28], Chopade et al. [31], and Khan et al. [56] propose blockchain-based frameworks for managing the chain of custody, recording evidence metadata, and tracking evidence transfers. This immutability prevents tampering with evidence, ensuring its authenticity and admissibility in court. Furthermore, blockchain's decentralized and transparent nature fosters trust among stakeholders involved in investigations. Papers by Siaam et al. [29] and Hsu et al. [34] highlight how blockchain can provide a verifiable and auditable record of all interactions with evidence, eliminating the need for intermediaries and increasing transparency in the investigation process. Moreover, the application of blockchain in digital forensics extends beyond traditional evidence management. Papers by Jin et al. [35] and Cong et al. [53] explore the use of blockchain for investigating cryptocurrency-related crimes, tracking the flow of funds, and identifying perpetrators. This demonstrates the potential of blockchain to address the unique challenges posed by the decentralized and anonymous nature of cryptocurrencies.

While reviewing the selected papers to highlight the benefits of utilizing blockchain in digital forensic investigations, we identified six common benefits: evidence integrity, chain of custody, transparency, auditability, security, and scalability. These benefits were chosen to categorize the perspectives on how blockchain can enhance digital forensic investigations because they represent core attributes essential for maintaining the integrity, security, and transparency of digital evidence. Evidence integrity and chain of custody are fundamental in ensuring that data remain untampered with, and its history is documented. Transparency and auditability are crucial for creating a trustworthy and verifiable trail of transactions and enhancing accountability. Security ensures the protection of sensitive data from unauthorized access and cyberattacks. Scalability addresses the need for blockchain systems to efficiently handle increasing volumes of transactions and data. The perspective of each author regarding how the blockchain can enhance digital forensic investigations was analysed in relation to these six features and summarized in Table 3.

**Table 3.** Benefits of using blockchain to enhance digital forensics investigations as identified by each author.

| Citation | Evidence Integrity | Chain of Custody | Transparency | Auditability | Security | Scalability |
|---|---|---|---|---|---|---|
| Ahmad et al. [28] | ✓ | × | × | × | ✓ | × |
| Siaam et al. [29] | × | × | ✓ | × | × | × |
| Billard [30] | × | ✓ | × | × | × | × |
| Cebe et al. [1] | × | ✓ | ✓ | ✓ | × | × |
| Chopade et al. [31] | ✓ | × | × | ✓ | × | × |
| Hsu et al. [34] | × | × | × | × | ✓ | × |
| Khan et al. [36] | × | ✓ | ✓ | × | × | × |
| Li et al. [38] | ✓ | × | ✓ | ✓ | × | × |
| Li et al. [7] | × | ✓ | ✓ | × | × | × |
| Mahrous et al. [39] | ✓ | × | × | × | × | × |
| Muyambo et al. [40] | × | ✓ | ✓ | × | × | × |
| Ryu et al. [42] | × | × | × | ✓ | × | × |
| Sheelvanth et al. [43] | × | ✓ | × | × | × | × |
| Xiao et al. [6] | × | ✓ | × | × | ✓ | × |
| Zarpala and Casino [44] | ✓ | × | × | ✓ | × | × |
| Alqahtany and Syed [46] | × | × | ✓ | ✓ | × | × |
| Kumar et al. [19] | × | ✓ | ✓ | × | ✓ | × |
| Jacob and Kumar [49] | ✓ | × | ✓ | × | × | × |
| Akbarfam et al. [50] | ✓ | ✓ | × | × | × | × |
| Almutairi and Moulahi [52] | × | ✓ | ✓ | × | × | ✓ |
| Alqahtany and Syed [54] | ✓ | × | × | × | × | × |
| Khan et al. [56] | ✓ | × | ✓ | ✓ | ✓ | × |
| Ragu and S. [58] | ✓ | × | × | ✓ | × | × |
| Bonomi et al. [60] | ✓ | ✓ | × | × | × | × |
| Tian et al. [61] | × | × | ✓ | × | ✓ | ✓ |
| Lusetti et al. [62] | × | × | × | ✓ | × | ✓ |
| Verma et al. [63] | × | × | ✓ | × | ✓ | ✓ |
| Chen at al. [64] | ✓ | ✓ | ✓ | × | × | × |
| Awuson-David et al. [65] | ✓ | × | × | × | ✓ | × |
| Olukoya et al. [66] | × | ✓ | ✓ | × | × | × |
| Burri et al. [67] | ✓ | ✓ | ✓ | × | × | × |

Researchers have consistently recognized the potential of blockchain to enhance evidence integrity. Blockchain's decentralized ledger ensures that once data are recorded, they cannot be altered or deleted, providing a tamper-proof record. For instance, Ahmad et al. [28] and Akbarfam et al. [50] highlight blockchain's capability to maintain the integrity of evidence through its immutability. This characteristic is crucial in sectors such as healthcare, legal, and digital forensics, where the authenticity of data over time is paramount. By leveraging cryptographic techniques, blockchain guarantees that any tampering attempts would be easily detectable, thus preserving the original state of the evidence. The chain of custody is also another critical feature in various fields, particularly in legal and forensic contexts, where the history of evidence handling needs to be meticulously documented. Billard [30] and Khan et al. [36] emphasize blockchain's ability to provide a transparent and immutable record of every transaction and transfer of evidence. This ensures that every change of hands is logged with timestamps and participant identities, creating a reliable and auditable trail. Blockchain's transparency and immutability help prevent unauthorized access and modifications, ensuring the integrity and trustworthiness of the chain of custody.

Transparency is another significant benefit of blockchain in the digital forensics context, as noted by researchers like Muyambo et al. [17], Alqahtany and Syed [46], and Chen et al. [64]. Blockchain's distributed ledger allows all participants in a network to have access to the same data in real time. This transparency is particularly valuable in supply chain management, public records, and financial transactions, where stakeholders require visibility into processes to build trust. For instance, Li et al. [7] discuss how blockchain can make every transaction visible and verifiable by all parties, reducing the chances of fraud and increasing accountability. Auditability is also a core feature of blockchain that supports thorough and efficient auditing processes. Cebe et al. [1] and Ryu et al. [42] illustrate how blockchain's comprehensive and immutable logs facilitate easy and reliable audits. Each transaction is recorded with a timestamp and is linked to previous transactions, forming a chronological chain that auditors can follow without the risk of missing or altered data. This capability is particularly useful in financial auditing, regulatory compliance, and quality assurance, where maintaining a clear and accessible record is crucial for transparency and accountability.

Security is a fundamental aspect of blockchain technology, extensively explored by researchers such as Hsu et al. [34], Kumar et al. [19], and Khan et al. [56]. Blockchain's cryptographic foundations ensure that data are securely encrypted and protected against unauthorized access and cyberattacks. Each block in the chain contains a hash of the previous block, a timestamp, and transaction data, making it extremely difficult for malicious actors to alter the information. This high level of security is beneficial in protecting sensitive data across various applications, including finance, healthcare, and governmental operations, where data breaches can have severe consequences. Scalability is also a crucial consideration for the widespread adoption of blockchain, as discussed by Almutairi and Moulahi [52], Tian et al. [61], and Lusetti et al. [62]. While blockchain's inherent security and transparency are advantageous, the technology must be able to handle an increasing number of transactions efficiently. Researchers highlight ongoing efforts to improve blockchain scalability through techniques such as sharding, off-chain transactions, and improved consensus algorithms. These advancements aim to ensure that blockchain can support large-scale applications, from global supply chains to extensive financial networks, without compromising performance or security.

The selected papers demonstrate that blockchain offers several key advantages in digital forensics, including enhanced data integrity, transparent audit trails, and decentralized trust mechanisms. By leveraging cryptographic hashing, smart contracts, and decentralized consensus mechanisms, blockchain ensures that forensic evidence remains tamper-proof and verifiable throughout its lifecycle. Moreover, blockchain's ability to store and timestamp forensic data securely and transparently facilitates collaboration among multiple stakeholders, including law enforcement agencies, forensic experts, and legal professionals. However, several challenges remain, such as integration with existing forensic systems and legal considerations surrounding data privacy and admissibility in court. Addressing these challenges will be crucial for realizing the full potential of blockchain in digital forensics.

**RQ3: What are the digital forensic frameworks and methodologies used in blockchain forensics?**

Blockchain-based forensic frameworks and methodologies present a sophisticated approach to digital evidence management by leveraging the decentralized and immutable nature of blockchain technology. Table 4 provides a summary of the blockchain-based forensic frameworks and methodologies that were discussed in the selected papers.

**Table 4.** Summary of the blockchain-based forensic frameworks and methodologies discussed in the selected papers.

| Citation | Digital Forensic Frameworks and Methodologies |
|---|---|
| Ahmad et al. [28] | The proposed framework consists of three layers: an evidence layer with smart locks for secure evidence storage, a blockchain layer using a private Ethereum for tamper-proof metadata recording, and a network layer enabling communication among authorized parties. |
| Siaam et al. [29] | The proposed IoT probe framework involves four key components: Transaction Creation, Insertion into Blockchain Ledgers, Escrow Service, and Investigation Analysis. |
| Billard [30] | This paper proposes a digital forensic framework consisting of three key components: the DEI, the Forensics Confidence Rating (FCR), and the GDT for timeline reconstruction and presentation. |
| Cebe et al. [1] | The proposed Block4Forensic (B4F) consists of a forensic daemon, a permissioned blockchain, and various stakeholders. B4F's forensic daemon mirrors collection, the blockchain acts as secure storage, and stakeholder interactions represent analysis and reporting. |
| Chopade et al. [31] | The proposed blockchain-based framework includes evidence creation, evidence hash transfer, and evidence display. This framework enhances the reliability and security of digital evidence throughout the investigation lifecycle. |
| Hsu et al. [34] | The proposed blockchain-based framework for IoT includes components for the acquisition of sensor logs, analysis of log data, and presentation of evidence in a tamper-proof and legally defensible manner. The framework also utilizes a signature chain to ensure data integrity and non-repudiation. |
| Khan et al. [36] | The proposed MF-Ledger framework consists of a private, permissioned network where stakeholders securely interact using smart contracts to record and manage evidence. This ensures transparency, immutability, and secure storage of the evidence chain of custody. |
| Li et al. [38] | The proposed LEChain framework manages evidence from its collection by victims, witnesses, and monitoring devices, through analysis by crime scene analysts, to its upload and access via the blockchain, closing in a court trial. |
| Li et al. [7] | The proposed IoTFC framework consists of users and IoT devices, Merkle tree, blocks, and smart contracts. The output of the framework includes a comprehensive view of evidence items, continuous integrity, immutability and audibility, tamper-proof environment, full provenance, and traceability. |
| Mahrous et al. [39] | The proposed framework consists of evidence acquisition, a forensic-chain framework, and blockchain-based evidence management. It involves acquisition for uploading fingerprinted records to the blockchain, analysis to verify the authenticity of the evidence items, and reporting to generate a report for the investigation |
| Muyambo et al. [40] | The proposed DFRMIV framework consists of four main layers: the acquisition layer to gather evidence from the blockchain network, the preservation layer to use cryptographic techniques and secure storage methods to preserve the integrity of the evidence, the analysis layer to analyse the preserved data to identify any anomalies or evidence of tampering, and the reporting layer to report the findings. |
| Ryu et al. [42] | The proposed framework consists of three layers: the IoT device layer for gathering the evidence, the blockchain layer to utilize a block structure with a block header and transaction data, where each transaction includes a transaction ID, digital signature, and PUF IDs of the sender and receiver devices, and the participants' layer where analysis and reporting of evidence occur. |
| Sheelvanth et al. [43] | The proposed framework supports evidence acquisition through secure storage on the blockchain, analysis by providing access to authorized personnel and reporting through transparent and auditable records. |

**Table 4.** *Cont.*

| Citation | Digital Forensic Frameworks and Methodologies |
|---|---|
| Xiao et al. [6] | The proposed framework comprises a decentralized blockchain storage mechanism, smart contract mechanisms for evidence retrieval and tracing, a token mechanism for access control, and an efficient batch consensus algorithm. |
| Zarpala and Casino [44] | The proposed framework consists of a smart contract deployed on the Ethereum blockchain that records all actions performed during the investigation. The framework also includes a mechanism for evidence custody changes and destruction, ensuring a complete and auditable trail of events. |
| Alqahtany and Syed [46] | The proposed framework consists of data preservation, where a forensic image of the evidence is created; data acquisition, where the evidence is collected and analysed; and finally reporting, where the findings are documented. |
| Kumar et al. [19] | The proposed IoF consists of four layers: Edge-IoF, Fog-IoF, Consortium-IoF, and Cloud Storage. Edge-IoF gathers evidence from heterogeneous devices, Fog-IoF performs forensic analysis and maintains the chain of custody, Consortium-IoF facilitates collaboration among various stakeholders, and Cloud Storage stores the evidence. |
| Jacob and Kumar [49] | The proposed framework involves collecting digital evidence, hashing it, and storing it in the blockchain using a hash directory to prevent duplicate data. The evidence stored on the blockchain is then analysed, and the findings are documented. |
| Akbarfam et al. [50] | The proposed ForensiBlock framework consists of three main components: blockchain, user nodes, and off-chain storage. The blockchain serves as a decentralized ledger for recording transactions and data changes. User nodes represent authorized individuals involved in investigations, while off-chain storage securely stores digital forensic data and maintains provenance records. |
| Almutairi and Moulahi [52] | The proposed framework uses federated learning for privacy-preserving model training on IoT devices, followed by model aggregation on a lightweight blockchain. This process involves the acquisition of data from IoT devices, analysing them through federated learning, preservation of model parameters on the blockchain, and reporting results based on the aggregated models. |
| Alqahtany and Syed [54] | The proposed framework consists of data collection, VPN traffic analysis using CNN and GNN models, and secure logging on a blockchain. The output of the framework is a comprehensive forensic report that includes the identification of the VPN protocol, the classification of VPN traffic, and the secure storage of the evidence on the blockchain. |
| Khan et al. [56] | The proposed framework utilizes blockchain forensics tools to collect blockchain data, analyse transactions and addresses, and identify suspicious activities. The output is a report that includes identified high-risk activities, real-time analysis, and a strong audit trail. |
| Ragu and S. [58] | The proposed framework consists of six stages: identification, preservation, collection, examination, analysis, and presentation. Blockchain is integrated into the framework to automate the acquisition and preservation phases, improving efficiency and reliability while providing continuous fraud detection and forensic readiness. |
| Bonomi et al. [60] | The proposed B-CoC framework consists of seven phases: investigation initiation, incident reporting, preparation and planning, evidence identification, acquisition, preservation, analysis, presentation, and investigation closure. Blockchain is used to address issues related to evidence integrity, chain of custody, and data privacy. |
| Tian et al. [61] | The proposed Block-DEF framework consists of three layers: a service layer for evidence submission and retrieval, a blockchain layer for consensus and storage of evidence information, and a network layer for communication. The evidence stored in the blockchain is then analysed, and the findings will be documented. |
| Lusetti et al. [62] | The proposed CC framework combines a secure online file storage system with a private implementation of the Hyperledger FabricTM blockchain. The framework encompasses encryption, file hashing, and a robust chain-of-custody mechanism. The framework includes the acquisition of digital files, processing through encryption and hashing, analysis of file properties, and reporting of access logs and evidence in a secure and verifiable manner. |
| Verma et al. [63] | The proposed NyaYa framework comprises four phases: registration of judicial stakeholders on the BC, case registration with meta-hash keys in the public BC to reference external off-chain interplanetary file storage, chronological updates of investigative findings among law enforcement agencies on the BC and IPFS, and case hearing and settlement through smart contracts. |

**Table 4.** *Cont.*

| Citation | Digital Forensic Frameworks and Methodologies |
|---|---|
| Chen et al. [64] | The proposed framework consists of data acquisition (screenshots and source code), data preservation (Factom blockchain), and data analysis (verification of SHA256 hash values, blockchain queries, and analysis of Bitcoin storage content). |
| Awuson-David et al. [65] | The proposed BCFL framework consists of four key components: blockchain distributed ledger technology (DLT), smart contracts, data validation, and immutability. These components are used to acquire, preserve, analyse, and report digital evidence in the cloud ecosystem. |
| Olukoya et al. [66] | The proposed framework utilizes Parnassus to record and manage forensic actions throughout the investigation lifecycle. This framework encompasses four key operations: acquisition of evidence using Parnassus to store evidence details, preservation of evidence integrity through blockchain immutability, analysis of evidence using tools integrated with Parnassus, and reporting of findings. |
| Burri et al. [67] | The proposed e-CoC framework includes a secure ledger managed by a trusted entity, with blocks linked by hash values. The e-CoC ledger is periodically secured to a public blockchain for tamper-proof verification. Digital evidence is hashed, and the hash values are timestamped and stored in the e-CoC ledger. The evidence stored in the blockchain is then analysed, and the findings will be documented. |

Numerous proposed frameworks leverage blockchain's inherent properties like immutability, transparency, security, and decentralization to address challenges in evidence management. Despite the diverse designs of the frameworks discussed in the selected papers of the literature, these frameworks share several common aspects. Each framework integrates blockchain to ensure the immutability and integrity of evidence, which is a crucial feature for maintaining the chain of custody and preventing tampering. The use of smart contracts is also widespread, providing automated and transparent processes for evidence management.

While the blockchain forensic frameworks reviewed share many common elements, they also exhibit significant differences in their focus areas, technical implementations, and the specific challenges they address. These differences highlight the versatility of blockchain technology in digital forensics and how various approaches can be leveraged to address distinct aspects of forensic investigations. For example, Hsu et al. [34] introduce a unique approach by incorporating a signature chain to ensure data integrity and non-repudiation, which is a feature not commonly emphasized in other frameworks. This method is particularly valuable in maintaining the authenticity of data throughout the forensic process, ensuring that any tampering attempts are easily detectable. Khan et al. [36] utilize smart contracts within a private and permissioned blockchain network to facilitate interaction between stakeholders involved in evidence management. This approach highlights the importance of managing relationships and transactions between different entities in a forensic investigation, ensuring transparency and accountability.

Li et al. [38] take a broader approach by including a comprehensive process that spans from evidence collection by victims and witnesses to its presentation in court. This framework is notable for its end-to-end scope, addressing the entire forensic process rather than focusing on a single aspect. On the other hand, Mahrous et al. [39] adopt a more narrowly focused but deeply technical approach by concentrating on uploading fingerprinted records to the blockchain for authenticity verification. This method is particularly effective in ensuring the veracity of specific pieces of evidence, though it does not address the broader forensic workflow.

Some frameworks focus on securing evidence at the source using smart locks [28], Escrow Services [29], or decentralized storage mechanisms [6]. Others prioritize secure storage and chain of custody management through blockchain-based logging [61,63,67]. Frameworks differ in their analytical capabilities, with some frameworks utilizing smart contracts for evidence retrieval and tracing [6], while others provide a comprehensive view of evidence items and their provenance [7]. Some frameworks also incorporate machine learning techniques for analysis [52,54]. Other frameworks emphasize cryptographic techniques and secure storage methods for evidence preservation, with additional layers for anomaly detection and reporting [40,42]. Some frameworks provide access control mechanisms and efficient consensus algorithms to manage evidence securely and transparently [6,43]. Other frameworks incorporate a smart contract mechanism for comprehensive tracking of custody changes and evidence destruction to ensure a complete audit trail [44,54,63]. Also, some frameworks emphasize collaborative forensic investigations to enable secure communication and data sharing among authorized parties [19,36].

In summary, while the core principles of blockchain-based forensic frameworks revolve around ensuring the integrity, immutability, and transparency of digital evidence, the specific implementations and additional features vary significantly. These differences cater to diverse forensic requirements and environments, demonstrating the flexibility and adaptability of blockchain technology in enhancing digital forensic investigations.

**RQ4: What are the common applications of blockchain-based digital forensic investigation frameworks?**

The applicability of blockchain-based forensic frameworks has been recognized in various applications to demonstrate their flexibility in addressing diverse challenges. For instance, in cryptocurrency investigations, blockchain frameworks have been instrumental in tracing illegal transactions and identifying perpetrators, leveraging the immutable record of transactions on the blockchain. This section provides a summary of the common applications where blockchain-based forensic frameworks have been applied, based on the selected papers in this systematic review, as summarized in Table 5. These applications are categorized into seven categories: IoT forensics, cloud forensics, vehicular forensics, mobile forensics, multimedia forensics, Internet voting systems, and the dark web.

**Table 5.** Summary of the common applications where blockchain-based forensic frameworks were applied.

| Citation | IoT Forensics | Cloud Forensics | Vehicular Forensics | Mobile Forensics | Internet Voting | Dark Web | Multimedia Forensics |
|---|---|---|---|---|---|---|---|
| Akinbi et al. [24] | ✓ | × | × | × | × | × | × |
| Siaam et al. [29] | ✓ | × | × | × | × | × | × |
| Cebe et al. [1] | × | × | ✓ | × | × | × | × |
| Hsu et al. [34] | ✓ | × | × | × | × | × | × |
| Jin et al. [35] | × | × | × | × | × | ✓ | × |
| Khan et al. [36] | × | × | × | × | × | × | ✓ |
| Khanji et al. [37] | ✓ | × | × | × | × | × | × |
| Li et al. [7] | ✓ | × | × | × | × | × | × |
| Mahrous et al. [39] | ✓ | × | × | × | × | × | × |
| Muyambo et al. [40] | × | × | × | × | ✓ | × | × |
| Ryu et al. [42] | ✓ | × | × | × | × | × | × |
| ×iao et al. [6] | ✓ | × | × | × | × | × | × |
| Sakshi et al. [45] | ✓ | × | × | × | × | × | × |
| Alqahtany and Syed [46] | × | ✓ | × | × | × | × | × |
| Kumar et al. [19] | ✓ | × | × | × | × | × | × |
| Almutairi and Moulahi [52] | ✓ | × | × | × | × | × | × |
| Alqahtany and Syed [54] | × | × | × | ✓ | × | × | × |
| Khan et al. [56] | ✓ | × | × | × | × | × | × |
| Ragu and S. [58] | × | ✓ | × | × | × | × | × |

**Table 5.** *Cont.*

| Citation | IoT Forensics | Cloud Forensics | Vehicular Forensics | Mobile Forensics | Internet Voting | Dark Web | Multimedia Forensics |
|---|---|---|---|---|---|---|---|
| Brotsis et al. [59] | ✓ | × | × | × | × | × | × |
| Awuson-David et al. [65] | × | ✓ | × | × | × | × | × |
| Burri et al. [67] | × | ✓ | × | × | × | × | × |

1. IoT Forensics

The integration of blockchain into IoT forensics has gained significant attention from researchers. The key objective in this domain is to enhance the integrity, traceability, and transparency of forensic data. Akinbi et al. [24] conducted a comprehensive systematic review to understand how blockchain can improve IoT forensic investigations. Their review sheds light on the current challenges and future research directions, emphasizing the potential of blockchain to address issues such as evidence tampering and data integrity in IoT environments. Also, Siaam et al. [29] introduced the Probe-IoT framework, which utilizes a public digital ledger to address evidence spoliation and lack of transparency in IoT crime cases. By recording interactions between IoT devices, users, and cloud services on a blockchain, the framework ensures that forensic investigators can trace the flow of data and identify potential perpetrators, thus enhancing the transparency and reliability of forensic investigations. Hsu et al. [34] also proposed an autonomous log storage management protocol for IoT that integrates blockchain mechanisms and a “signature chain” concept. This approach provides robust identity verification, data integrity, and tamper resistance, making it particularly suitable for digital forensic investigations in IoT environments. Similarly, Li et al. [7] introduced IoT Forensic-Chain (IoTFC), a framework that records all examination operations in a chain of blocks, ensuring the traceability and integrity of forensic processes in IoT systems.

Furthermore, Mahrous et al. [39] enhanced IoT digital forensics by incorporating fuzzy hashing into the blockchain’s Merkle tree. This technique improves the detection of benign or malicious alterations in evidence, which traditional hashing methods might miss, so ensuring the authenticity and integrity of forensic data. Ryu et al. [42] proposed a blockchain framework that stores all IoT device communications as transactions, simplifying the chain of custody process and enhancing data integrity. Kumar et al. [19] developed the IoF framework, which uses a consortium blockchain and lattice-based cryptography to secure evidence in IoT forensics. This approach addresses transparency and heterogeneity issues prevalent in IoT systems. Also, Brotsis et al. [59] reviewed recent blockchain-enabled IoT forensic frameworks and implemented a novel platform using Hyperledger Fabric. Their evaluation of a virtualized testbed demonstrated the platform’s effectiveness in enhancing forensic investigations in IoT environments. These contributions highlight the potential of blockchain in IoT forensics to offer innovative solutions to established challenges and pave the way for more secure and transparent forensic practices.

2. Cloud Forensics

One of the primary concerns in cloud forensics is ensuring the integrity and security of evidence collected from decentralized and often opaque cloud services. Several key papers have explored how blockchain can enhance cloud forensic processes by providing immutable, transparent, and tamper-proof logs and records. Ragu and S. [58] propose a cloud forensic framework that integrates SDN with blockchain to predict privacy leaks. This approach leverages blockchain’s decentralized nature to enhance the security and reliability of forensic data and address the concerns of centralized evidence collection and integrity. Awuson-David et al. [65] introduce the BCFL framework, which integrates a permissioned blockchain within the cloud to maintain tamper-proof log evidence to improve compliance with regulations like GDPR. This framework ensures a secure chain of custody for forensic evidence and enhances transparency and accountability in cloud forensic processes. Burri et al. [67] focus on developing an electronic chain of custody (e-CoC) ledger using a private blockchain managed by a trusted entity and periodically updated on a public blockchain. This solution ensures chronological and independently verifiable management of digital evidence, addressing the critical need for maintaining the integrity and authenticity of forensic evidence for legal proceedings and investigations. The common goal across these papers is to enhance the security and reliability of forensic investigations in cloud environments, ensuring that digital evidence remains trustworthy and admissible in legal contexts.

3. Vehicular Forensics

Vehicular forensics involves investigating accidents, crimes, and other incidents involving vehicles. Traditional methods often rely on physical evidence, which can be easily tampered with or lost. Blockchain technology offers a secure and tamper-proof solution for managing vehicle data and ensuring the integrity of evidence. Cebe et al. [1] proposed a framework called Block4Forensic (B4F). The framework provides a secure and trustworthy platform for collecting and analysing vehicle data, ensuring its integrity and authenticity. It incorporates privacy-preserving mechanisms to protect sensitive vehicle data during analysis. It also enables trustless and traceable post-accident analysis, facilitating dispute resolution and identifying faulty parties.

4. Mobile Forensics

Mobile forensics involves the investigation and analysis of mobile devices to uncover evidence related to blockchain transactions and activities. Mobile forensics is the process of recovering digital evidence from mobile devices, which includes extracting data such as text messages, emails, call logs, photos, and application data. The extracted data are then analysed to find relevant information for the investigation, such as patterns, timelines, and connections between different pieces of data. Alqahtany and Syed [54] proposed a framework for mobile VPN forensics that integrates blockchain with deep learning models. In this framework, blockchain serves as a secure, tamper-proof ledger for recording VPN transactions to enhance the integrity and admissibility of mobile forensic evidence.

5. Multimedia Forensics

Multimedia forensics involves the investigation and analysis of digital media, such as images, videos, and audio files, to uncover evidence related to blockchain transactions and activities. This process benefits from the immutable and transparent nature of blockchain technology, which can securely record and verify the chain of custody and authenticity of multimedia evidence. Khan et al. [56] proposed a blockchain-based digital forensic framework for multimedia forensics investigations using Hyperledger Sawtooth. The proposed system employs a private permissioned network to enable secure collaboration among stakeholders to facilitate the exchange of video surveillance data and chain-of-custody information.

6. Internet Voting Systems

Internet voting systems are increasingly being used to facilitate democratic processes. However, concerns about security and integrity persist, as these systems are vulnerable to manipulation and fraud. Blockchain technology offers a robust solution to address these concerns, enhancing the security and transparency of online voting. Muyambo et al. [40] proposed a blockchain-based digital forensic-ready internet voting system DFRMIV, which addresses issues of transparency, privacy, integrity, confidentiality, and auditability in online voting systems. DFRMIV provides a transparent and auditable record of the voting process, allowing for the verification of vote counts and the identification of any irregularities. It incorporates privacy-preserving mechanisms to protect voter identities and ensure the confidentiality of votes. It also utilizes blockchain's immutable ledger to ensure the integrity of votes and hold accountable all parties involved in the voting process.

7. Dark Web

Blockchain-based forensic solutions play a crucial role in tracking dark web activities by leveraging the transparency and traceability of blockchain transactions. Forensic investigators can analyse blockchain records to trace the flow of funds associated with illegal activities on the dark web. By following the movement of cryptocurrency from one address to another, investigators can map out networks of transactions, identify patterns, and uncover connections between different entities involved in illegal activities. Jin et al. [35] propose a methodology for tracing operators of illegal dark websites through cryptocurrency transactions. It emphasizes the importance of tracking the flow of funds on the blockchain to link Bitcoin addresses to real-world bank accounts, which can be crucial in digital forensic investigations.

**RQ5: What are the legal and regulatory challenges in conducting a forensic investigation on a blockchain system?**

Conducting a forensic investigation on a blockchain system presents unique legal and regulatory challenges that arise from the decentralized and immutable nature of blockchain. One of the primary legal challenges in blockchain forensics is jurisdiction. Blockchain networks are inherently decentralized and global, often operating across multiple countries simultaneously. This decentralization means that transactions recorded on a blockchain can involve parties from different legal jurisdictions, each with its own laws and regulations. Investigators must navigate a maze of international laws to determine which jurisdiction's laws apply to a particular case. This complexity is compounded by the anonymity of blockchain transactions, making it difficult to determine the locations of the parties involved. Without clear jurisdiction, obtaining legal authorizations such as search warrants and subpoenas can be problematic, potentially hindering the investigation [6,7].

Siaam et al. [29] acknowledge the need for a scalable and policy-compliant blockchain-based evidence-collection system, addressing jurisdictional differences in legal systems and ensuring that blockchain transactions are low-cost or free for practical adoption. Furthermore, their paper emphasizes the importance of combining the chain of custody with a hybrid blockchain architecture to maximize security and computational efficiency while also ensuring the system's scalability and adherence to legal standards. Also, Al-Khateeb [57] highlights the legal and regulatory challenges in conducting forensics investigations on blockchain systems by emphasizing the need for a tamper-proof audit trail. It acknowledges the complexity of multijurisdictional investigations and the need for standardized guidelines to ensure compliance with digital investigation principles.

Another challenge is the interpretation and admissibility of blockchain evidence. The decentralized and distributed nature of blockchain systems, with no central authority controlling data, requires investigators to grapple with the concept of "truth" in a decentralized environment. The immutability of blockchain data, while ensuring data integrity, also eliminates the possibility of altering or modifying evidence, potentially hindering traditional forensic techniques that rely on analysing changes in data over time. This raises questions about how to establish the authenticity and reliability of blockchain evidence, especially when dealing with complex transactions and intricate network interactions [68,69].

Billard [30] highlights legal challenges related to ensuring the reliability and accuracy of blockchain-based forensic processes, as well as the difficulties in integrating blockchain evidence with traditional legal standards. Similarly, Lusetti et al. [62] discuss the legal and regulatory challenges of using blockchain for the custody of digital files in forensic medicine. It highlights the importance of ensuring data integrity and security, as well as compliance with relevant regulations. Tian et al. [61] explore the legal and regulatory challenges of utilizing blockchain for digital evidence management. It emphasizes the need for a secure and tamper-proof system to ensure the integrity and admissibility of digital evidence in court. Also, Verma et al. [63] discussed the legal and regulatory challenges of implementing a blockchain-based electronic law record management scheme. It emphasizes the importance of ensuring data privacy, security, and compliance with existing legal frameworks. Alqahtany and Syed [46] acknowledge the importance of ensuring the admissibility of evidence in legal proceedings and mention the need for a clear record of the evidence's history. Chen et al. [64] and Brotsis et al. [59] discuss the legal and regulatory challenges of using blockchain for electronic evidence generation and IoT, respectively. They highlight the need for a secure and verifiable system that meets legal requirements for admissibility.

The lack of established legal frameworks specifically tailored to blockchain forensics poses another significant challenge. Existing legal frameworks designed for traditional digital evidence may not adequately address the unique characteristics of blockchain data. This creates uncertainty about the legal standards for collecting, preserving, and presenting blockchain evidence in court. The need for clarity in legal frameworks is crucial to ensure the admissibility of blockchain evidence and the effectiveness of forensic investigations [68]. Cebe et al. [1] acknowledge the lack of universal standards for collecting, examining, and analysing data from digital devices in vehicles, highlighting the need for a framework that ensures data integrity and user privacy. Sheelvanth et al. [43] also highlights the need for internationally recognized standards to codify forensic investigative procedures in complex digital environments like the IoT. This suggests a lack of clear legal frameworks for handling evidence stored on blockchains.

In summary, the unique attributes of blockchain technology necessitate significant legal and regulatory adaptations for effective forensic investigations. Addressing jurisdictional ambiguities, ensuring the reliability and admissibility of evidence, and developing specific legal frameworks tailored to blockchain's unique characteristics are critical steps. Future research should focus on creating scalable, policy-compliant systems, establishing standardized guidelines, and developing secure, tamper-proof mechanisms to manage and present blockchain evidence in court. Enhanced international cooperation and harmonized regulations will be essential to navigate the complexities of blockchain forensics and ensure effective enforcement of the law in this evolving technological landscape.

## 6. Open Issues and Future Directions

Blockchain forensics has become an essential field within the landscape of digital forensics, especially with the increasing use of cryptocurrencies and blockchain technology across various domains. However, this area faces numerous challenges that need to be addressed, and several future research directions still need to be investigated to improve the efficacy of forensic investigations and keep up with evolving technology. These issues and future research directions include the following:

### 6.1. Lack of Standardization

There is a lack of standardized methodologies and tools in blockchain forensics. Different blockchain platforms have unique structures and functionalities, necessitating diverse forensic approaches. The absence of standardization hinders the development of universally applicable forensic tools and techniques, leading to inefficiencies and inconsistencies in investigations [33]. For instance, forensic tools available for blockchain analysis are often developed independently and tailored to specific blockchains or use cases, leading to inconsistencies in functionality and interoperability. Tools like Chainalysis and CipherTrace are widely used for Bitcoin and Ethereum but may not be as effective for other blockchain platforms [70].

Moreover, interpreting blockchain data requires a deep understanding of the specific blockchain's structure and transaction protocols. Without standardized methodologies for data interpretation, different investigators might arrive at different conclusions when analysing the same data. This lack of consensus can undermine the credibility of forensic findings and complicate legal proceedings. Also, the rapid evolution of blockchain technology further complicates the situation, requiring investigators to constantly adapt to new advancements [44]. Hence, there is a need for more research to develop standardized and universally applicable methodologies and tools to effectively investigate blockchain transactions in a forensically sound way as well as to utilize blockchain effectively in digital forensics investigations.

### *6.2. Regulatory and Legal Issues*

One of the most significant challenges in blockchain forensics is the lack of a unified regulatory framework. Different countries have varying regulations concerning blockchain and cryptocurrencies, which can create substantial obstacles for forensic investigators. For instance, while some countries like Japan and Malta have embraced cryptocurrencies with supportive regulations, others like China and India have imposed strict bans or severe restrictions [71]. This discrepancy means that an action deemed legal and compliant in one jurisdiction might be illegal in another, complicating international investigations. Hence, there is a need for international cooperation to balance regulations concerning blockchain and cryptocurrencies. Developing global standards can help streamline forensic investigations and ensure consistency in the legal treatment of blockchain evidence.

The global and decentralized nature of blockchain technology means that forensic investigations often span multiple jurisdictions. This cross-border nature introduces legal complexities, as investigators must navigate the legal requirements and regulations of each involved jurisdiction. Mutual legal assistance treaties and other forms of international cooperation can help, but these processes are often slow and bureaucratic. Additionally, differences in legal systems can result in conflicting requirements for evidence collection and preservation. For example, what constitutes a legal search and seizure in one country might be considered a violation of rights in another, complicating the collection of blockchain evidence across borders [72]. Therefore, jurisdictions should work towards creating comprehensive legal frameworks that recognize the unique characteristics of blockchain evidence. In addition, future research should focus on proposing frameworks for international cooperation and legal standards that address the decentralized nature of blockchain.

### *6.3. Scalability Challenges*

Scalability in blockchain forensics is a critical concern due to the rapidly increasing volume of transactions and the complexity of blockchain networks. As blockchain adoption grows, the capacity to process and analyse vast amounts of data efficiently becomes increasingly challenging [73]. With the widespread adoption of blockchain technology, the number of transactions recorded on various blockchains is growing exponentially. For instance, Bitcoin processes around 300,000 transactions per day, while Ethereum handles even more due to its extensive use in decentralized applications and smart contracts [74].

Furthermore, forensic analysis of blockchain data involves resource-intensive processes, including data extraction, parsing, indexing, and pattern recognition. These processes require significant computational power and storage capacity, especially when dealing with large-scale blockchain networks like Ethereum or Bitcoin. Scalability issues arise when current forensic tools and infrastructure cannot efficiently manage these resource demands, leading to slower analysis and increased costs [22]. Therefore, future research should focus on upgrading computational infrastructure to handle large-scale data processing. This includes leveraging cloud computing and distributed computing technologies to ensure that forensic tools can scale according to the volume and complexity of the data being analysed.

### *6.4. Applicability of Blockchain Forensic Frameworks*

The real-world applicability of blockchain forensic frameworks faces several significant challenges that hinder their widespread adoption and effectiveness. One of the primary challenges is that the frameworks must be adaptable to the diverse range of blockchain platforms, each with its unique protocols, structures, and encryption methods. A framework designed for one specific blockchain may not easily transfer to another, limiting its utility in a multi-blockchain environment. Also, the high costs associated with implementing these frameworks, including the need for specialized hardware, software, and expertise, may limit their accessibility to larger organizations, leaving smaller entities and individuals at a disadvantage [6,69].

Furthermore, the novelty of the frameworks is often constrained by the inherent complexity of blockchain technology, which may limit their usability. Highly innovative forensic methods might be too complex for widespread adoption, requiring deep technical knowledge that most law enforcement agencies or cybersecurity professionals may not possess. This creates a gap between theoretical advancements and practical utility, where even the most novel approaches may fail to gain traction if they cannot be easily implemented or understood by practitioners. Hence, future research should focus on simplifying forensic frameworks to enhance usability and reduce implementation costs.

### *6.5. Integration of AI and ML in Blockchain Forensics*

The integration of Artificial Intelligence (AI) and Machine Learning (ML) into blockchain forensics represents a significant advancement in the field. These technologies enhance the ability to analyse complex blockchain data, identify patterns, and automate forensic processes [75]. AI and ML are exceptionally proficient at recognizing patterns and detecting anomalies in large datasets. In blockchain forensics, these capabilities can be used to identify suspicious transactions and activities that deviate from typical behaviour. For example, ML algorithms can analyse transaction histories to flag irregular patterns that might indicate money laundering or other illegal activities [76]. In addition, predictive models can anticipate potential security threats and fraudulent activities. By analysing trends and patterns, these models can provide early warnings and help in proactive risk management. Therefore, future research should focus on integrating AI and ML into blockchain forensics to enhance pattern recognition, anomaly detection, and automation, thus improving the accuracy and efficiency of digital forensic investigations.

### *6.6. Education and Training*

As blockchain technology evolves, continuous education and training for forensic professionals are essential. Providing specialized training programs that cover the latest developments in blockchain technology, forensic tools, and investigative techniques can ensure that forensic experts are well-equipped to handle complex cases. As blockchain adoption grows, there is a need for skilled professionals who can investigate and analyse blockchain transactions effectively [77]. Universities and professional organizations can play significant roles in offering such educational opportunities. Developing advanced training modules that focus on specific aspects of blockchain forensics, such as smart contract analysis, cross-chain investigations, and AI-driven forensic techniques, can help professionals stay ahead of emerging challenges. Also, given the dynamic nature of blockchain technology, continuous learning and professional development are vital. Forensic professionals should be encouraged to engage in lifelong learning through advanced courses, workshops, conferences, and peer-to-peer learning networks. Also, Universities and professional organizations should work on designing targeted training programs to equip professionals with the necessary skills to tackle blockchain forensic challenges effectively.

## 7. Conclusions

Blockchain forensics is increasingly important in the digital age, addressing the unique investigative challenges posed by blockchain technology. As blockchain systems become integral to various industries, the need for specialized forensic methods to trace, analyse, and secure blockchain transactions has grown. The immutable and decentralized nature of blockchain, while providing security and transparency, also complicates traditional forensic approaches. Blockchain forensics offers the tools and techniques necessary to navigate these complexities, ensuring the integrity and reliability of digital evidence. This paper presented a comprehensive systematic literature review that explored the rapidly evolving field of blockchain forensics, emphasizing its critical importance in the digital age. This paper highlighted that while blockchain technology offers numerous security and transparency benefits, it also introduces unique challenges for digital forensic investigations due to its decentralized and immutable nature. Following a rigorous search strategy, a total of 46 articles were selected from an initial pool of 672 publications across multiple reputable databases. The selected articles were examined to evaluate recent advancements in blockchain forensic investigation models, methodologies, applications, and legal and regulatory challenges. This paper highlighted the significant interest in leveraging blockchain technology to enhance digital forensic investigations due to its inherent features of immutability, transparency, and security. This paper also identified that while blockchain technology offers promising solutions for tamper-proof evidence management and secure forensic processes, there are still challenges that need to be addressed, such as standardization, scalability, integration with AI and ML, education and training, and legal and regulatory implications.

**Author Contributions:** Conceptualization, H.F.A. and N.E.; methodology, H.F.A.; software, N.E.; validation, M.A.A. and H.S.L.; formal analysis, H.F.A.; investigation, H.F.A.; resources, N.E.; data curation, N.E.; writing—original draft preparation, H.F.A.; writing—review and editing, N.E., M.A.A. and H.S.L.; visualization, H.S.L.; supervision, H.F.A.; project administration, H.F.A. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** This research received no external funding. No new data were created or analysed in this study. Data sharing is not applicable to this article.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## References

1. Cebe, M.; Erdin, E.; Akkaya, K.; Aksu, H.; Uluagac, S. Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles. *IEEE Commun. Mag.* **2018**, *56*, 50–57. [CrossRef]
2. Akanfe, O.; Lawong, D.; Rao, H.R. Blockchain technology and privacy regulation: Reviewing frictions and synthesizing opportunities. *Int. J. Inf. Manag.* **2024**, *76*, 102753. [CrossRef]
3. Conti, M.; Kumar, G.; Lal, C.; Saha, R. Blockchain-Based Distributed and Secure Digital Forensic Investigation Systems. In *Blockchains: A Handbook on Fundamentals, Platforms and Applications*; Ruj, S., Kanhere, S.S., Conti, M., Eds.; Springer International Publishing: Cham, Switzerland, 2024; pp. 337–362, ISBN 978-3-031-32146-7.
4. Atlam, H.F.; Wills, G.B. Technical aspects of blockchain and IoT. In *Advances in Computers*; Kim, S., Deka, G.C., Zhang, P., Eds.; Role of Blockchain Technology in IoT Applications; Elsevier: Amsterdam, The Netherlands, 2019; Volume 115, pp. 1–39.
5. Mercan, S.; Cebe, M.; Aygun, R.S.; Akkaya, K.; Toussaint, E.; Danko, D. Blockchain-based video forensics and integrity verification framework for wireless Internet-of-Things devices. *Secur. Priv.* **2021**, *4*, e143. [CrossRef]
6. Xiao, N.; Wang, Z.; Sun, X.; Miao, J. A novel blockchain-based digital forensics framework for preserving evidence and enabling investigation in industrial Internet of Things. *Alex. Eng. J.* **2024**, *86*, 631–643. [CrossRef]
7. Li, S.; Qin, T.; Min, G. Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems. *IEEE Trans. Comput. Soc. Syst.* **2019**, *6*, 1433–1441. [CrossRef]
8. Dasaklis, T.K.; Casino, F.; Patsakis, C. SoK: Blockchain Solutions for Forensics. *arXiv* **2020**, arXiv:2005.12640.
9. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* **2021**, *372*, n71. [CrossRef]
10. Jena, S.K.; Barik, R.C.; Priyadarshini, R. A systematic state-of-art review on digital identity challenges with solutions using conjugation of IOT and blockchain in healthcare. *Internet Things* **2024**, *25*, 101111. [CrossRef]
11. Atlam, H.F.; Azad, M.A.; Alzahrani, A.G.; Wills, G. A Review of Blockchain in Internet of Things and AI. *Big Data Cogn. Comput.* **2020**, *4*, 28. [CrossRef]
12. Atlam, H.F.; Alenezi, A.; Alassafi, M.O.; Wills, G.B. Blockchain with Internet of Things: Benefits, Challenges, and Future Directions. *Int. J. Intell. Syst. Appl.* **2018**, *10*, 40. [CrossRef]
13. Atlam, H.F.; Wills, G.B. Intersections between IoT and distributed ledger. In *Advances in Computers*; Kim, S., Deka, G.C., Zhang, P., Eds.; Role of Blockchain Technology in IoT Applications; Elsevier: Amsterdam, The Netherlands, 2019; Volume 115, pp. 73–113.
14. Indrason, N.; Saha, G. Exploring Blockchain-driven security in SDN-based IoT networks. *J. Netw. Comput. Appl.* **2024**, *224*, 103838. [CrossRef]
15. Choi, W.; Woo, J.; Hong, J.W. Fractional non-fungible tokens: Overview, evaluation, marketplaces, and challenges. *Int. J. Netw. Manag.* **2024**, *34*, e2260. [CrossRef]

16. Garfinkel, S.L. Digital forensics research: The next 10 years. *Digit. Investig.* **2010**, *7*, S64–S73. [CrossRef]
17. Atlam, H.F.; Alenezi, A.; Alassafi, M.O.; Alshdadi, A.A.; Wills, G.B. Security, Cybercrime and Digital Forensics for IoT. In *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*; Peng, S.-L., Pal, S., Huang, L., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 551–577, ISBN 978-3-030-33596-0.
18. Atlam, H.F.; El-Din Hemdan, E.; Alenezi, A.; Alassafi, M.O.; Wills, G.B. Internet of Things Forensics: A Review. *Internet Things* **2020**, *11*, 100220. [CrossRef]
19. Kumar, G.; Saha, R.; Lal, C.; Conti, M. Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications. *Future Gener. Comput. Syst.* **2021**, *120*, 13–25. [CrossRef]
20. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2019**, *36*, 55–81. [CrossRef]
21. Aswal, P. Blockchain Nodes-Blockchain Council. Available online: https://www.blockchain-council.org/blockchain/blockchain-nodes/ (accessed on 26 August 2024).
22. Haque, E.U.; Shah, A.; Iqbal, J.; Ullah, S.S.; Alroobaea, R.; Hussain, S. A scalable blockchain based framework for efficient IoT data management using lightweight consensus. *Sci. Rep.* **2024**, *14*, 7841. [CrossRef]
23. Liberati, A.; Altman, D.G.; Tetzlaff, J.; Mulrow, C.; Gøtzsche, P.C.; Ioannidis, J.P.A.; Clarke, M.; Devereaux, P.J.; Kleijnen, J.; Moher, D. The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate healthcare interventions: Explanation and elaboration. *BMJ* **2009**, *339*, b2700. [CrossRef]
24. Akinbi, A.; MacDermott, Á.; Ismael, A.M. A systematic literature review of blockchain-based Internet of Things (IoT) forensic investigation process models. *Forensic Sci. Int. Digit. Investig.* **2022**, *42–43*, 301470. [CrossRef]
25. Atlam, H.F.; Oluwatimilehin, O. Business Email Compromise Phishing Detection Based on Machine Learning: A Systematic Literature Review. *Electronics* **2023**, *12*, 42. [CrossRef]
26. Atlam, H.F.; Azad, M.A.; Alassafi, M.O.; Alshdadi, A.A.; Alenezi, A. Risk-Based Access Control Model: A Systematic Literature Review. *Future Internet* **2020**, *12*, 103. [CrossRef]
27. Förstl, N.; Adler, I.; Süß, F.; Dendorfer, S. Technologies for Evaluation of Pelvic Floor Functionality: A Systematic Review. *Sensors* **2024**, *24*, 4001. [CrossRef] [PubMed]
28. 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, Virtual Event, Ireland, 25–28 August 2020; pp. 1–8.
29. Siaam, I.B.S.; Mahmud, N.; Titas, A.R. *Securing Digital Evidence with Blockchain*; Islamic University of Technology: Gazipur, Bangladesh, 2022.
30. Billard, D. Weighted Forensics Evidence Using Blockchain. In Proceedings of the 2018 International Conference on Computing and Data Engineering, Shanghai, China, 4–6 May 2018; pp. 57–61. [CrossRef]
31. Chopade, M.; Khan, S.; Shaikh, U.; Pawar, R. Digital Forensics: Maintaining Chain of Custody Using Blockchain. In Proceedings of the 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 12–14 December 2019; pp. 744–747.
32. Florid, M.I.; Mutaqin, H.; Purnamasari, P. Analyze the Application of Blockchain Technology in Digital Forensics and Hunt for Threats Lurking in Security. *Asian J. Manag. Entrep. Soc. Sci.* **2024**, *4*, 1407-1017.
33. Fröwis, M.; Gottschalk, T.; Haslhofer, B.; Rückert, C.; Pesch, P. Safeguarding the evidential value of forensic cryptocurrency investigations. *Forensic Sci. Int. Digit. Investig.* **2020**, *33*, 200902. [CrossRef]
34. Hsu, C.-L.; Chen, W.-X.; Le, T.-V. An Autonomous Log Storage Management Protocol with Blockchain Mechanism and Access Control for the Internet of Things. *Sensors* **2020**, *20*, 6471. [CrossRef] [PubMed]
35. Jin, P.; Kim, N.; Lee, S.; Jeong, D. Forensic investigation of the dark web on the Tor network: Pathway toward the surface web. *Int. J. Inf. Secur.* **2024**, *23*, 331–346. [CrossRef]
36. 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* **2021**, *9*, 103637–103650. [CrossRef]
37. Khanji, S.; Alfandi, O.; Ahmad, L.; Kakkengal, L.; Al-kfairy, M. A systematic analysis on the readiness of Blockchain integration in IoT forensics. *Forensic Sci. Int. Digit. Investig.* **2022**, *42*, 301472. [CrossRef]
38. Li, M.; Lal, C.; Conti, M.; Hu, D. LEChain: A blockchain-based lawful evidence management scheme for digital forensics. *Future Gener. Comput. Syst.* **2021**, *115*, 406–420. [CrossRef]
39. Mahrous, W.A.; Farouk, M.; Darwish, S.M. An Enhanced Blockchain-Based IoT Digital Forensics Architecture Using Fuzzy Hash. *IEEE Access* **2021**, *9*, 151327–151336. [CrossRef]
40. Muyambo, E.; Baror, S. Systematic Review to Propose a Blockchain-based Digital Forensic Ready Internet Voting System. *Int. Conf. Cyber Warf. Secur.* **2024**, *19*, 219–230. [CrossRef]
41. Patil, H.; Kohli, R.K.; Puri, S.; Puri, P. Potential applicability of blockchain technology in the maintenance of chain of custody in forensic casework. *Egypt. J. Forensic Sci.* **2024**, *14*, 12. [CrossRef]
42. Ryu, J.H.; Sharma, P.K.; Jo, J.H.; Park, J.H. A blockchain-based decentralized efficient investigation framework for IoT digital forensics. *J. Supercomput.* **2019**, *75*, 4372–4387. [CrossRef]
43. Sheelvant, Y. An Implementation of Blockchain Technology in Forensic Evidence Management system. *Int. Res. J. Mod. Eng. Technol. Sci. (IRJMETS)* **2023**, *5*, 194–198.

44. Zarpala, L.; Casino, F. A blockchain-based Forensic Model for Financial Crime Investigation: The Embezzlement Scenario. *Digit. Finance* **2021**, *3*, 301–332. [CrossRef]
45. Sakshi; Malik, A.; Sharma, A.K. A survey on blockchain based IoT forensic evidence preservation: Research trends and current challenges. *Multimed. Tools Appl.* **2023**, *83*, 42413–42458. [CrossRef]
46. Alqahtany, S.S.; Syed, T.A. ForensicTransMonitor: A Comprehensive Blockchain Approach to Reinvent Digital Forensics and Evidence Management. *Information* **2024**, *15*, 109. [CrossRef]
47. Onyeashie, B.I.; Leimich, P.; McKeown, S.; Russell, G. A Bibliometric Analysis and Systematic Review of a Blockchain-Based Chain of Custody for Digital Evidence. In *Big Data Technologies and Applications*; Tan, Z., Wu, Y., Xu, M., Eds.; Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Springer Nature: Cham, Switzerland, 2024; Volume 555, pp. 112–131, ISBN 978-3-031-52264-2.
48. Goyal, R. Blockchain Technology in Forensic Science. A Bibliometric Review. In Proceedings of the 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 17–18 December 2021.
49. Jacob, J.; Kumar, S. A Framework for Digital Forensics Using Blockchain to Secure Digital Data. In Proceedings of the 2022 IEEE World Conference on Applied Intelligence and Computing (AIC), Sonbhadra, India, 17–19 June 2022; pp. 899–904.
50. Akbarfam, A.J.; Heidaripour, M.; Maleki, H.; Dorai, G.; Agrawal, G. ForensiBlock: A Provenance-Driven Blockchain Framework for Data Forensics and Auditability. *arXiv* **2023**, arXiv:2308.03927.
51. Mas'ud, M.Z.; Hassan, A.; Shah, W.M.; Abdul-Latip, S.F.; Ahmad, R.; Ariffin, A.; Yunos, Z. A Review of Digital Forensics Framework for Blockchain in Cryptocurrency Technology. In Proceedings of the 2021 3rd International Cyber Resilience Conference (CRC), Langkawi Island, Malaysia, 29–31 January 2021; pp. 1–6.
52. Almutairi, W.; Moulahi, T. Joining Federated Learning to Blockchain for Digital Forensics in IoT. *Computers* **2023**, *12*, 157. [CrossRef]
53. Cong, L.; Grauer, K.; Rabetti, D.; Updegrave, H. Blockchain Forensics and Crypto-Related Cybercrimes. *SSRN J.* **2023**, 1–115. [CrossRef]
54. Alqahtany, S.S.; Syed, T.A. Integrating Blockchain and Deep Learning for Enhanced Mobile VPN Forensics: A Comprehensive Framework. *Appl. Sci.* **2024**, *14*, 4421. [CrossRef]
55. Srivasthav, D.P.; Maddali, L.P.; Vigneswaran, R. Study of Blockchain Forensics and Analytics tools. In Proceedings of the 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 27–30 September 2021; pp. 39–40.
56. 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.* **2023**, *48*, 10173–10188. [CrossRef]
57. Al-Khateeb, H.; Epiphaniou, G.; Daly, H. Blockchain for Modern Digital Forensics: The Chain-of-Custody as a Distributed Ledger. In *Blockchain and Clinical Trial*; Jahankhani, H., Kendzierskyj, S., Jamal, A., Epiphaniou, G., Al-Khateeb, H., Eds.; Advanced Sciences and Technologies for Security Applications; Springer International Publishing: Cham, Switzerland, 2019; pp. 149–168, ISBN 978-3-030-11288-2.
58. Ragu, G.; Ramamoorthy, S. A blockchain-based cloud forensics architecture for privacy leakage prediction with cloud. *Healthc. Anal.* **2023**, *4*, 100220. [CrossRef]
59. Brotsis, S.; Grammatikakis, K.P.; Kavallieros, D.; Mazilu, A.I.; Kolokotronis, N.; Limniotis, K.; Vassilakis, C. Blockchain meets Internet of Things (IoT) forensics: A unified framework for IoT ecosystems. *Internet Things* **2023**, *24*, 100968. [CrossRef]
60. Bonomi, S.; Casini, M.; Ciccotelli, C. B-CoC: A Blockchain-Based Chain of Custody for Evidences Management in Digital Forensics. *Open Access Ser. Inform. (OASIcs)* **2020**, *71*, 12:1–12:15. [CrossRef]
61. Tian, Z.; Li, M.; Qiu, M.; Sun, Y.; Su, S. Block-DEF: A secure digital evidence framework using blockchain. *Inf. Sci.* **2019**, *491*, 151–165. [CrossRef]
62. Lusetti, M.; Salsi, L.; Dallatana, A. A blockchain based solution for the custody of digital files in forensic medicine. *Forensic Sci. Int. Digit. Investig.* **2020**, *35*, 301017. [CrossRef]
63. Verma, A.; Bhattacharya, P.; Saraswat, D.; Tanwar, S. NyaYa: Blockchain-based electronic law record management scheme for judicial investigations. *J. Inf. Secur. Appl.* **2021**, *63*, 103025. [CrossRef]
64. Chen, S.; Zhao, C.; Huang, L.; Yuan, J.; Liu, M. Study and implementation on the application of blockchain in electronic evidence generation. *Forensic Sci. Int. Digit. Investig.* **2020**, *35*, 301001. [CrossRef]
65. Awuson-David, K.; Al-Hadhrami, T.; Alazab, M.; Shah, N.; Shalaginov, A. BCFL logging: An approach to acquire and preserve admissible digital forensics evidence in cloud ecosystem. *Future Gener. Comput. Syst.* **2021**, *122*, 1–13. [CrossRef]
66. Olukoya, O. Distilling blockchain requirements for digital investigation platforms. *J. Inf. Secur. Appl.* **2021**, *62*, 102969. [CrossRef]
67. 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.* **2020**, *33*, 300976. [CrossRef]
68. Naqvi, S. Challenges of Cryptocurrencies Forensics: A Case Study of Investigating, Evidencing and Prosecuting Organised Cybercriminals. In Proceedings of the 13th International Conference on Availability, Reliability and Security, Association for Computing Machinery, New York, NY, USA, 27–30 August 2018; pp. 1–5.
69. Rana, S.K.; Rana, A.K.; Rana, S.K.; Sharma, V.; Lilhore, U.K.; Khalaf, O.I.; Galletta, A. Decentralized Model to Protect Digital Evidence via Smart Contracts Using Layer 2 Polygon Blockchain. *IEEE Access* **2023**, *11*, 83289–83300. [CrossRef]

70. Agarwal, U.; Rishiwal, V.; Tanwar, S.; Yadav, M. Blockchain and crypto forensics: Investigating crypto frauds. *Int. J. Netw. Manag.* **2024**, *34*, e2255. [CrossRef]
71. Ellul, J.; Galea, J.; Ganado, M.; Mccarthy, S.; Pace, G.J. Regulating Blockchain, DLT and Smart Contracts: A technology regulator's perspective. *ERA Forum* **2020**, *21*, 209–220. [CrossRef]
72. Batista, D.; Mangeth, A.L.; Frajhof, I.; Alves, P.H.; Nasser, R.; Robichez, G.; Silva, G.M.; Miranda, F.P. de Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review. *J. Risk Financ. Manag.* **2023**, *16*, 360. [CrossRef]
73. Rožman, N.; Corn, M.; Škulj, G.; Berlec, T.; Diaci, J.; Podržaj, P. Exploring the Effects of Blockchain Scalability Limitations on Performance and User Behavior in Blockchain-Based Shared Manufacturing Systems: An Experimental Approach. *Appl. Sci.* **2023**, *13*, 4251. [CrossRef]
74. Zbrog, M. Digital Forensics in Blockchain: How Investigators Track Crypto. Forensics Colleges. Available online: https://www.forensicscolleges.com/blog/blockchain-forensics (accessed on 20 July 2024).
75. Atlam, H.F.; Azad, M.A.; Altamimi, M.; Fadhel, N. Role of Blockchain and AI in Security and Privacy of 6G. In *AI and Blockchain Technology in 6G Wireless Network*; Dutta Borah, M., Singh, P., Deka, G.C., Eds.; Springer Nature: Singapore, 2022; pp. 93–115, ISBN 978-981-19286-8-0.
76. Mani, N.; Parab, S.S.; Manaswini, S.; Philip, S.; Hari, P.B.; Singh, N. Forensic Block Chain and it's linkage with Artificial Intelligence: A new Approach. In Proceedings of the 2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, 19–21 January 2021; pp. 70–74.
77. BIG Investigations. The New Era Must-Have Blockchain Investigator Training. Blockchain Intelligence Group. 2024. Available online: https://blockchaingroup.io/the-new-era-must-have-blockchain-investigator-training/ (accessed on 20 July 2024).

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.