blockchains

MDPI

Review

The Application of Blockchain Technology in the Field of Digital Forensics: A Literature Review

Oshoke Samson Igonor *, Muhammad Bilal Amin * and Saurabh Garg

School of Information and Communication Technology (ICT), University of Tasmania, Hobart 7005, Australia; saurabh.garg@utas.edu.au

* Correspondence: osigonor@utas.edu.au (O.S.I.); bilal.amin@utas.edu.au (M.B.A.)

Abstract: Blockchain technology has risen in recent years from its initial application in finance to gain prominence across diverse sectors, including digital forensics. The possible application of blockchain technology to digital forensics is now becoming increasingly explored with many researchers now looking into the unique inherent properties that blockchain possesses to address the inherent challenges in this sector such as evidence tampering, the lack of transparency, and inadmissibility in court. Despite the increasing interest in integrating blockchain technology into the field of digital forensics and its domains, no systematic literature review currently exists to provide a holistic perspective on this integration. It is a challenge to find a comprehensive resource that examines how blockchain is being applied to enhance the digital forensics process. This paper provides a systematic literature review to explore the application of blockchain technology in digital forensics, focusing on its potential to address these challenges and enhance forensic methodologies. Through a rigorous review process, this paper examines selected studies to identify diverse frameworks, methodologies, and blockchain-driven enhancements applied to digital forensic investigations. The discussion highlights how blockchain properties such as immutability, transparency, and automation have been leveraged to improve evidence management and forensic workflows. Furthermore, this paper explores the common applications of blockchain-based forensic solutions across various domains and phases while addressing the associated limitations and challenges. Open issues and future research directions, including unexplored domains and operational gaps, are also discussed. This study provides valuable insights for researchers, investigators, and policymakers by offering a comprehensive overview of the state of the art in blockchain-based digital forensics, summarizing key contributions and limitations, and identifying pathways for advancing the field.

Keywords: blockchain; digital forensics; cybersecurity; review; systematic; smart contracts; chain of custody; blockchain application; blockchain-based; digital evidence

Academic Editors: Keke Gai and Liehuang Zhu

Received: 12 December 2024
Revised: 19 February 2025
Accepted: 20 February 2025
Published: 25 February 2025

Citation: Igonor, O.S.; Amin, M.B.; Garg, S. The Application of Blockchain Technology in the Field of Digital Forensics: A Literature Review. *Blockchains* **2025**, *3*, 5. https://doi.org/10.3390/blockchains3010005

1. Introduction

It is no news that our modern society is an ever-growing network of interconnections. This growth has embedded devices in most areas of our everyday lives, which has caused the consistent creation of data that act as digital footprints of almost all our daily interactions. For example, a smartphone may possess sensitive data (text messages, emails, financial transactions, etc.) that reveal background information about the owner and their social networks [1]. These data have become extremely valuable for diverse purposes, and, in the context of digital forensics, they represent an opportunity to combat cybercrime and tackle

other applicable cases as they are proven useful in civil litigations, criminal investigations, regulatory compliance, and other exploratory investigations [2]. The traditional method of digital forensics, while effective, faces significant challenges including maintaining the chain of custody, evidence integrity, and access-control issues [3].

As part of efforts to address these challenges, there has been increasing interest in blockchain technology over the past few years evidenced by the increasing amount of research in this area since 2016 (upon careful research using the Google Scholar tool, it was noted that the earliest research efforts of blockchain application in digital forensics was around 2015–2016). The adoption of blockchain solutions for digital forensics is hinged on the inherent properties that blockchain provides such as auditability due to append-only characteristics, immutability, transparency, automation capabilities through smart contracts, and file storage capabilities [4], as well as its security features, all leading to the establishment of verifiable chains of custody that can be legally admissible [2]. Initially developed as the underlying technology for cryptocurrencies like Bitcoin, Ethereum, etc. [5], the inherent properties blockchain possess has caused the expansion of its potential applications across various domains, including healthcare [6], supply chain and finance [7], etc., and, more recently, digital forensics. By recording evidence-related actions in an append-only ledger, blockchain solutions could potentially mitigate tampering risks and strengthen the evidence chain of custody all in an automated manner [8]. Blockchain technology through these capabilities has emerged as a promising solution to address many of the challenges in digital forensics. These features align well with the core principles of digital forensics, including evidence integrity and the chain of custody, making blockchain a transformative tool for enhancing forensic processes. However, despite its potential, the application of blockchain in digital forensics is still evolving, with significant gaps in certain domains and challenges that require deeper investigation.

Building on this interest in blockchain-based forensics, this paper examines how blockchain is employed to address key digital forensic requirements through a systematic literature review (SLR). By reviewing and analyzing existing blockchain-based approaches or solutions, across the various domains (e.g., cloud, network, multimedia, etc.), we aim to uncover limitations in current practices and highlight open issues where blockchain could further bolster digital forensic processes. This study aims to bridge these gaps by systematically exploring how blockchain has been integrated into digital forensics, identifying the challenges and opportunities, providing a visual schema of the current state, and proposing directions for future research to realize its full potential in advancing this critical field.

The rest of this paper is organized as follows. Section 1 presents research goals, contributions, and an overview of the related works; Section 2 is a brief background study of digital forensics and blockchain technology; Section 3 describes the systematic literature review research methodology used; Section 4 presents a summary of the SLR analysis of the studies; Section 5 describes findings from this systemic review and presents a visual schema to illustrate the findings; Section 6 presents how the review findings answer the research questions; Section 7 presents the open issues and future research directions; Section 8 and Section 9 are the limitations of the study and the conclusion.

1.1. Research Goals

The goal of this study is to analyze existing research on the application of blockchain technology to the digital forensics process and to summarize the key findings and contributions made thus far. This study specifically seeks to explore the following aims:

1. Identify key blockchain-based forensic approaches by examining how blockchain's core properties are leveraged to secure and streamline digital forensic investigations across various sub-domains.
2. Highlight limitations or open issues with blockchain-based forensic approaches.
3. Propose a structured representation of findings through a visual schema that can serve as a conceptual framework that illustrates blockchain applications in digital forensics. This will allow researchers to quickly identify and have a holistic understanding of the entire blockchain-in-digital forensics landscape before diving into specifics.
4. Answer the following research questions:
    1. RQ1: How is blockchain technology currently integrated into digital forensics to address its challenges, and what key advantages does its application offer?
    2. RQ2: What key challenges or limitations do current blockchain-based forensic solutions face, and how do they vary across different digital forensics domains?

By addressing these core objectives, this study aims to provide a comprehensive understanding of how blockchain technology could strengthen digital forensic investigations while providing a comprehensive resource that could act as a starting point for deeper investigation and innovation in the area.

1.2. Research Contributions

Our SLR stands out for its comprehensive focus on diverse digital forensic domains beyond just IoT, physical evidence, or a few domains. By analyzing the literature up to 2025, this study systematically compiles and evaluates how blockchain's core properties (e.g., immutability, transparency, and decentralization) are being leveraged to improve evidence collection, preservation, and chain of custody management in areas like IoT forensics, cloud forensics, and multimedia forensics and other domains.

To build from prior efforts, our review does the following:

- Presents a visual representation of the state-of-the-art in blockchain application in the digital forensics field: We offer a visual schema that can serve as a structured conceptual framework that consolidates current findings on blockchain-based digital forensic solutions and highlights both widely explored and relatively understudied avenues.
- Examines practical blockchain approaches of blockchain-based solutions: We investigate blockchain-based solutions (frameworks, methodologies, and tools) proposed or implemented to tackle forensic challenges with a consideration of blockchain types, platforms and blockchain properties explored by the solutions, synthesizing key insights on how these solutions enhance, or could enhance, evidence integrity, privacy, and process automation.
- Identifies open issues and future directions: Our analysis highlights open challenges such as legal admissibility, scalability, and blockchain limitations such as computational costs, thus laying the groundwork for future research and the development of more robust, scalable blockchain-forensics systems.

By providing a thorough and systematic review of the latest blockchain-driven solutions and pinpointing potential for improvement, our study aims to serve as a go-to resource for researchers, digital forensic practitioners, and stakeholders seeking to implement or improve blockchain technology for digital forensic requirements.

1.3. Related Works

Upon the completion of a thorough search of six databases, which include MDPI, SpringerLink, ACM, Google Scholar, ResearchGate, and the Scopus Search Engine, we could not find any studies relating specifically to a systematic literature review (SLR) of the application of blockchain technology to the field of digital forensics in an encompassing

manner as this research has strived to provide with thoroughness and precision. However, there are other studies that have conducted SLRs, surveys, or reviews in related domains in this field.

Akinbi et al. [9], in an SLR, provided a comprehensive report of the application of blockchain in forensic investigation process models of Internet of Things (IoT). They specifically reviewed how blockchain is used to improve the IoT forensic investigation process and discussed the efficacy of the models; they provided insights into challenges, issues, and future research directions of blockchain technology in this domain. Their findings revealed that most of the blockchain-based solutions in IoT forensics are targeted at improving the chain of custody, evidence integrity, provenance, privacy, and identity anonymity. However, this literature only focused on the IoT forensics domain, thus making it not as encompassing. Similarly, in another SLR, Khanji et al. [10] investigated the readiness of blockchain technology into IoT forensics by analyzing existing or proposed frameworks and models to identify blockchain-integrated readiness factors in IoT forensics, which they highlighted to be data Integrity, distributed storage, legality and regulations, management, transparency, authenticity, and security. They concluded that the legal and regulatory aspects of blockchain's application in IoT forensics are still being overlooked, and more research is needed to address the legal and ethical processing of the digital evidence and chain of custody in this domain. This lack of other digital forensics domains in these works prompted our dive into exploring other domains where blockchain has been applied as well as the nature of their application. On the other hand, Batista et al. [11], in their SLR, explored literature that used blockchain to tackle the chain of custody of physical evidence instead of digital evidence, thus rendering it out of our intended scope.

Another related work is the study by Dasaklis et al. [1] where they classified available blockchain-based digital forensic tools and discussed their main features as well as the benefits and drawbacks of the application of blockchain in the field of digital forensics; they take into consideration more domains and extensively discussed the limitation of blockchain as well as the challenges that existing blockchain solutions face. They recommended that future work focuses on the development of a blockchain-based forensic framework that facilitates the gathering of heterogeneous digital evidence and forensic procedures in a standardized approach. The most related study is that by Atlam et al. [12]; they conducted a highly detailed systematic literature review of techniques, applications, challenges, and future directions for blockchain forensics. Their study provides a detailed examination of 46 selected articles, offering valuable insights into how blockchain's decentralization and immutability introduce both advantages and complications for a digital investigation of blockchain-related events. They highlighted that while decentralization enhances security, it makes linking blockchain addresses to real-world entities more difficult; similarly, immutability prevents evidence manipulation but can complicate the rectification of fraudulent or erroneous data. Their SLR also explores various digital forensic frameworks and techniques tailored to blockchain environments and, by extension, highlights the application of blockchain to the field of digital forensics through its summary of recent studies related to blockchain forensics and blockchain-based forensics. They discuss legal and regulatory hurdles that investigators often encounter during blockchain forensics and highlight open issues such as scalability and privacy, pinpointing areas for further research.

Atlam et al.'s SLR [12] provides a strong foundation for understanding current solutions and remaining gaps in blockchain forensics, and our SLR builds on their work by taking into consideration more factors that affect the current state of the art. We find these factors through a background review of both fields such as the blockchain platforms being utilized over time, the blockchain types, and blockchain platforms being mostly explored as well as domains of digital forensics where blockchain is mostly applied. Also, we pro-

pose a visual schema that illustrates a comprehensive view of the current applications of blockchain technology in the field of digital forensics. Table 1 highlights the contribution of this SLR compared to the related works.

Table 1. Related works: A comparative summary.

Related Work	Multiple Digital Forensics Domains	Challenges or Limitations of Blockchain-Based Solutions	Blockchain Type	Blockchain Platform	Blockchain Properties of Interest	Visual Schema of Blockchain Application to Digital Forensics
Akinbi et al. [9]	Only IoT	×	✓	✓	✓	×
Khanji et al. [10]	Only IoT	×	×	✓	✓	×
Batista et al. [11]	×	×	✓	✓	×	×
Dasaklis et al. [1]	✓	✓	×	×	×	×
Atlam et al. [12]	✓	✓	×	×	✓	×
Our SLR	✓	✓	✓	✓	✓	✓

2. Brief Background Study of Digital Forensics and Blockchain Technology

2.1. Digital Forensics

In simple terms, digital forensics is a branch of forensic science that is applied to the digital domain where digital investigation occurs [13]. Digital forensics is the application of scientific principles to law and so it follows some specific methodologies, processes, and techniques to ensure an admissibility of the investigative process in a court of law; some of these include evidence exchange, forensic soundness, authenticity and integrity, and the chain of custody [14]. It is a critical discipline within forensic science that deals with the recovery, analysis, preservation of electronic data or digital evidence, and reporting of the findings, primarily for use in legal proceedings [4]. It encompasses various digital environments, including computers, mobile devices, IoT, networks, and cloud-based systems. The field has evolved significantly over recent years, driven by advancements in technology and the increasing complexity of digital crimes [15].

2.2. The Digital Forensics Process

From the initial literature review, we found that in the digital forensics process, many researchers like [16–23] represent their DF process model in different ways depending either on technological advancements in the period when their research was conducted or the use cases, frameworks, or models that were being proposed [24]. Our careful review of these works shows that the process models described by these authors generally describe the same concepts. We summarize them into five phases using the ISO/IEC 27037 forensic guidelines and the NIST SP 800-101 forensic process as general standards [25].

1. Identification: The Identification phase is the first phase in the digital forensics process, and it focuses on first responders planning, recognizing and identifying relevant digital (mostly physical) data sources that may contain relevant digital evidence [26,27].
2. Collection: The collection phase, otherwise known as acquisition phase, is the stage where the identified media or devices are collected by practitioners for investigative purposes, and evidence is extracted from the devices. Data are meticulously copied to make forensics copies for investigative purposes, and the authentication of the entire process occurs mainly through cryptographic hashing and time-stamping; finally, documenting the extraction process into a chain of custody occurs to provide integrity from the collection phase [28].

3. Preservation: The preservation phase involves maintaining the custody of digital evidence on devices or removable media in a way that prevents any modification or alterations to its content. This phase is important for ensuring that prospective digital evidence remains original and usable in an investigation and retains reliability for legal admissibility [25]. Upholding the preservation methods through the investigation process is crucial in deciding a case.
4. Examination: In this phase, practitioners carefully analyze and correlate the extracted digital evidence to find patterns, prove or disprove theories, and uncover relationships or connections that are pertinent to the investigated event [23]. This typically involves interpreting the data, comparing and correlating with other discovered evidence, and applying forensic techniques to determine its relevance.
5. Reporting: The DF process culminates in this reporting stage where the investigator compiles and presents the final documentation and summary reports that contain the findings of the investigation, including the investigative steps taken throughout the process [25] to the relevant audience, i.e., a court of law, employers, or cybersecurity teams, etc. This final report relies on a thorough DF investigative process that guarantees a sufficient level of certainty in its objective conclusions.

2.3. Principles of Digital Forensics

Digital forensics' primary goal is concerned with digital evidence, which has a complex nature that often involves issues relating to volatility and anonymity. This has made it very susceptible to integrity losses and, if not properly handled, can lead to the inadmissibility of the evidence in court or sketchy results [29]. Because of this, digital forensics runs on two key principles to meet legal and ethical standards, as well as to mitigate against the current challenges that come with it. These principles are Evidence Integrity and Chain of Custody as evidenced in [13].

1. Integrity of Digital Evidence: Digital evidence has a complex nature that often involves issues relating to volatility and anonymity. This has made it very susceptible to integrity losses and, if not properly handled, can lead to the inadmissibility of the evidence in court or sketchy results [29]. The integrity of digital evidence is the most important requirement of the entire forensics process as it is critical to trustworthiness and admissibility of the evidence in a court of law [30]. If the evidence or data have been tampered with or changed in any way during the process, they may be challenged by opposition and rejected by the court, which can sabotage the entire investigation. Typically, examination and analysis is carried out on a replica of the digital media, and the integrity of this replica should also be maintained during the different phases of the investigation process [29]. To prove the integrity of digital evidence, a form of cryptographic hashing [31] is employed on some data at the acquisition stage to generate a unique "digital fingerprint" or signature of that data; this hash can then be compared to the hash of the evidence presented later in the digital forensics process [13]. Requirements like authenticity, security to ensure non-alteration and privacy during preservation and the transmission of digital evidence, and ethical handling are of utmost importance; thus, the forensic examiner must make use of proper tools and techniques to ensure that the data are preserved in the exact form as when they were acquired.
2. Chain of Custody (CoC): This involves the sequential documentation and accountability for the custody, management, control, transfer, analysis, and final disposition of assets or evidence from collection to presentation in a court of law [32]. CoC has an important impact since it establishes integrity and safeguards the admissibility of digital evidence in court proceedings due to the volatile and complex nature of digital

evidence. In digital forensics, the chain of custody acts like a secure auditable trail [11] ensuring that digital assets—whether physical devices containing evidence or the digital evidence itself—remain accounted for and untampered during the investigation process. It is a meticulous record-keeping system that tracks an asset's journey from its origin to its destination. This documentation includes essential details such as date, time, location, individuals involved, and any custody transitions. Investigators typically must adhere to strict protocols to safeguard against unauthorized meddling and maintain the asset's integrity. In simple terms, it is like a protective shield for evidence, ensuring its reliability throughout its entire lifecycle. Requirements of this principle include access control, data provenance, privacy/confidentiality, auditability, process automation, security, transparency, integrity, immutability, storage, and record-keeping [11].

2.4. Requirements and Challenges of Digital Forensics

Upon a survey of the existing literature, it is difficult to provide an exhaustive list of challenges that plague digital forensics as a field. However, the authors Karie and Venter reviewed, highlighted, and classified the large number of challenges faced in the domain in the previous 10 years. They classified them into four categories, each with its own diverse set of sub-categories as (i) Technical Challenges, (ii) Legal/Law Enforcement Challenges, (iii) Personnel-Related Challenges, and (iv) Operational Challenges [33].

Moving on to the coming years, researchers have revised the identification of challenges as they have emerged over time and started classifying them based on the type or domain of digital forensics investigation. For example, challenges are identified by four domains: IoT forensics challenges, cloud forensics, network forensics, and social media forensics challenges [34]. Casino et al., in their review of reviews, succinctly identified numerous challenges while classifying them into eight domains: (i) IoT, (ii) Cloud, (iii) Multimedia, (iv) Blockchain, (v) Mobile, (vi) Networks, (vii) Filesystems, Memory, and Data Storage Forensics, and (viii) Miscellaneous [35]. Although many challenges have been identified and established by the papers referenced above, which span reviews of the last two decades, most of them, when carefully considered, will fall under one of the four categories as classified by the study of Karie and Venter in 2015, with the significant differences being the challenges that have emerged with new technologies over the years during the period.

For the purpose of this SLR, we present a unique classification where we map the discovered challenges into requirements as we find that most of them are repeated across several studies. Using Karie and Venter's [33] categories as reference, we classified each challenge according to whether it arises from (a) technical constraints, (b) legal/legislative contexts, or (c) operational factors. Although we could not find a single standard that explicitly labels these exact three classes of requirements, multiple international guidelines collectively cover these core dimensions of digital forensics. In particular, the ISO/IEC corpus (e.g., 27037, 27041, 27042, 27043, and 27050), the European Network of Forensic Science Institutes (ENFSI) Best Practice Manual, and the Council of Europe's Electronic Evidence Guide (EEG) all recognize that digital forensic investigations involve technical responsibilities, compliance with legal and regulatory requirements, and organizational operations or personnel-related elements [36]. We then analyzed the nature of each distinct challenge; for example, whether the issue falls primarily within a technical context (e.g., anti-forensics techniques), legal or policy contexts (e.g., jurisdiction), or personnel and procedural aspects (e.g., training). Finally, we aligned each challenge to its corresponding requirement.

Table 2 shows our classification scheme of digital forensics challenges into requirements, which include the most recent challenges discovered. It is possible that in the real

world, these challenges and requirements rarely occur in isolation. Also, not all of these challenges may be pertinent to the application of blockchain to digital forensics; finding out the challenges that blockchain has been identified to address will help researchers identify the areas that have been of focus and underexplored areas, prompting research into these overlooked areas to uncover other opportunities.

Table 2. Requirements and challenges in digital forensics.

Requirements of Digital Forensics	Challenges in Digital Forensics	Description of Challenge
Technical Requirements	Vast Volumes of Data (Big Data)	Handling and processing large datasets efficiently, which complicates analysis. Issues related to decentralized data, data accessibility and management during investigation, data duplication, heterogeneity of data and data sources, etc.
	New and Emerging Technologies and Devices	Challenges posed by new digital devices and technologies such as Cloud, IoT, AI, Smart Contract Vulnerabilities, etc. This includes difficulties in extracting data from small and embedded devices as well as data dispersed across multiple platforms, cloud environment, and diverse formats.
	Security of Digital Evidence	Issues relating to preservation of integrity evidence tampering, confidentiality (data leakage and access control), and availability of digital evidence.
	Instability of Digital Evidence (Time Sensitivity)	Issues related to the transient and volatile nature of digital data, making timely collection crucial. Concerns over the durability and degradation of storage media.
	Anti-Forensics Techniques	Methods that make it difficult to conduct forensic analysis and increase sophistication in cybercriminal methods cause the need for high computational resources and thus lead to more cost for tools, time needed per investigation, etc.
	Network Forensic Analysis Tools	Improving the functionalities of tools for traffic sniffing, analyzing encrypted network data, intrusion detection, protocol analysis, and Security Event Management (SEM).
	Forensics Process Automation	High reliance on manual processes in forensic investigations. This means a need for automating forensic tasks to improve efficiency.
Legal Systems Requirements	Jurisdiction	Legal complications arising from cross-border data storage, exchange, and/or access, as well as inconsistent legal protocols across jurisdictions.
	Admissibility of Digital Forensic Methods and Tools	Ensuring forensic methods are legally accepted.
	Privacy and Ethical Concerns	Balancing investigative needs with privacy rights.
	Chain of Custody	Ensuring integrity, provenance, reliability, and proper documentation of evidence from collection to presentation. Access control and evidence-tampering concerns.
	Omission of Terms and Conditions in Service Level Agreements (SLAs)	Lack of forensic provisions in SLAs with tech service providers.

Table 2. *Cont.*

Requirements of Digital Forensics	Challenges in Digital Forensics	Description of Challenge
Operational Requirements	Inadequate Knowledge Sharing and Communication among experts	Inefficiencies in sharing and communication of forensic expertise and findings.
	Forensic Investigator Licensing Requirements	Need for formal certification and regulation of forensic investigators.
	Challenge of Digital Forensic Preparedness in Organizations	Ensuring organizations are prepared for forensic investigations through resource allocation, policies, processes, guidelines, and procedures.
	Training Gaps	Shortage of trained and certified digital forensic experts. Continuous need for updated training to keep pace with technological advancements.
	Incidence Detection, Response, and Prevention	Challenges in identifying and mitigating digital incidents in organizations.

2.5. Domains of Digital Forensics

Through our brief background study, we find that digital forensics has evolved from the traditional DF on computers and servers alone to keep pace with new and emerging technology and digital media. This has seen the need for the application of DF techniques in different domains that include mobile devices, blockchain, multimedia, filesystems, databases, networks, cloud-based platforms, and the Internet of Things (IoT), and a corresponding rise in cybersecurity incidents because of these digital technologies has been observed. These domains are typically named after the data source of digital evidence as the proliferation of these devices and technologies in everyday lives makes them a necessary aspect that requires unique skill sets and idiosyncrasies for investigation. Well-established domains in digital forensics have been documented [35,37–39], which include Storage Forensics and Its Relevant Sub-Domains for the different kinds of media such as Memory Forensics [40–43], Filesystems Forensics [44], Database Forensics [35,45,46], and Disk Forensics [47]. Other domains include Network Forensics [48–50]; Mobile Forensics [37,51,52]; Multimedia Forensics [53–55]; IoT Forensics [56,57]; Cloud Forensics [58,59]; Malware Forensics [60]; Blockchain Forensics [12].

2.6. Blockchain

Blockchain can be defined as "a conditionally growing decentralized and distributed digital ledger comprising cryptographically signed records of assets that are grouped in a chain of blocks upon validation" [61]. It is a shared distributed ledger that makes it easier to track assets in a network and record transactions where an asset can be tangible for instance a car or intangible entity like intellectual property [62]. These assets are stored in "blocks" on a decentralized "chain", which are cryptographically encrypted and connected to one another. This decentralized nature of blockchain allows for the distribution of computing power and resources across all devices on the network, which enhances reliability. Its Peer-to-Peer architecture makes it a highly redundant and efficient system that ensures consistency and dependable performance. This exists through replication across multiple nodes (writers), ensuring that data are duplicated and stored across the entire network. This built-in redundancy enhances robustness by safeguarding against data loss and system failures [63]. Furthermore, its decentralized nature eliminates the need for central authority, which further enhances reliability against disruptions and increases

trust [64]. This decentralized nature also thrives on the peer-to-peer architecture, which facilitates direct interactions between the node [65].

Due to this "block" design, a strong tie is established between the blocks that ensure their order through a strong time-stamping mechanism. As a result, it is impossible to change a block without it altering all its successive blocks [66]. This premise of blockchain technology causes it to have inherent properties that make it an ideal working scheme for digital forensics, which our study identifies through the SLR. However, blockchain is not without its issues such as the computing needs for mining, which is the process in which nodes authenticate new blocks and append them to the chain via consensus protocols [67], as well as others, which this study investigates.

2.7. Blockchain Types

According to [61], there are three types of blockchain based on the governance model of consensus mechanisms. These are public blockchain (permissionless), private blockchain (permissioned), and consortium blockchain. The distinction between these blockchain types is based on three tenets, which are (1) the nodes that have reachability to the ledger, (2) the permissions granted to the participating nodes and, most significantly, (3) the consensus mechanism accessible to the participating nodes, essentially meaning how the blockchain network is governed or administered.

1. Public Blockchain: A public blockchain, also referred to as a permissionless blockchain, enables unrestricted participation, allowing anyone to join, create, and update the blockchain through transactions. This open access makes all transactions and data stored on the blockchain visible and accessible to everyone, which can raise privacy concerns in situations where data confidentiality is crucial [68].
2. Private Blockchain: A private blockchain, also called a permissioned blockchain, operates with restricted access, allowing only authorized and trusted entities to participate. Unlike public blockchains, private blockchains limit the visibility of the chain data to these trusted participants, which can be advantageous for use cases that require more control and confidentiality [68].
3. Consortium Blockchain: A hybrid model that combines elements of both public and private blockchains. This is a permissioned blockchain where participation is restricted to a group of pre-selected members, typically organizations or institutions. Each node represents a participant within the consortium, and the number of nodes is based on the size of the group that governs. Consortium blockchains provide the member institutions with access to the network via gateways, offering features such as member authentication, data access control, transaction monitoring, and member management [69].

2.8. The Inherent Properties of Blockchain Technology

Understanding the inherent properties of blockchain technology is crucial to the reason why many researchers have explored its use in diverse areas. We conduct a brief literature review to identify these properties.

1. Integrity and Traceability Properties: Blockchain technology is established to possess characteristics that ensure trust and accountability of preserved data. These properties include auditability [1], transparency [70], immutability, provenance [4], and a host of other names that describe similar properties in other literature such as coherence, persistency [71], trackability [72], or tamper-proof [2], etc. It is important to note that while blockchain is designed to be highly resistant to tampering, calling it completely immutable is an oversimplification; thus, it is more accurate to say that any changes or attacks are typically highly resource-intensive and highly detectable [73]. However,

when all of these properties are considered together, it can guarantee near-complete integrity. Auditability/provenance allows for the verification of transactions, ensuring that all actions can be traced back to their origin, thus verifying authenticity and ownership; immutability ensures that once data are recorded, they cannot be changed discretely, while the transparency property allows for all transactions or changes to be visible to authorized parties, promoting trust, non-repudiation, and accountability.

2. Enhanced Security and Privacy: Blockchain technology offers a high level of security and encryption, which creates a layer of trust without needing a centralized intermediary [74]. This is because advanced cryptographic techniques protect the data and transactions on the blockchain. Blockchain employs key cryptographic methods such as public key cryptography, zero-knowledge proofs, and hash functions to ensure data integrity, authenticity, and privacy [75]. It is also established that blockchain enhances anonymity by allowing users to perform transactions without revealing their real-world identities [76]. Public key cryptography provides pseudonymous addresses, zero-knowledge proofs, and a secure verification of smart contracts, which allow for the verification of transactions without disclosing sensitive information [74]. These generated addresses ensure high-level anonymity for both the transactions and actors on blockchain [77]. Furthermore, hash functions ensure the "chain of block" where each block contains a hash value and which connects it to the next block, causing an increased protection of sensitive data as any change in the data will alter the hash, which would affect the overall change [78]; this ability ensures the integrity of data, which is a very important characteristic of blockchain as explained.
3. Automation Capabilities: The automation capabilities of blockchain have been highlighted by multiple authors, and these are usually exemplified by (a) smart contracts [79], for instance, the practicability of blockchain for automation was considered in e-government because of its decentralized nature [80]. A smart contract is a digital representation of a relationship or a contractual agreement between different parties that is enforceable by code, without any underlying obligations under the contract [81]. These self-executing contracts with the predefined rules directly written into code enable the automatic execution of agreements when the corresponding pre-defined conditions are met. (b) Consensus mechanisms such as proof-of-work (PoW) or proof-of-stake (PoS), etc., which automate the process of validating and appending transactions to the blockchain [82]. These properties of blockchain speed up transactions and increase efficiency while ensuring that the terms of the agreements are enforced automatically, accurately, and transparently without the need for intermediaries.
4. Data Storage and Management Capabilities: Blockchain has been established to possess decentralized file storage and transfer capabilities and database functionalities [83], which allow it to store and manage large volumes of data securely and efficiently. Zhu et al. (2023) established the integration of blockchain into traditional databases through their survey and examined how blockchain contributes to efficient data management and storage [84]. These attributes of blockchain have also been explored to enhance the security and efficiency of file sharing based on the Inter-Planetary File System (IPFS) [85], highlighting the unique characteristics that blockchain brings to data management. Furthermore, the enhanced security and data provenance properties of blockchain make it an ideal solution to ensure trust in databases [86]. Furthermore, these capabilities allow blockchain to serve as a robust database solution that can handle diverse data types while ensuring data integrity, accessibility, and decentralized storage for chain of custody especially, which further enhances the reliability and security of the system.

All of these properties work together to make blockchain a highly resilient and efficient technology, which ensures consistency and dependable performance. In blockchain systems, redundancy is inherently provided through replication across multiple nodes, ensuring that data is duplicated and stored across the entire network. This built-in redundancy enhances robustness by safeguarding against data loss and system failures [63]. Furthermore, its decentralized and peer-to-peer nature eliminates the need for central authority, which further enhances reliability against disruptions [64] and facilitates direct interactions between the nodes in the network [65].

3. Systematic Literature Review

To meet the objectives of reviewing the most pertinent studies concerning the application of blockchain technology to digital forensics and addressing the research questions posed, a research protocol was developed following the guidelines for conducting a systematic literature review (SLR) as outlined by [87] and finetuned with the Preferred Reporting Items for Systematic Review and Meta-Analyses (PRISMA) 2020 protocol [88]. This research protocol is outlined in this section and includes the methodology used to identify, screen, and select available evidence related to the research questions. An elaboration of the stages of the SLR is shown in the Supplementary Materials.

3.1. Objectives and Scope

The primary objective of this systematic literature review (SLR) is to analyze existing studies on the application of blockchain technology to the domain of digital forensics investigation. We summarize research efforts and findings, identify the specific properties of blockchain that are applied, and determine the digital forensics challenges that these applications address. The scope of this survey encompasses research in the objective area conducted from 2018 to 2025, covering various aspects of digital forensics regardless of the specific domain within digital forensics (as identified in the background section) that the literature addresses. The rationale for choosing research works from 2018 is due to the fact that the blockchain technology integration into the field of digital forensics is relatively new as most of the talk of blockchain before this period was focused on cryptocurrency, finance, and other digital investigations of other finance-related issues as we have confirmed using the in-built Google Scholar "Search by Custom Range" advanced feature.

3.2. SLR Research Protocol

To ensure a comprehensive and transparent review of the selected literature, the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) protocol was utilized throughout the screening and data extraction process. This approach was designed to enhance the transparency, accuracy, and credibility of the systematic literature review (SLR). The PRISMA protocol involves several key steps as outlined by the PRISMA 2020 Statement paper [88]: the identification phase where we used keywords to create initial search strategy to identify the possible literature, the screening phase where a literature selection criteria are used to filter out irrelevant or duplicated studies, the eligibility phase where we selected results using title and abstract screening to confirm quality and relevance of results, and the inclusion phase where the studies are aggregated into a primary study. This approach is elaborated in this section. Figure 1 displays the PRISMA flow diagram.

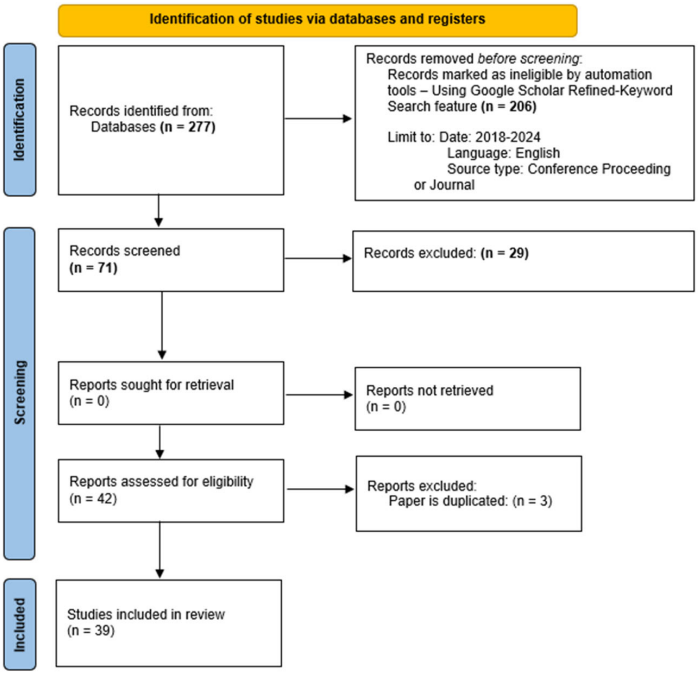

Figure 1. Flowchart for literature selection using Preferred Reporting Items for Systematic Review and Meta-Analyses (PRISMA).

3.2.1. Search Strategy

The literature search was conducted across multiple reputable academic databases and search engines, including MDPI, SpringerLink, ACM, Google Scholar, ResearchGate, and the Scopus Search Engine. A comprehensive search strategy was employed using keywords. These keywords were used in multiple iterations using the following linking words "and", "in", "for", "with", and "to" to ensure a thorough and exhaustive search of the relevant literature. Also, the Identified Keywords were combined with the identified blockchain properties and challenges in digital forensics in the search engines and combined with the in-built "sort by relevance" features to produce more relevant results. A breakdown is provided in Table 3.

Table 3. Database search strategy.

Database Search Strategy	
Keywords	"Blockchain Digital Forensics", "Blockchain", "Digital Forensics", "Computer Forensics", "Blockchain-based digital forensics", "Blockchain-based forensics", "Blockchain Application Digital Forensics", "Legal investigation", "Judicial investigation", "digital investigation", "digital enquiry", "Litigation"
Linking words	"and", "in", "for", "with", "to"
Identified blockchain properties used as keywords	"immutability", "integrity", "traceability", "resilience", "security", "privacy", "automation", "smart contracts", "decentralized", "peer-to-peer", "chain", "auditability", "trust", "decentralized storage"
Scope	2003–2025 (Until January)
Databases and Search Engines	MDPI, SpringerLink, ACM digital library, ResearchGate, Scopus Search Engine (Science Direct), Google Scholar
Last date searched	9 January 2025

3.2.2. Literature Selection Criteria

The inclusion and exclusion criteria for this study were defined to ensure that selected papers are directly relevant to the application of blockchain technology in digital forensics and its investigation processes. The selection process employs the logical operator AND for inclusion criteria, as all inclusion requirements must be met for a paper to be considered relevant for this study, while it employs the logical operator OR for exclusion criteria as any paper that meets one of these is considered irrelevant for this study. Detailed criteria are provided in Table 4. The abstracts, introduction, and conclusion of these literature works were carefully examined, while the body and content were skimmed through to establish correspondence with the pre-defined inclusion and exclusion criteria. We also put into minor considerations renowned papers identified with a citation count to further capture the research works that other authors use as reference points.

Table 4. Inclusion and exclusion criteria for systematic literature review.

Inclusion Criteria	Exclusion Criteria
The selected paper must be relevant to blockchain technology application to digital forensics and the digital forensics investigation process regardless of the specific digital forensics' domain.	The paper focuses on the application of digital forensic processes to investigate blockchain technology.
The paper must provide a practical or theoretical application of blockchain to the digital forensics investigation process.	The paper falls outside the broader field of blockchain technology application to digital forensics and digital forensics investigation process.
The paper must not be a review or survey paper or other studies.	The paper does not discuss concepts, models, or frameworks integrating blockchain technology to digital forensics.
The paper must be peer-reviewed.	Papers that are not peer-reviewed.
The paper must be written in English.	Papers not written in English and duplicates of published papers.
The paper must be published in a conference proceeding or journal.	Grey literature (white papers, editorial comments, book reviews, government documents, and blog posts).
The paper must be within 2018–2025.	Papers that are outside the years 2018–2025.

3.2.3. Selection of Results

The identified databases were searched using a combination of the relevant string searches and keywords, and the initial results yielded a total of 277 publications across all selected online databases. To refine the results and focus on relevant studies, the literature selection criteria were applied, which resulted in the removal of 206 studies, narrowing down the results to 71 studies.

Next, we conducted a thorough screening of titles and abstracts to further eliminate irrelevant studies based on research questions by determining if they addressed the questions posed in this study. This resulted in the exclusion of 29 publications. The rest of the 42 full studies were then thoroughly reviewed. Finally, we reapplied the inclusion and exclusion criteria and did a quality assessment check to reduce the chances of highly similar papers to a minimal level, which resulted in the removal of three papers. At the end of this selection process, 39 primary studies remained. Figure 1 shows the PRISMA flow of the selection process. The list of selected studies derived using the PRISMA protocol is included, chronologically, in the summary of the primary studies section and references section.

3.2.4. Data Extraction and Analysis

To gain a comprehensive understanding of the selected literature, each paper was read in full by three authors. This hands-on approach was utilized for data extraction and analysis, employing both content and thematic analysis. This method allows for a more

nuanced and detailed understanding of the literature as it involves our direct engagement with the content of each study. The manual extraction and analysis process included documenting basic information (such as authors, publication year, and source), capturing key elements (such as research objectives, methodologies, findings, and conclusions), and organizing notes in a structured format. The thematic analysis involved identifying patterns and themes within the literature through critical thinking processes, coding the data accordingly, and periodically reviewing and refining these findings to ensure accuracy and relevance.

3.3. Results of Systematic Literature Review

The findings of this SLR are presented and discussed in three sections. Firstly, a summary of the selected studies is presented through Table 5 in Section 3, which shows the full list of analyzed studies and findings. Secondly in Section 5, we organized the findings into a visual schema, providing a visual illustration of the broader landscape of blockchain applications in digital forensics and offering a clear overview of how different studies have contributed to this domain. Finally, the research questions are discussed in Section 6. We have used Python (version 3.10) programming language for data analysis in the Google Collab environment to present statistical figures in this review.

Table 5. Results of primary study.

Primary Study	Summary of Contribution	Blockchain-Driven Enhancements to Forensic Principles	Drawbacks or Challenges of Approach	Primary Digital Forensics Domain in Focus	Primary Phase(s) Addressed
PS1—Khan et al. [89]	This study introduces a framework leveraging Hyperledger Sawtooth to enhance real-time video surveillance in multimedia forensics. By integrating blockchain with IoT, it ensures secure chain-of-custody management and addresses issues like frame filtering and object-of-interest identification. Smart contracts streamline validation processes, and immutable distributed storage (IPFS) improves evidence handling. Performance evaluations indicate notable resource efficiency and reduced consumption.	Evidence Integrity: Data Preservation and Transmission Integrity, Access Control; Chain of Custody: Provenance, Immutability	This solution still faces challenges, which include significant computational demands and bandwidth requirements for handling real-time multimedia data, along with the complexity of implementing automated processes for filtering and identification.	Multimedia Forensics	Collection, Preservation
PS2—Mahrous et al. [90]	This paper proposes a framework for IoT digital forensics that incorporates fuzzy hashing into a blockchain-based architecture. The fuzzy hash technique improves evidence detection by enabling the identification of variations in digital evidence while enhancing data integrity through Merkle trees and a simplified proof-of-work consensus mechanism. The framework also handles heterogeneity in IoT devices and explores forensic analysis on resource-constrained systems.	Evidence Integrity: Data Integrity, Evidence Collection; Chain of Custody: Traceability, Provenance	Issues that this framework still grapples with include scalability issues, which arise due to the increased computational and storage demands of processing large volumes of IoT data on the blockchain, particularly in real-time scenarios. Additionally, integrating fuzzy hashing adds computational overhead.	IoT Forensics	Identification, Collection

Table 5. *Cont.*

Primary Study	Summary of Contribution	Blockchain-Driven Enhancements to Forensic Principles	Drawbacks or Challenges of Approach	Primary Digital Forensics Domain in Focus	Primary Phase(s) Addressed
PS3—Xiao et al. [91]	This paper presents a framework for digital forensics in the Industrial Internet of Things (IIoT) using blockchain technology. The framework introduces a novel batch consensus mechanism based on an improved delegated proof-of-stake (DPoS) algorithm, enabling tamper-proof, non-repudiable, and real-time storage of evidence. A token-based access control mechanism enhances security and ensures efficient retrieval of evidence.	Evidence Integrity: Tamper Resistance, Data Security; Chain of Custody: Traceability, Provenance; Access Control	The limitation of this approach centers around scalability issues as data volumes grow to big data levels in IIoT systems, whereas the proposed model is currently limited to simulated environments, requiring real-world testing for broader applicability.	IoT Forensics	Collection, Preservation
PS4—Rana et al. [2]	This paper proposes a model leveraging the Layer 2 Polygon blockchain and IPFS for decentralized storage and management of digital evidence. Smart contracts automate access control, ensuring tamper-proof evidence handling. The model enhances transparency, reduces reliance on centralized authorities, and facilitates multi-country investigations.	Evidence Integrity: Data Integrity, Tamper Resistance; Chain of Custody: Traceability, Access Control	Limitations in this approach include vulnerabilities in smart contracts, a potential of 51% attacks, Sybil attacks, which involve creating multiple nodes to launch cyberattacks, and the scalability of managing increasing evidence volumes in real-world applications.	Storage Forensics	Collection, Reporting
PS5—Rane and Dixit [92]	The approach presented by this paper is the BlockSLaaS, a blockchain-assisted secure logging-as-a-service framework for cloud forensics. The solution uses a private-permissioned blockchain to ensure a tamper-proof chronological recording of logs, thereby preserving their integrity and confidentiality. Fine-grained access controls allow forensic investigators to retrieve logs securely while addressing multi-stakeholder collusion problems.	Evidence Integrity: Tamper Resistance, Log Integrity; Chain of Custody: Traceability, Access Control	The model faces challenges related to scalability in handling vast volumes of cloud generated logs, potential system delays, and the computational overhead of cryptographic operations.	Cloud Forensics	Collection, Preservation, Examination

Table 5. *Cont.*

Primary Study	Summary of Contribution	Blockchain-Driven Enhancements to Forensic Principles	Drawbacks or Challenges of Approach	Primary Digital Forensics Domain in Focus	Primary Phase(s) Addressed
PS6—Ragu and Ramamoorthy [93]	This paper proposes cloud forensics architecture integrating Software-Defined Networking (SDN) and blockchain technologies for privacy leakage prediction. The system leverages SAD-ECC encryption, fuzzy-based smart contracts, and Logical Graphs of Evidence (LGoE) to enhance evidence collection, analysis, and reporting in IaaS cloud environments. The architecture ensures secure, decentralized data storage and processing while addressing data provenance and traceability challenges.	Evidence Integrity: Data Integrity, Provenance; Chain of Custody: Traceability, Automation	Scalability issues due to the growing volume of evidence, computational overhead from complex cryptographic techniques, and the potential latency in forensic workflows.	Cloud Forensics	Identification, Collection, Preservation, Examination, Reporting
PS7—Pourvahab and Ekbatanifard [94]	This paper presents DFeSB, a digital forensic architecture integrating Software-Defined Networking (SDN) and blockchain technologies for evidence collection, provenance preservation, and forensic analysis in IaaS cloud environments. The system employs SA-DECC encryption, fuzzy-based smart contracts (FSCs), and Logical Graph of Evidence (LGoE) for comprehensive forensic processes. It ensures tamper-proof evidence storage, secure user authentication, and traceable evidence provenance.	Evidence Integrity: Data Integrity, Provenance; Chain of Custody: Traceability, Ownership Proof	Challenges of this architecture include scalability issues due to large-scale evidence volumes, high computational costs that are needed for the cryptographic algorithms, and latency in evidence verification workflows.	Cloud Forensics	Collection, Preservation, Examination, Reporting
PS8—Yan et al. [95]	This paper proposes a blockchain-based protocol for managing the chain of custody of digital evidence. The protocol integrates ciphertext-policy attribute-based encryption (CP-ABE) for secure access control, BLS signature for group consensus and verification, and blockchain for maintaining an immutable, traceable record of evidence creation, transfer, and storage. The approach emphasizes balancing privacy and traceability while ensuring evidence integrity and validity.	Evidence Integrity: Tamper Resistance, Traceability; Chain of Custody: Provenance, Transparency	Scalability issues arise from the increased computational and communication demands of the consensus mechanism as the size of groups and the number of transactions grow. These challenges can lead to delays in reaching consensus and broadcasting transactions to all nodes in the network.	Storage Forensics	Preservation, Collection, Examination

Table 5. *Cont.*

Primary Study	Summary of Contribution	Blockchain-Driven Enhancements to Forensic Principles	Drawbacks or Challenges of Approach	Primary Digital Forensics Domain in Focus	Primary Phase(s) Addressed
PS9—Liu et al. [96]	This paper presents a model that uses blockchain and multidimensional hash algorithms to preserve digital evidence securely. The model introduces dual custody chains: a branch chain for individual cases and a main chain for overarching integrity using multidimensional hashing. The model ensures high levels of automation, minimizes human intervention, and strengthens the chain of custody for digital forensics applications.	Evidence Integrity: Tamper Resistance, Provenance; Chain of Custody: Traceability, Automation	Challenges that this model face revolve around computational overhead issues due to multidimensional hashing and heavy encryption approach, also potential inefficiency in scalability when managing large volumes of evidence and users.	Storage Forensics	Preservation, Collection
PS10—Li et al. [97]	This paper proposes LEChain, a lawful evidence management framework using blockchain to secure the entire chain of custody in digital forensics. It incorporates randomizable signatures for witness privacy, CP-ABE for fine-grained access control, and PoA consensus on a consortium blockchain for managing evidence records. It also integrates juror voting during court trials with a privacy-preserving mechanism.	Evidence Integrity: Tamper Resistance, Immutability, Traceability; Chain of Custody: Transparency, Access Control	In the LEChain, scalability issues arise due to the significant computational resources required for cryptographic operations like CP-ABE and randomizable signatures. Additionally, the PoA consensus mechanism can introduce high communication overhead as the network grows, potentially causing delays. The complexity of managing multiple stakeholders with varying access levels further complicates real-world deployment.	Storage Forensics	Preservation, Reporting
PS11—Lone and Mir [98]	This paper proposes forensic chain, a blockchain-based model implemented using Hyperledger Composer to strengthen the chain of custody in digital forensics. The model incorporates evidence creation, transfer, deletion, and display functions to ensure the integrity, traceability, and authenticity of digital evidence throughout its lifecycle. The system uses a permissioned blockchain to securely store metadata and logs related to evidence transactions.	Evidence Integrity: Tamper Resistance, Traceability; Chain of Custody: Transparency, Immutability	Scalability challenges may be experienced as a result of the limited throughput of Hyperledger Composer blockchain platform when there is large volume of data to be processed. It also faces challenges of high computational overhead for managing large volumes of evidence, and the complexity of real-time integration with existing forensic tools.	Storage Forensics	Preservation, Reporting

Table 5. *Cont.*

Primary Study	Summary of Contribution	Blockchain-Driven Enhancements to Forensic Principles	Drawbacks or Challenges of Approach	Primary Digital Forensics Domain in Focus	Primary Phase(s) Addressed
PS12—Cebe et al. [66]	This paper proposes a lightweight blockchain-based framework called Block4Forensic (B4F) for vehicular forensics. The framework leverages Vehicular Public Key Infrastructure (VPKI) for membership management and privacy preservation and uses a fragmented ledger approach to reduce blockchain storage overhead. By storing hashes of data in a shared ledger and maintaining detailed information in fragmented ledgers, the framework ensures evidence integrity and privacy while facilitating efficient accident analysis.	Evidence Integrity: Tamper Resistance, Immutability; Chain of Custody: Traceability, Privacy Preservation	Scalability challenges could arise from managing membership and fragmented ledger synchronization with millions of vehicles. Additionally, the framework lacks mechanisms for ensuring the availability of critical forensic data in cases of participant failures.	IoT Forensics	Collection, Preservation
PS13—Billard and Bartolomei [99]	This paper presents a blockchain-based navigation system for IoT-enabled vehicles, emphasizing digital forensics and privacy by design. Their proposed prototype leverages Hyperledger Fabric to ensure pseudonymized storage of GPS data for traffic analysis while maintaining user privacy under GDPR compliance. The system supports forensic investigations by providing immutable, non-repudiable logs of navigation history.	Evidence Integrity: Tamper Resistance, Immutability; Chain of Custody: Traceability, Privacy Preservation	This approach faces limitations concerning the practical challenges of integrating the blockchain-based system with existing vehicular systems. Furthermore, potential security vulnerabilities and risks associated with pseudonymized data patterns persist such as the inability to guarantee the accuracy of submitted data and privacy risks around the probability of identifying users through data patterns remains.	IoT Forensics	Preservation, Examination
PS14—Li, Chen et al. [100]	This paper introduces Eunomia, a vehicular digital forensics (VDF) framework leveraging a consortium blockchain to ensure privacy, accountability, and traceability. The framework models investigations as finite state machines executed through smart contracts, enabling evidence management and traitor tracing. Data confidentiality is maintained using CP-ABE and Bulletproofs, while pseudonymous identities safeguard user privacy. The framework is evaluated using an Ethereum-based prototype.	Evidence Integrity: Tamper Resistance, Confidentiality; Chain of Custody: Traceability, Privacy Preservation	Scalability issues arise from computational and communication overheads in cryptographic operations (e.g., CP-ABE and Bulletproofs). Additionally, pseudonymity risks user identity exposure through data patterns, and the system complexity poses integration challenges.	IoT Forensics	Collection, Preservation, Examination

Table 5. *Cont.*

Primary Study	Summary of Contribution	Blockchain-Driven Enhancements to Forensic Principles	Drawbacks or Challenges of Approach	Primary Digital Forensics Domain in Focus	Primary Phase(s) Addressed
PS15—Menard and Abouy-oussef [101]	This paper proposes a privacy-preserving vehicular digital forensics (VDF) strategy utilizing a consortium blockchain and group signatures. The strategy ensures user anonymity while maintaining traceability in cases of misconduct. Two ledgers are used: one for general vehicular data and another for evidence. Performance evaluations demonstrate low computational overhead and efficient communication.	Evidence Integrity: Tamper Resistance, Traceability; Chain of Custody: Anonymity, Privacy Preservation	Limitations of this model include potential scalability issues in managing two ledgers with increasing vehicle and evidence data. Computational overhead from cryptographic operations like group signatures may affect real-time processing in larger networks.	IoT Forensics	Collection, Preserva-tion
PS16—Philip and Sara-vanaguru [102]	This paper proposes a smart contract-based digital evidence management framework for vehicle accident investigations on the Internet of Vehicles (IoV) era. The framework integrates blockchain and InterPlanetary File System (IPFS) to collect, preserve, and manage evidence from vehicles, neighboring devices, and infrastructure. Dynamic access control is implemented using smart contracts, ensuring data sharing among stakeholders such as law enforcement and insurance providers. The framework is evaluated for performance and cost-efficiency in both public and private blockchain environments.	Evidence Integrity: Tamper Resistance, Immutability; Chain of Custody: Traceability, Access Control	Limitations of this framework include high computational and communication overhead when deploying smart contracts on public blockchains, as well as scalability concerns existing as well because as accident-related data grows, the storage and retrieval of evidence on the blockchain and IPFS require substantial computational resources, which may lead to bottlenecks. Also, the dependence on IPFS pinning services for long-term evidence storage introduces external risks if it cannot be sustained.	IoT Forensics	Collection, Preserva-tion,
PS17—Hu et al. [103]	This paper proposes TFChain, a blockchain-based trusted forensics scheme for the entire lifecycle of mobile phone data. By integrating memory analysis and blockchain technology, the framework ensures the authenticity, timeliness, and traceability of evidence. It minimizes manual intervention by automating evidence collection, storage, and analysis while maintaining security through Practical Byzantine Fault Tolerance (PBFT) on Hyperledger Fabric. Evidence is stored in IPFS, with blockchain maintaining metadata and transaction records.	Evidence Integrity: Tamper Resistance, Immutability, Auditability; Chain of Custody: Traceability, Automation	Scalability limitations arise due to increased storage demands and computational resources for IPFS and PBFT as evidence volume grows. Reliance on off-chain storage (IPFS) introduces dependency risks and potential delays in data retrieval. Additionally, the scheme relies on a trusted authority, which could be a single point of failure.	Mobile Forensics	Collection, Preserva-tion, Reporting

Table 5. *Cont.*

Primary Study	Summary of Contribution	Blockchain-Driven Enhancements to Forensic Principles	Drawbacks or Challenges of Approach	Primary Digital Forensics Domain in Focus	Primary Phase(s) Addressed
PS18—Liang et al. [104]	This paper presents a blockchain-based IoT forensics system that integrates alliance chains and distributed storage to improve the integrity and traceability of IoT evidence. The framework supports evidence collection, analysis, and reporting while ensuring data security and access control through blockchain technology. A case study on drone forensics demonstrates the applicability of the system in real-world scenarios.	Evidence Integrity: Tamper Resistance, Traceability; Chain of Custody: Transparency, Access Control	The framework faces scalability issues as the IoT data volumes grows, straining the distributed storage systems and leading to potential bottlenecks in storage and retrieval. Additionally, the reliance on IoT convergence devices introduces a single point of failure as these devices are responsible for data aggregation and validation before uploading to the blockchain. If compromised it could result in the loss of evidence integrity, risking the forensic process. Furthermore, ensuring the security and synchronization of alliance chain nodes across different jurisdictions adds complexity to deployment.	IoT Forensics	Collection, Preserva-tion, Reporting
PS19—Tsai [105]	This paper proposes a blockchain-based chain of custody framework implemented on a private Ethereum blockchain to enhance digital evidence management. The framework uses smart contracts to enforce role-based access control, ensuring secure evidence collection, transfer, and verification across the preliminary investigation, case management, and court phases. The framework's immutability and traceability features strengthen the admissibility of digital evidence in judicial proceedings.	Evidence Integrity: Tamper Resistance, Traceability; Chain of Custody: Transparency, Access Control	The framework faces scalability challenges, particularly as the volume of digital evidence grows, increasing computational demands on Ethereum nodes. Also, there is the issue of managing cross-border case sharing, which introduces complexities in synchronizing data across different jurisdictions.	Storage Forensics	Collection, Preserva-tion, Reporting

Table 5. *Cont.*

Primary Study	Summary of Contribution	Blockchain-Driven Enhancements to Forensic Principles	Drawbacks or Challenges of Approach	Primary Digital Forensics Domain in Focus	Primary Phase(s) Addressed
PS20—Lusetti et al. [106]	This paper proposes a blockchain-based solution for the custody of digital forensic files in forensic medicine, using Hyperledger Fabric. The solution incorporates a hybrid cryptographic system (AES and RSA) to encrypt and securely store digital evidence in redundant online storage while ensuring traceability via a private blockchain. It enables role-based access management and records all user actions on the blockchain to maintain evidence integrity and access transparency.	Evidence Integrity: Tamper Resistance, Confidentiality; Chain of Custody: Traceability, Access Control	Scalability challenges stem from managing large volumes of digital files and user operations on the blockchain. The system also depends heavily on the proper deployment of secure hardware, such as USB devices and tamper-resistant modules. The study also highlights that compatibility of this solution with varying legal frameworks across jurisdictions may be complex.	Storage Forensics	Preservation, Reporting
PS21—Awuson-David et al. [107]	This paper proposes a Blockchain Cloud Forensic Logging (BCFL), a framework for acquiring and preserving log evidence in cloud ecosystems. The framework, which is built on Hyperledger Fabric, ensures tamper-proof evidence collection and traceability using smart contracts and distributed ledger technology. BCFL also addresses compliance with GDPR by maintaining an auditable chain of custody for evidence. The framework's effectiveness is demonstrated through a case study in a simulated cloud environment.	Evidence Integrity: Tamper Resistance, Traceability; Chain of Custody: Transparency, Access Control	Scalability concerns exist due to increased demands on the distributed ledger as cloud log inevitably grows. Also, reliance on a single simulated environment rather than operational cloud ecosystems raises questions about real-world applicability especially as different cloud environments exist.	Cloud Forensics	Collection, Preservation, Reporting
PS22—Tyagi et al. [108]	This paper proposes a blockchain-enabled intelligent digital forensics system for autonomous connected vehicles (ACVs). The system combines blockchain with AI to collect, analyze, and report digital evidence while maintaining privacy and security. It utilizes short randomizable signatures for witness anonymity, ciphertext-policy attribute-based encryption (CP-ABE) for access control, and a distributed ledger for immutable evidence storage. The framework supports multi-stakeholder collaboration in ACV incident investigations.	Evidence Integrity: Tamper Resistance, Immutability; Chain of Custody: Traceability, Privacy Preservation	High computational and communication overhead due to cryptographic operations like CP-ABE and randomizable signatures. Scalability concerns also arise with large-scale data from numerous sensors, and nodes in ACV ecosystems are considered. Finally, since real-time data processing in the distribution system is implemented, it may introduce some delay.	IoT Forensics	Collection, Preservation, Reporting

Table 5. *Cont.*

Primary Study	Summary of Contribution	Blockchain-Driven Enhancements to Forensic Principles	Drawbacks or Challenges of Approach	Primary Digital Forensics Domain in Focus	Primary Phase(s) Addressed
PS23—Rao et al. [109]	This paper introduces a blockchain-based digital evidence management system for maintaining the chain of custody (CoC). The system ensures tamper-proof evidence handling from collection to presentation in court by storing evidence records in a private blockchain and enforcing integrity through cryptographic hashes. The proposed system supports evidence tracking, validation, and synchronization across participants in a forensic investigation.	Evidence Integrity: Tamper Resistance, Traceability; Chain of Custody: Transparency, Auditability	Scalability challenges arise as the volume of evidence grows, increasing storage and synchronization demands on the blockchain. The reliance on private blockchains limits interoperability with external systems and raises trust concerns in multi-stakeholder scenarios.	Storage Forensics	Collection, Preservation, Reporting
PS24—Khan et al. [110]	This paper introduces MF-Ledger, a blockchain-enabled multimedia forensic investigation architecture built on Hyperledger Sawtooth. The architecture supports the collection, preservation, and analysis of multimedia evidence, leveraging smart contracts for automated processes and maintaining the chain of custody through an immutable and distributed ledger. The system incorporates Practical Byzantine Fault Tolerance (PBFT) and Proof of Elapsed Time (PoET) consensus mechanisms to ensure security and scalability.	Evidence Integrity: Tamper Resistance, Traceability; Chain of Custody: Provenance, Transparency	This approach faces scalability challenges, which stem from its ability to handle large multimedia files and integrate distributed storage solutions. Furthermore, additional computational overhead is introduced due to the use of PBFT and PoET consensus mechanisms. Further, managing stakeholder coordination in a decentralized environment adds complexity.	Multimedia Forensics	Collection, Preservation, Reporting
PS25—Yunianto et al. [111]	This paper presents B-DEC (Blockchain Digital Evidence Cabinet), a blockchain-based digital evidence management system designed to secure the chain of custody (CoC). Built on Ethereum private blockchain, the system integrates smart contracts for automating access control and ensuring evidence integrity. B-DEC enhances the traditional Digital Evidence Cabinet (DEC) by adding features such as evidence splitting, detailed logging, and JSON-based structured CoC documentation for forensic investigations.	Evidence Integrity: Tamper Resistance, Traceability; Chain of Custody: Auditability, Transparency	Scalability concerns arise from the increased computational requirements and storage needs for managing the resulting complex CoC structures. Additionally, this prototype requires high GAS fees, and some execution delays persist, which could impede real-time evidence management. Finally, the lack of standardization across digital evidence formats is an issue that may impede the integration with real-word applications.	Storage Forensics	Collection, Preservation, Reporting

Table 5. *Cont.*

Primary Study	Summary of Contribution	Blockchain-Driven Enhancements to Forensic Principles	Drawbacks or Challenges of Approach	Primary Digital Forensics Domain in Focus	Primary Phase(s) Addressed
PS26—Duy et al. [112]	This paper proposes the SDNLog-Foren system, a blockchain-based log management system for Software Defined Networking (SDN) forensics. The system integrates Hyperledger Fabric to ensure tamper resistance and integrity of log files used in forensic investigations. SDNLog-Foren employs log filtering, segmentation, and distributed ledger storage to manage and preserve log evidence securely while providing fine-grained access control for investigators.	Evidence Integrity: Tamper Resistance, Auditability; Chain of Custody: Traceability, Transparency	The system faces concerns with scalability due to the high volume of log data generated in SDN environments, which can overwhelm the blockchain's transaction handling and storage capacity. This will lead to slower performance as the size of the ledger grows larger. Also, managing frequent transactions and syncing them across multiple blockchain nodes increases latency and computational overhead.	Network Forensics	Collection, Preservation, Reporting
PS27—Kumar et al. [8]	This paper proposes the Internet-of-Forensics (IoF) framework, a blockchain-based digital forensics system designed for IoT applications. The framework integrates a hierarchical blockchain structure with chain of custody (CoC), evidence chain (EC), and case chain (CC) to ensure transparency, traceability, and integrity of evidence. It leverages lattice-based cryptography for post-quantum security and efficient computation. The system addresses cross-border legal challenges through consortium blockchain.	Evidence Integrity: Tamper Resistance, Traceability; Chain of Custody: Transparency, Automation	Scalability concerns arise due to the growing number of IoT devices and the increasing size of blockchain records, which can lead to storage and processing delays. Additionally, the high computational cost of lattice-based cryptographic operations and synchronization issues in cross-border consortium blockchain setups still poses challenges that need to be handled such as diverse legal frameworks across regions and time zone differences.	IoT Forensics	Collection, Preservation, Reporting
PS28—Pourvahab and Ekbatanifard [113]	This paper proposes a forensics architecture for SDN-IoT environments integrating blockchain technology to address challenges such as evidence tampering, traceability, and chain of custody (CoC) management. The system uses the Linear Homomorphic Signature (LHS) algorithm for device authentication and a Neuro Multi-Fuzzy classifier for packet analysis. Logs and evidence are stored immutably in the blockchain, ensuring transparency and accountability for forensic investigations.	Evidence Integrity: Tamper Resistance, Traceability; Chain of Custody: Provenance, Automation	Managing extensive log data and computational requirements for the LHS algorithm and Neuro Multi-Fuzzy model poses scalability concerns. Also, integration with existing SDN-IoT infrastructure is complex, and the distributed nature of the architecture may lead to synchronization delays in evidence updates across nodes.	Network Forensics	Collection, Preservation, Reporting

Table 5. *Cont.*

Primary Study	Summary of Contribution	Blockchain-Driven Enhancements to Forensic Principles	Drawbacks or Challenges of Approach	Primary Digital Forensics Domain in Focus	Primary Phase(s) Addressed
PS29—Mothukuri et al. [114]	This paper proposes BlockHDFS, a blockchain-integrated Hadoop Distributed File System (HDFS) for secure provenance traceability. By using Hyperledger Fabric, the system records file metadata, such as hash values, access times, and modification times, in an immutable blockchain ledger. This ensures tamper-proof logging, allowing investigators to trace file changes and verify evidence integrity during forensic investigations.	Evidence Integrity: Tamper Resistance, Traceability; Chain of Custody: Provenance, Transparency	Performance overheads occur in metadata extraction and blockchain logging processes, particularly during high data loads. This indicates scalability issues likely arising due to increasing metadata size and synchronization demands as file volumes grow. Also, the periodic execution of the NodeJS client introduces potential delays in real-time applications.	Storage Forensics	Preservation, Reporting
PS30—Nyaletey et al. [115]	This paper proposes BlockIPFS, a blockchain-integrated Interplanetary File System (IPFS) for enhancing forensic traceability and secure data sharing. By utilizing Hyperledger Fabric, the system logs metadata, such as file hashes, access timestamps, and owner details in an immutable ledger, while raw files remain on the IPFS network. The solution provides clear audit trails for forensic investigations and authorship protection, ensuring accountability and privacy in distributed file systems.	Evidence Integrity: Tamper Resistance, Traceability; Chain of Custody: Provenance, Transparency	Managing large volumes of metadata and synchronizing blockchain logs introduces significant overhead that can impact system efficiency. Furthermore, the framework lacks robust mechanisms to restrict access to file hashes outside the blockchain, which may lead to unauthorized sharing. The execution of smart contracts also adds computational complexity, affecting overall performance.	Storage Forensics	Preservation, Reporting
PS31—Sakshi et al. [116]	This paper proposes the Blockchain-based Evidence Preservation Framework for IoT (BEvPF-IoT), which integrates Ethereum blockchain and IPFS for preserving the integrity and chain of custody (CoC) of digital evidence in IoT environments. The framework ensures secure and tamper-proof storage of evidence metadata on the blockchain while leveraging IPFS for cost-efficient storage of the actual evidence. The use of smart contracts automates evidence management and facilitates accountability during forensic investigations.	Evidence Integrity: Tamper Resistance, Immutability; Chain of Custody: Traceability, Transparency	High transaction latency is observed when the number of transactions per second exceeds 35, leading to performance bottlenecks. Gas consumption increases with the complexity of transactions, raising operational costs. Additionally, the system's reliance on IPFS introduces risks related to the availability and long-term pinning of evidence data.	IoT Forensics	Collection, Preservation, Reporting

Table 5. *Cont.*

Primary Study	Summary of Contribution	Blockchain-Driven Enhancements to Forensic Principles	Drawbacks or Challenges of Approach	Primary Digital Forensics Domain in Focus	Primary Phase(s) Addressed
PS32—Zarpala and Casino [117]	This paper proposes a blockchain-based forensic model for financial crime investigations, focusing on embezzlement scenarios. The system uses Ethereum blockchain and smart contracts to manage evidence and preserve the chain of custody. The architecture ensures integrity, traceability, and tamper-proofness of evidence while supporting cross-border collaboration. It includes functionalities for evidence collection, logging, and secure reporting.	Evidence Integrity: Tamper Resistance, Auditability; Chain of Custody: Traceability, Transparency	Synchronization challenges arise when integrating with cross-border financial systems due to differing regulations and data-sharing protocols. The use of Ethereum introduces gas costs, which can increase operational expenses. Additionally, the system's adaptability to other financial crimes requires further customizations and testing.	Storage Forensics	Collection, Preserva-tion, Reporting
PS33—Verma et al. [118]	This paper introduces NyaYa, a blockchain-based electronic law record (ELR) management scheme for judicial investigations. The system leverages Ethereum blockchain and IPFS for secure storage, ensuring the transparency and traceability of ELRs. Smart contracts automate case registration, metadata updates, and legal proceedings. NyaYa addresses issues such as chronology, trust, and privacy among judicial stakeholders while optimizing data storage using an off-chain approach.	Evidence Integrity: Tamper Resistance, Traceability; Chain of Custody: Transparency, Automation	In this scheme, managing the increasing volume of ELRs leads to performance overhead in blockchain synchronization and querying, especially during intensive investigative updates. The reliance on IPFS for off-chain storage introduces risks related to long-term data retention and the availability of evidence records. Additionally, gas fees on Ethereum may make the framework cost-intensive for frequent transactions.	Storage Forensics	Preservation, Reporting
PS34—Fu et al. [119]	This paper presents BZK (Blockchain Zhengju Keeper), a lightweight blockchain-based storage mechanism for managing digital evidence (DE). The system subtracts Hyperledger Fabric's complex functionalities to optimize DE storage and verification. BZK utilizes on-chain storage for DE metadata and off-chain storage for original files, ensuring integrity and scalability. The Votes-as-a-Proof (VaaP) consensus protocol is employed to enable efficient and parallel transaction execution.	Evidence Integrity: Tamper Resistance, Traceability; Chain of Custody: Provenance, Auditability	The reliance on off-chain storage introduces risks of data loss if DE keepers fail to retain files properly. Synchronization challenges may arise in managing metadata updates across blockchain nodes. Additionally, the absence of smart contract functionalities limits system extensibility for more complex use cases.	Storage Forensics	Preservation, Reporting

Table 5. *Cont.*

Primary Study	Summary of Contribution	Blockchain-Driven Enhancements to Forensic Principles	Drawbacks or Challenges of Approach	Primary Digital Forensics Domain in Focus	Primary Phase(s) Addressed
PS35—Lawrence and Shreelekshmi [120]	This paper presents a blockchain-enabled video integrity verification framework utilizing the Edwards Curve Digital Signature Algorithm (EdDSA) and BLAKE2b hash function. The system ensures tamper-proof video integrity and traceability by storing video segment signatures and block hashes on a blockchain. The chained structure of signatures across blocks enhances security and provides 100% detection of forgery. The framework is designed for use in resource-constrained environments such as surveillance systems.	Evidence Integrity: Tamper Resistance, Traceability; Chain of Custody: Transparency, Automation	The computational requirements for signature generation and validation may be challenging for highly resource-constrained devices. Also, the reliance on a pre-segmented video structure may limit its applicability for continuous, non-segmented video streams. Integration with legacy video storage systems could also pose challenges.	Multimedia Forensics	Collection, Preservation
PS36—Apirajitha and Devi [121]	This paper introduces a blockchain-based forensic framework for cloud environments using the Multi-objective Krill Herd Cuckoo Search Optimization Algorithm (MKHCSOA). The system leverages blockchain and smart contracts to enhance data integrity, traceability, and preservation while reducing computational overhead. MKHCSOA optimizes data encryption and decryption processes, ensuring security and efficiency in managing evidence. The framework is tested on a private Ethereum blockchain with real-world datasets, demonstrating improved throughput and reduced latency compared to traditional methods.	Evidence Integrity: Tamper Resistance, Traceability; Chain of Custody: Provenance, Transparency	The framework faces challenges in ensuring seamless data sharing across cloud environments due to jurisdictional differences and regulatory compliance requirements. The computational demands of the MKHCSOA algorithm could limit its scalability in environments with limited resources. Furthermore, the operational costs linked to Ethereum gas fees may hinder the adoption of this solution for large-scale forensic investigations.	Cloud Forensics	Collection, Preservation, Reporting
PS37—Akhtar and Feng [122]	This paper proposes a blockchain-based model for ensuring the integrity of digital forensic evidence collected in IoT environments. The system combines blockchain technology with hashing algorithms and machine learning models (XGBoost and KMeans) to predict anomalies in forensic evidence and secure transactions. The model ensures data integrity, tamper resistance, and real-time threat prediction, addressing the challenges of confidentiality and security in IoT forensic investigations.	Evidence Integrity: Tamper Resistance, Traceability; Chain of Custody: Provenance, Transparency	In this model, the computational demands of integrating blockchain with machine learning models may strain resource-constrained IoT devices. It is also possible that synchronization delays may occur due to this, which can affect real-time detection of anomalies or threats.	IoT Forensics	Collection, Preservation, Reporting

Table 5. *Cont.*

Primary Study	Summary of Contribution	Blockchain-Driven Enhancements to Forensic Principles	Drawbacks or Challenges of Approach	Primary Digital Forensics Domain in Focus	Primary Phase(s) Addressed
PS38—Rani et al. [123]	This paper introduces a blockchain-based secure digital evidence preservation system for IoT-enabled smart environments. The system integrates Ethereum blockchain and IPFS to address challenges in the chain of custody, evidence integrity, and privacy. The proposed model incorporates smart contracts to automate evidence management and employs a consortium blockchain for secure and transparent collaboration among stakeholders. Simulation results demonstrate improved throughput and reduced latency compared to centralized solutions.	Evidence Integrity: Tamper Resistance, Traceability; Chain of Custody: Transparency, Privacy Preservation	Ethereum blockchain's mining process (10 to 15 s or more in some cases) may delay real-time evidence processing, affecting time-sensitive forensic investigations. While IPFS resolves storage issues, high transaction volumes could still impact overall system performance.	IoT Forensics	Collection, Preservation, Reporting
PS39—Ghaderi and Ghahyazi [124]	This paper proposes a conceptual blockchain-based framework for secure remote monitoring in Industrial IoT (IIoT) environments. Using Hyperledger Fabric (HFB), the system ensures real-time data monitoring, integrity, and tamper resistance. Experiments validate the framework's ability to minimize data packet loss by optimizing parameters such as block generation time and transaction intervals.	Evidence Integrity: Tamper Resistance, Traceability; Chain of Custody: Provenance, Transparency	The system's performance heavily relies on meeting specific conditions, such as ensuring that the transaction generation period is greater than or equal to the block generation time. Failure to meet this condition can lead to data packet loss and reduced network functionality. Also, the reliance on robust hardware for network nodes adds to the operational complexity as insufficient processing and storage capabilities may hinder real-time data monitoring.	IoT Forensics	Collection, Preservation

4. Summary of Primary Study

As a result of our background review, the following areas are reflected in the summary of the primary studies in Table 5. The Summary of Contribution column helps us answer RQ1 by providing insights into how different studies apply blockchain technology to address key challenges such as evidence integrity, the chain of custody, and privacy or other targeted requirements in those studies. This column provides a summary of the specific contributions of each study and the innovative approaches employed to integrate blockchain into digital forensic processes.

The inclusion of the Blockchain-Driven Enhancements to Forensic Principles column is rooted in the critical role that digital forensic principles play in ensuring the admissibility, reliability, and ethical handling of digital evidence. Through a background review, it was established that the two core principles of digital forensics are evidence integrity and the chain of custody (CoC). This column expands on the blockchain properties explored in

the solutions, such as immutability, transparency, traceability, and automation, and their alignment with these foundational principles.

The Drawbacks or Challenges of Approach column helps us answer RQ2 by detailing the limitations and barriers that blockchain-based solutions face in the field of digital forensics. These challenges include scalability, computational costs, integration difficulties, and jurisdictional complexities, providing an understanding of the current gaps and opportunities for improvement in blockchain applications.

The Primary Digital Forensics Domain in Focus column is essential for answering RQ1 as it identifies the specific areas within digital forensics—such as IoT forensics, cloud forensics, and storage forensics—where blockchain technology has been most actively explored. Finally, the Primary Phase(s) Addressed column supports answering RQ2 by categorizing the phases of the forensic process—such as collection, preservation, and reporting—where blockchain technology has been predominantly applied. This helps in understanding the emphasis placed on certain phases and the gaps in others.

5. State of the Art in Blockchain Application in the Field of Digital Forensics: A Visual Schema

The high-level schema illustrating the application of blockchain technology in digital forensics is presented in Figure 2 where a description of the intersection between these two fields is identified. The schema is further divided into Figures 3 and 4 to provide a low-level view of each field and the findings. This visual schema is developed by reviewing the existing body of literature on the subject through this SLR. The focus of the proposed schema is on addressing the key challenges that we have categorized into requirements in Section 2, as well as the domains and phases of digital forensics where blockchain has been applied, the blockchain properties leveraged by the reviewed papers, and the platforms, types, and technologies involved.

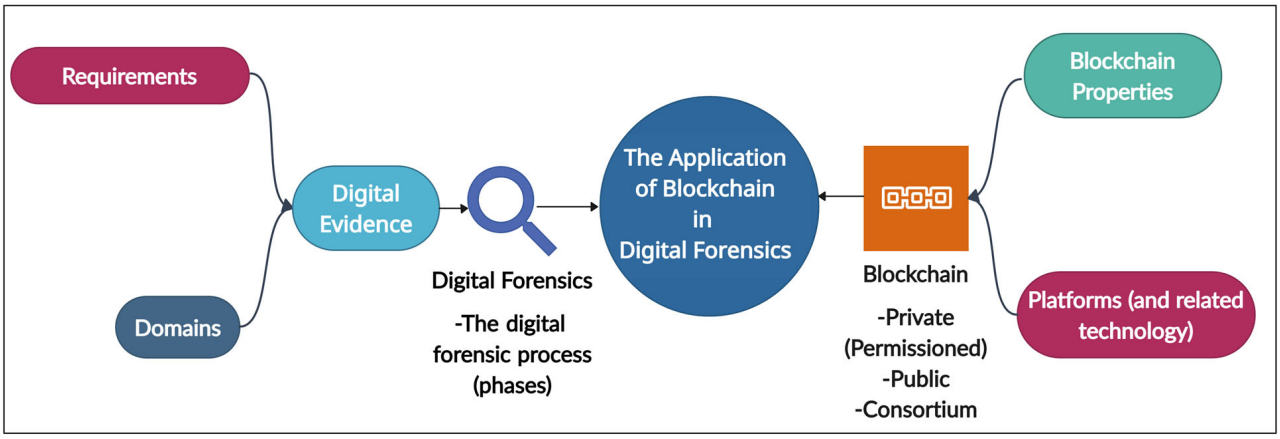

Figure 2. High-level visual schema of blockchain application in digital forensics.

To construct the schema, we conducted a background review of digital forensics and blockchain technology as aforementioned in Section 2. After which, we conducted a systematic review of the existing literature and summarized it in Table 5. We first classified the requirements of digital forensics into three distinct groups based on the literature. Secondly, we identified the domains where blockchain applications have been implemented in digital forensics; next, we examined the blockchain properties utilized to meet the identified requirements as well as the blockchain platforms and related technology employed in these studies. A detailed description of the visual schema is presented in this section.

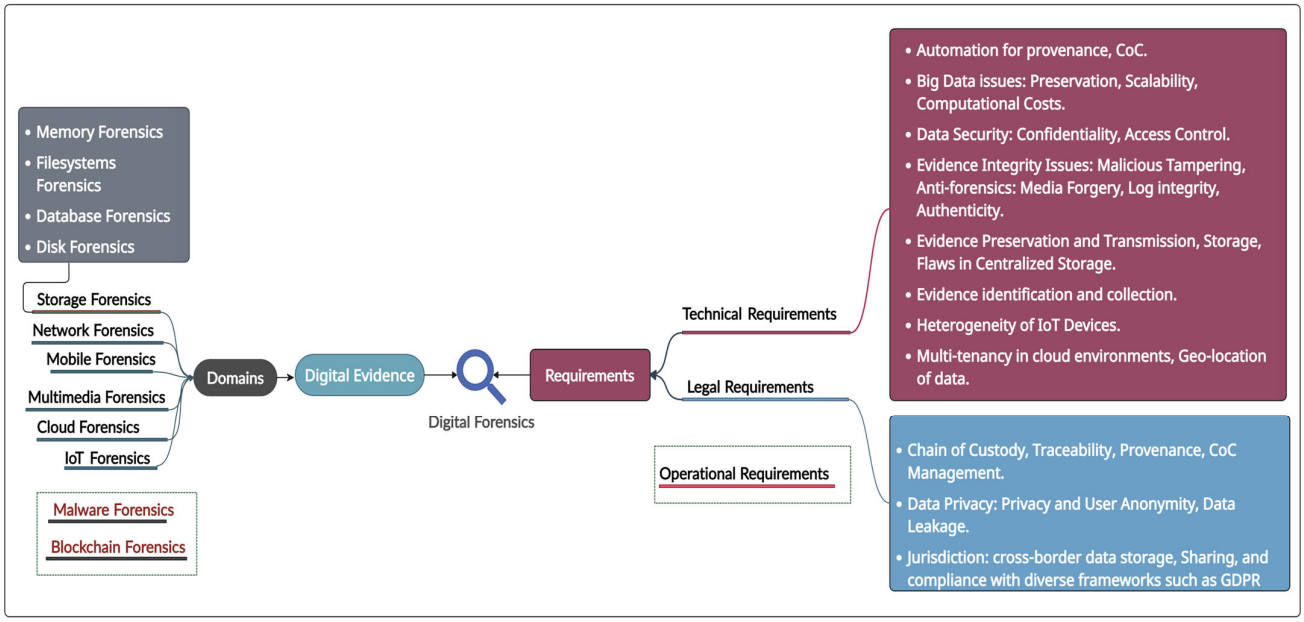

Figure 3. Digital forensics findings (visual schema of application of blockchain to digital forensics).

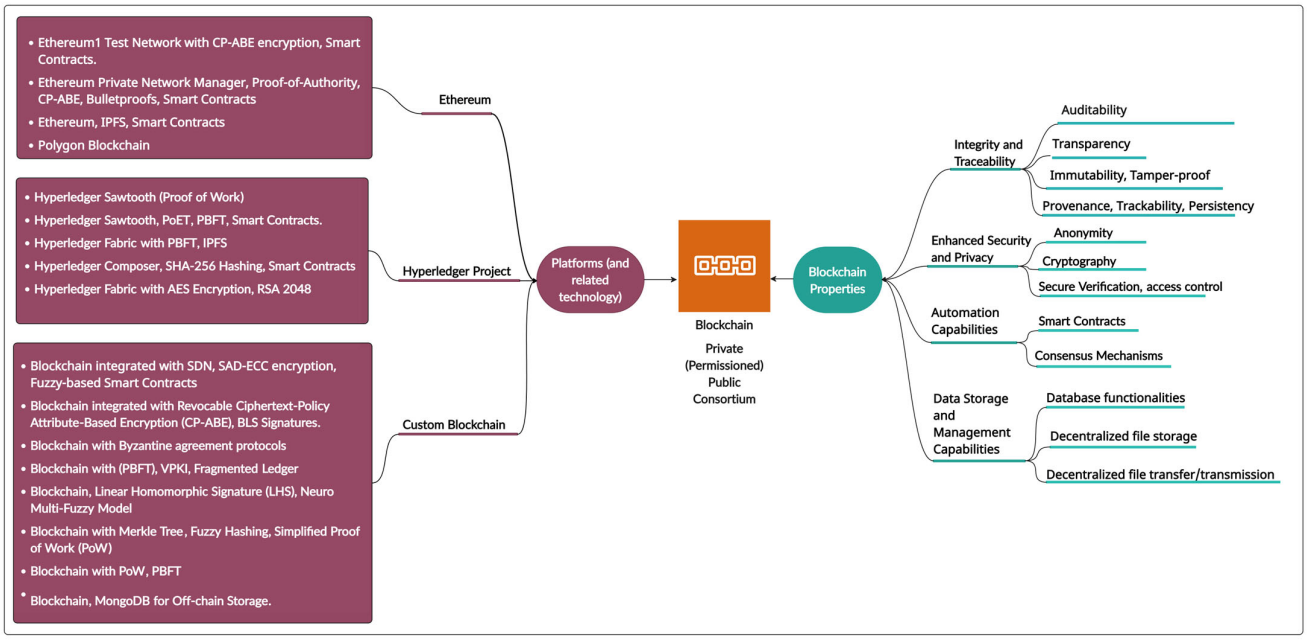

Figure 4. Blockchain findings (schema of application of blockchain to digital forensics).

This visual schema provides a comprehensive view of the current state of blockchain applications in the field of digital forensics. By systematically categorizing the key challenges and requirements, it provides valuable insights into how blockchain technology is being utilized to address critical issues such as evidence integrity, the chain of custody, and data privacy. It further identifies the domains and phases of digital forensics where blockchain has shown potential and the properties and platforms of blockchain that have so far been explored. This structured analysis reflects not only the versatility and applicability of blockchain technology in enhancing the different facets of digital forensic processes but also serves as a foundational reference for future research and development in this evolving field.

5.1. Digital Forensics Domains Explored

The findings from the systematic literature review (SLR) indicate that blockchain technology has been applied to six key domains within digital forensics. As illustrated in Figure 5, most of the research has centered on IoT Forensics and Storage Forensics, with these two domains receiving significantly more attention than others.

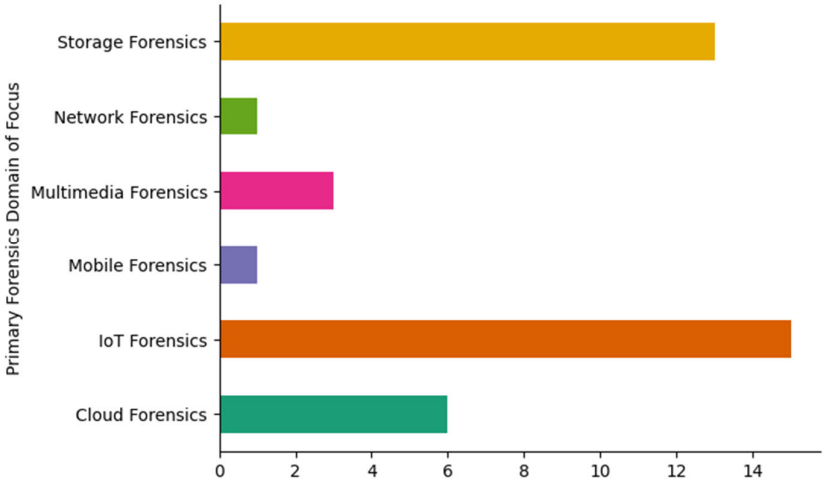

Figure 5. Primary forensics domain of focus.

IoT Forensics has emerged as the most prominent domain, reflecting the growing reliance on IoT devices in modern infrastructure. The big amount of data generated by these devices and the complexity that comes with their ecosystems have created a pressing need for robust forensic solutions. Blockchain technology, with its properties to ensure data integrity, traceability, and tamper resistance, provides a valuable opportunity for addressing these challenges. Also, Storage Forensics has seen considerable interest, particularly in contexts where the integrity and immutability of stored evidence at rest are paramount. With the rise of cloud computing and distributed storage systems, ensuring secure and reliable storage of digital evidence has become a significant concern. Blockchain has been widely employed in this domain to enhance the generation of the chain of custody (CoC), proving that stored data remain intact and trustworthy throughout its lifecycle.

As depicted in Figure 5, other domains, such as Cloud Forensics and Multimedia Forensics, are also notably explored in the subject area with Cloud Forensics dealing with the unique challenges associated with investigating incidents and collecting evidence from cloud environments, and Multimedia Forensics addressing the secure transmission, storage, size, and verification of multimedia data, such as images or videos. Network Forensics and Mobile Forensics appear less frequently in the primary study, which indicates a need for further exploration of blockchain-based solutions in these areas. Both domains pose unique challenges, but the existing studies show that blockchain has the potential to enhance the forensic process in both fields if there is additional research to fully harness its capabilities.

Most notably, we found no existing blockchain-based solutions in the areas of Malware Forensics and Blockchain Forensics (the forensic investigation of blockchain technology itself). This absence highlights a potential gap in the research and presents a novel opportunity for future exploration. Researchers could focus on developing blockchain solutions for these unexplored domains, particularly given the increasing prevalence of malware attacks and the growing importance of blockchain technology in various sectors.

5.2. Digital Forensics Phases Explored

The results of this systematic literature review reveal a clear emphasis on the preservation phase of digital forensics, as seen in Figure 6. A significant 37.3% of the analyzed

studies (38 out of 39 papers) incorporate blockchain technology to address challenges related to this phase. This could be because preservation plays a critical role in ensuring the integrity and authenticity of digital evidence throughout its lifecycle. Blockchain's inherent properties—immutability, traceability, and secure storage—make it exceptionally well suited for this phase as they prevent unauthorized tampering and maintain a reliable chain of custody. The collection phase is another heavily explored area, with 28.4% of the papers (29 studies) leveraging blockchain to address issues related to gathering and securely storing digital evidence. Blockchain's ability to create a tamper-proof ledger of evidence acquisition activities could provide investigators with a reliable method for safeguarding evidence at the point of collection, thereby improving its admissibility in court and its reliability during investigations.

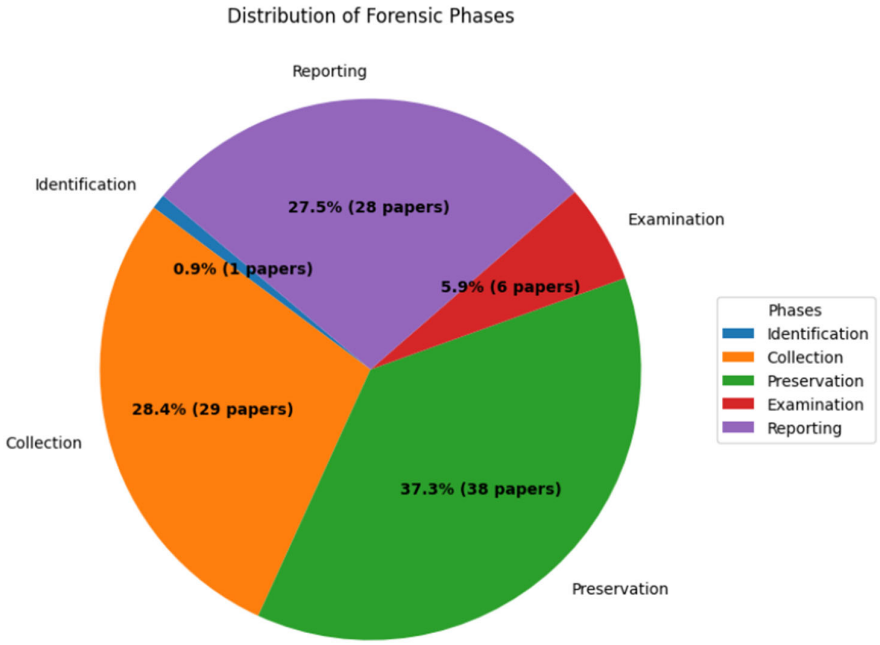

Figure 6. Digital forensics phase of focus.

The reporting phase is addressed by 27.5% of the studies (28 papers). Blockchain has been used to create transparent and auditable trails of evidence handling, which greatly aid in generating verifiable forensic reports and a reliable chain of custody. The focus on reporting demonstrates the importance of blockchain in maintaining accountability and ensuring evidence integrity during the final stages of forensic investigations.

Interestingly, only 5.9% (six studies) of the reviewed papers apply blockchain to the examination phase, and just 1% (one paper) explores its potential in the identification phase. For instance, Mahrous et al. [90] introduced blockchain to automate evidence detection and variation identification. While these phases receive less attention, they present opportunities for further research. Blockchain's ability to automate processes, establish provenance, and generate tamper-proof logs can potentially enhance both evidence identification and analysis in forensic investigations.

The findings highlight that the collection, preservation, and reporting phases dominate current blockchain applications in digital forensics. However, the lack of focus on the identification and examination phases points to gaps in research, suggesting opportunities to explore blockchain's transformative potential in these underrepresented areas. Future studies may uncover new ways to utilize blockchain to address challenges in these phases, further strengthening the overall digital forensics process.

5.3. Blockchain Type Utilized

The findings from this systematic literature review (SLR) highlight the diverse range of blockchain types applied in digital forensics solutions, as depicted in Figure 7. Most solutions rely on private or permissioned blockchains, with 25 out of 39 papers adopting this approach. This preference reflects the sensitive nature of forensic data and the necessity for stringent access control. Private or permissioned blockchains restrict participation to authorized parties, ensuring that evidence remains confidential and protected from unauthorized access. However, the use of this blockchain type also presents a potential challenge when viewed from a legal perspective. In legal domains, transparency is critical to ensuring fairness and accountability. A blockchain controlled by only a few authorized entities, as is the case with private or permissioned blockchains, could undermine this transparency. Such centralized control might raise concerns about the impartiality of evidence handling and the ability of stakeholders to independently verify evidence integrity.

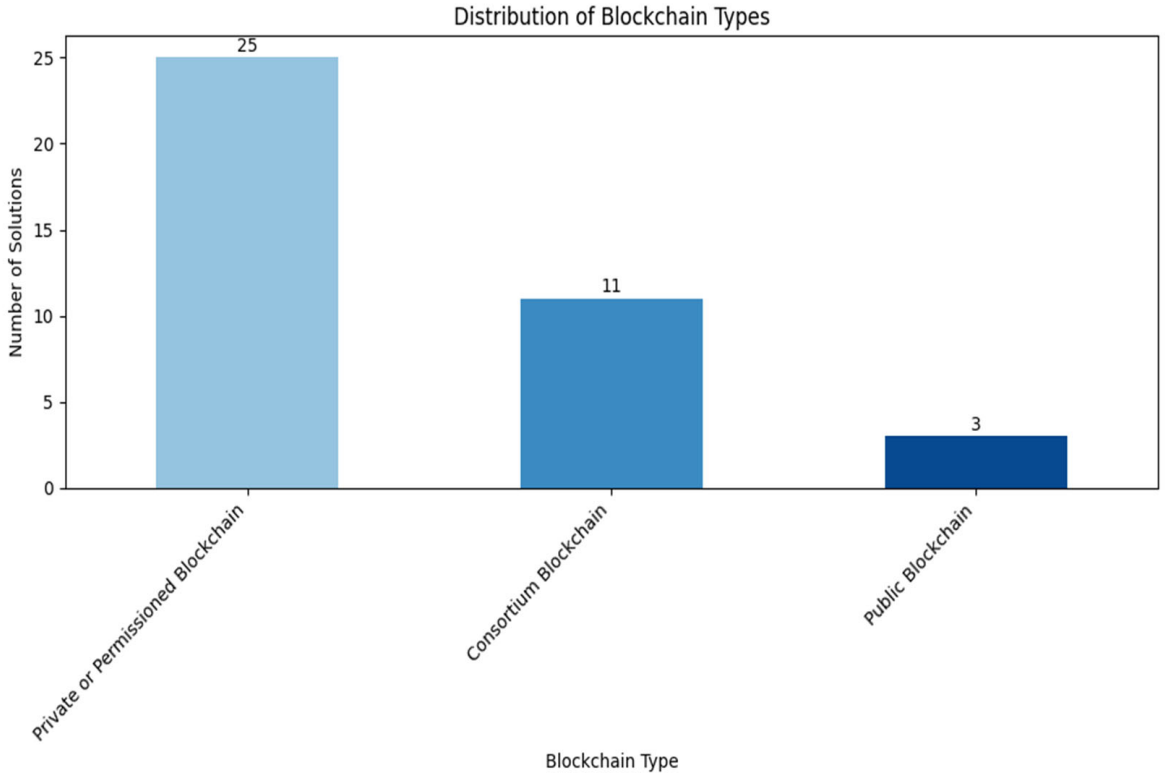

Figure 7. The blockchain types utilized.

Consortium blockchains, used in 11 of the reviewed studies, attempts to strike a balance as it offers a hybrid solution to this concern by combining the transparency of public blockchains with restricted participation in certain activities [101,122]. The general approach is to involve multiple pre-selected entities in the management of the blockchain. This setup enables collaboration and control among stakeholders, such as law enforcement agencies and private organizations, while maintaining transparency to other stakeholders like the court [102]. However, even in this model, the limited number of participants could lead to similar concerns about centralized control and accountability.

The adoption of public blockchains remains relatively low, with only three papers utilizing this approach. The limited use of public blockchains can be attributed to their inherent openness and transparency, but this often conflicts with the privacy and confidentiality requirements of digital forensics [92,98]. Also, the nature of digital forensics where

sensitive information is frequently involved is also a factor why public blockchain is not preferred, especially in domains like cloud forensics [121].

These trends suggest that the choice of blockchain type is heavily influenced by the unique requirements of digital forensics, particularly the need for privacy, controlled access, and collaborative flexibility. In the future, further research could focus more on consortium blockchains, which show potential in addressing the balance of transparency and confidentiality in forensic investigations.

5.4. Blockchain Platforms Utilized

The existing literature on blockchain solutions for digital forensics shows the utilization of several leading blockchain platforms to address key forensic challenges. The schema highlights the main platforms used, including Ethereum, the Hyperledger Project (and its variants), and a range of custom blockchain platforms, as shown in Figure 4. Each of these platforms has been employed to integrate blockchain properties such as Integrity and Traceability, Enhanced Security and Privacy, Automation, and Data Storage and Management into digital forensic solutions.

Many authors opt to create custom blockchains tailored to the unique requirements of digital forensics. For example, Rao et al. [109] utilize a private custom blockchain for managing digital evidence, ensuring tamper-proof logging from collection to court presentation. Similarly, Menard and Abouyoussef [101] develop a consortium-based blockchain to enable privacy-preserving vehicular forensics, utilizing dual ledgers to maintain anonymity, traceability, and efficient evidence handling. Pourvahab and Ekbatanifard [113] integrate a Linear Homomorphic Signature (LHS) with a custom blockchain to authenticate IoT devices and ensure the integrity of evidence logs in SDN-IoT environments. Another notable example is Mothukuri et al. [114], who design BlockHDFS, a custom blockchain integrated with the Hadoop Distributed File System (HDFS) to enhance provenance traceability for digital evidence by recording metadata on a tamper-proof ledger.

Although not a popular as Ethereum and Hyperledger project in the field, the use of the Polygon blockchain is also evident in the literature. Rana et al. [2] leverage the Polygon blockchain for decentralized storage and management of digital evidence, integrating IPFS to ensure tamper-proof handling and scalability. This combination highlights the adaptability of different blockchain platforms to meet specific forensic requirements.

The selection of Ethereum and Hyperledger underscores their suitability for addressing diverse forensic challenges. Ethereum, known for its public and decentralized nature, is often chosen for its ability to execute smart contracts, which automate processes such as evidence validation and access control. Philip and Saravanaguru [102] and Tyagi et al. [108] utilize Ethereum to implement dynamic access control and secure evidence sharing. Hyperledger, on the other hand, is preferred for permissioned environments where controlled access and customizable governance are required. Studies such as Hu et al. [103], Duy et al. [112], and Khan et al. demonstrate the use of Hyperledger for securely managing log evidence, automating the chain of custody, and ensuring privacy in multi-stakeholder scenarios.

In addition to blockchain platforms, several studies integrate non-blockchain technologies to enhance forensic solutions. For example, SDN is utilized in Ragu and Ramamoorthy [93] and Pourvahab and Ekbatanifard [94] to enable secure evidence collection and decentralized data management in cloud and IoT environments. LHS, as demonstrated by Pourvahab and Ekbatanifard [113], provides device authentication and secure log storage, ensuring tamper-proof evidence handling. Tyagi et al. [108] integrate AI with blockchain to predict and analyze forensic evidence in autonomous connected vehicles, enhancing accuracy and efficiency. IPFS is another widely used technology, as seen in [116] and

Nyaletey et al. [115], where it is leveraged for decentralized evidence storage, reducing on-chain storage burdens and improving scalability. Additionally, Mahrous et al. [90] utilize Merkle Trees to ensure data integrity by enabling verifiable proofs for evidence storage and retrieval.

The selection and integration of these platforms and technologies reflect the critical role of blockchain in enhancing the reliability, transparency, and scalability of digital forensics solutions. These findings underline the adaptability of blockchain platforms to diverse forensic contexts while highlighting the need for careful selection based on specific domain requirements.

6. Discussion of Results

6.1. RQ1: How Is Blockchain Technology Currently Integrated into Digital Forensics to Address Its Challenges, and What Key Advantages Does Its Application Offer?

The integration of blockchain technology into digital forensics has brought forth innovative approaches to addressing long-standing challenges in the field. The reviewed literature illustrates a variety of methods for applying blockchain to enhance key aspects of forensic investigations, such as evidence integrity, chain of custody (CoC), access control, and traceability. Blockchain's inherent features—immutability, decentralization, and transparency—serve as a foundation for improving the reliability and credibility of forensic processes. We summarize how blockchain is being explored by researchers and the key benefits their works propose in the following points.

6.1.1. Blockchain-Driven Enhancements to Forensic Principles: Enhancing Evidence Integrity and Chain of Custody

A recurring focus across the studies is the application of blockchain to ensure the integrity of evidence and establish a tamper-proof chain of custody, critical for admissibility in court. Kahn et al. [89] and Rana et al. [92] use blockchain to secure CoC information by creating immutable records of evidence handling. Lone and Mir [98] propose the Forensic-Chain framework to maintain CoC through secure metadata and log storage on a permissioned blockchain. Similarly, Hu et al. [103] employ blockchain for lifecycle management of mobile forensic data, ensuring that evidence remains traceable and authentic. Yan et al. [95] integrate cryptographic protocols like CP-ABE and BLS signatures to enhance CoC in storage forensics, while Li, Lal et al. [97] extend blockchain's CoC capabilities to judicial investigations by automating role-based access control through smart contracts.

Additionally, Kumar et al. [8] employ hierarchical blockchain structures to improve transparency and traceability in IoT forensics, demonstrating blockchain's adaptability to various CoC scenarios and chronological tracking of evidence handling. Several studies also focus on ensuring evidence traceability and improving accessibility without compromising security. For example, Duy et al. [112] propose SDNLog-Foren, a log management system for network forensics that employs blockchain to preserve log integrity and enable fine-grained access control. Similarly, Pourvahab and Ekbatanifard [113] use Linear Homomorphic Signature (LHS) algorithms to authenticate devices and maintain transparent logs in SDN-IoT environments.

Verma et al. [118] address challenges in judicial investigations by proposing NyaYa, a blockchain-based electronic law record (ELR) management system that ensures traceability and transparency while automating case registration and metadata updates. In IoT forensics, Rani et al. [123] integrate blockchain with smart contracts to facilitate evidence sharing among stakeholders, addressing challenges in evidence access and collaboration.

6.1.2. Applications Across IoT, Cloud, and Emerging Domains

Blockchain's versatility has been explored in domains with complex and dynamic environments, such as IoT, cloud forensics, mobile ecosystems, and vehicular systems. Its application to address the unique challenges posed by these emerging fields, such as user privacy, cross-jurisdictional collaboration, and regulatory compliance, is highly represented in this review. For instance, Mahrous et al. [90] integrate fuzzy hashing with blockchain to enhance evidence detection and integrity in IoT systems. Similarly, Pourvahab and Ekbatanifard [94] and Ragu and Ramamoorthy [93] demonstrate blockchain's potential in cloud forensics, leveraging technologies like Software-Defined Networking (SDN) to address privacy leakage and provenance challenges. These frameworks highlight blockchain's capacity to ensure secure evidence collection, automated workflows, and reliable provenance tracking in highly distributed environments.

Emerging domains like mobile and IoT-vehicular forensics further highlight blockchain's adaptability. Hu et al. [103] present TFChain, a blockchain-based system for managing mobile forensic data, which automates evidence collection and ensures traceability through decentralized storage. In IoT-vehicular forensics, Billard and Bartolomei [99] propose a privacy-focused framework leveraging blockchain to pseudonymize GPS data while maintaining immutable navigation logs. Meanwhile, Philip and Saravanaguru [102] integrate blockchain with IPFS to manage evidence in Internet-of-Vehicles (IoV) investigations, ensuring secure collaboration among stakeholders like law enforcement and insurers. Similarly, Cebe et al. [66] address IoT-vehicular forensics by leveraging fragmented ledgers to manage data efficiently, balancing privacy and traceability. Lawrence and Shreelekshmi [120] extend blockchain's applicability to multimedia forensics where their video integrity framework prevents forgery and enhances traceability. Finally, financial crime forensics also benefit from blockchain's capabilities. Zarpala and Casino [117] propose a blockchain-based forensic model to manage evidence for embezzlement investigations, supporting secure evidence collection and cross-border collaboration.

6.1.3. Strengthening Storage Forensics

Blockchain's ability to secure and preserve digital evidence is particularly evident in storage forensics. Some studies demonstrate how blockchain is applied to tackle technical and legal challenges in the area, particularly in relation to tamper-proofing evidence and handling high data volumes. For example, Liu et al. [96] propose a blockchain model with multidimensional hashing to manage large volumes of evidence securely, as do Yan et al. [95], who incorporate cryptographic protocols such as CP-ABE and BLS signatures to balance evidence integrity and privacy in rest storage. In the same vein, Fu et al. [119] introduce BZK, a lightweight blockchain-based storage mechanism that optimizes digital evidence storage and verification by leveraging on-chain and off-chain storage solutions. Similarly, Tsai [105] enhances evidence storage and transfer processes with smart contracts, providing secure role-based access in judicial investigations.

6.1.4. Automating Forensic Processes

Blockchain's automation properties through smart contracts are frequently highlighted as a means of automating forensic processes, reducing reliance on manual intervention, and improving efficiency and trust. For example, Rane and Dixit's [92] BlockSLaaS framework leverages smart contracts to automate access control and logging processes in cloud forensic investigations. These smart contracts ensure that logs are recorded immutably and that only authorized users can retrieve them. This reduces the complexity of managing large-scale evidence logs and mitigates the risk of collusion among stakeholders by enforcing cryptographic access control mechanisms. In a similar vein, Philip and Saravanaguru [102]

integrate smart contracts with IPFS in a framework for the Internet of Vehicles (IoV). Smart contracts dynamically manage access control, enabling secure evidence sharing among law enforcement and other stakeholders.

Also, Yunianto et al. [111] present B-DEC, a blockchain-based Digital Evidence Cabinet system that uses smart contracts to automate chain-of-custody management. These smart contracts allow for evidence splitting, logging, and structured documentation, ensuring that each piece of evidence is securely stored and accessible only to authorized investigators. By minimizing human involvement in CoC processes, B-DEC enhances both efficiency and accuracy in evidence handling and CoC reporting. Finally, the LEChain proposed by Li, Lal et al. [97] explores the use of smart contracts in automating the juror voting process during court trials, providing a novel mechanism to enhance transparency and accountability in judicial proceedings.

Key Advantages of Blockchain Integration in Digital Forensics

The reviewed studies collectively demonstrate blockchain's ability to address critical challenges in digital forensics. We observed several efforts targeting both technical and legal requirements. Blockchain has been particularly effective in addressing technical requirements such as evidence integrity, traceability, and tamper resistance and even automating these requirements through enforcements with smart contracts. We also find that many technical solutions are designed to meet the legal requirements of the forensics process such as chain of custody, admissibility, and privacy concerns. This is perhaps because the legal challenges often necessitate the implementation of secure, transparent, traceable, and auditable systems for the purpose of ensuring admissibility in court. This is usually provisioned with cryptography, access control, and smart contracts, which are all key features of blockchain.

It is also notable that this research did not find any blockchain-based applications aimed at addressing the operational requirements of digital forensics. This domain, which includes the practical aspects of managing forensic investigations and teams, remains largely unexplored with blockchain technology, presenting a valuable area for future research.

To conclude, Blockchain's immutability ensures the authenticity of evidence, which is crucial for legal admissibility. The decentralized nature of blockchain minimizes reliance on centralized authorities, reducing the risk of evidence tampering or loss. Furthermore, its transparency fosters trust among stakeholders, while its traceability and automation capabilities streamline forensic processes, enabling faster and more efficient investigations.

6.2. RQ2: What Key Challenges or Limitations Do Current Blockchain-Based Forensic Solutions Face, and How Do They Vary Across Different Digital Forensics Domains?

Blockchain technology offers immense potential for digital forensics, yet this SLR finds several recurring challenges and limitations that researchers and practitioners must address to enable effective adoption in real-world scenarios. We have grouped these challenges, drawn from the reviewed blockchain approaches in 39 studies, into four groups, which reflect critical barriers to the widespread implementation of blockchain technology in the field of digital forensics. The reviewed studies also reveal that these challenges vary slightly across digital forensics domains. These slight variations are perhaps due to the unique characteristics of the domains. Table 6 highlights the challenges that blockchain-based forensic solutions currently faced by domain.

Table 6. Key challenges by domain.

Digital Forensics Domain	Key Challenges Identified	Primary Studies
IoT Forensics	Scalability issues due to high data volumes.	Mahrous et al. [90], Kumar et al. [8], Rani et al. [123]
	Computational overhead for cryptographic operations.	Tyagi et al. [108], Hu et al. [103], Xiao et al. [91]
	Integration challenges with IoT ecosystems.	Billard and Bartolomei [99], Philip and Saravanaguru [102]
	Interoperability and scalability in multi-purpose frameworks.	Ghaderi and Ghahyazi [121], Xiao et al. [91]
	Jurisdictional issues in cross-border systems.	Liang et al. [104], Rani et al. [123]
Cloud Forensics	Scalability constraints from managing large-scale logs.	Pourvahab and Ekbatanifard [94], Philip and Saravanaguru [102], Awuson-David et al. [107]
	High computational costs for managing logs.	Rane and Dixit [92], Duy et al. [112], Apirajitha and Devi [121]
	Integration issues in multi-stakeholder systems.	Rane and Dixit [92], Lusetti et al. [106], Awuson-David et al. [107]
	Interoperability and scalability in multi-purpose frameworks.	Apirajitha and Devi [121]
	Privacy and jurisdictional challenges in investigations.	Tsai [105], Liang et al. [104], Apirajitha and Devi [121]
Storage Forensics	Scalability issues with growing evidence volumes.	Liu et al. [96], Yan et al. [95], Verma et al. [118]
	Synchronization and metadata management issues.	Nyaletey et al. [115], Fu et al. [119], Rao et al. [109]
	Jurisdictional complexities in cross-border evidence sharing.	Rao et al. [109], Tsai [105], Zarpala and Casino [117]
	Challenges in handling large datasets and storage costs.	Rana et al. [2], Lone and Mir [98], Yunianto et al. [111]
Multimedia Forensics	Computational demands for processing large multimedia files.	Khan et al. [89], Lawrence and Shreelekshmi [120], Khan et al. [110]
	Coordination challenges in decentralized multimedia systems.	Khan et al. [110], Khan et al. [89]
	Scalability issues with high-resolution media storage.	Lawrence and Shreelekshmi [120], Khan et al. [110]
Network Forensics	Synchronization delays in distributed node management.	Duy et al. [112], Pourvahab and Ekbatanifard [113]
	Scalability issues with increasing log data.	Pourvahab and Ekbatanifard [113], Duy et al. [112]
	Integration barriers with network monitoring tools.	Duy et al. [112], Pourvahab and Ekbatanifard [113]
Mobile Forensics	Resource bottlenecks in managing evidence storage.	Hu et al. [103], Tyagi et al. [108]
	Privacy and traceability concerns.	Billard and Bartolomei [99], Hu et al. [103]
	Scalability limitations in large-scale mobile investigations.	Hu et al. [103], Tyagi et al. [108]

Despite the significant advancements highlighted in the reviewed studies, common limitations persist across blockchain-based forensic solutions. Scalability remains a critical issue, as blockchain systems struggle to handle the increasing storage and processing demands posed by large volumes of evidence data. Integration challenges with existing forensic workflows further complicate adoption, requiring significant technical and operational efforts to ensure seamless interoperability. Privacy concerns, particularly in the context of public or multi-stakeholder systems, demand robust mechanisms to safeguard sensitive information.

Additionally, legal and jurisdictional complexities are noteworthy issues especially in cross-border investigations where diverse legal frameworks and data-sharing protocols must be considered by the blockchain-based approach. These complexities highlight the need for standardized global frameworks and jurisdiction-specific adaptations to ensure blockchain's effective deployment. Moreover, many frameworks lack detailed implementation and performance evaluations, limiting their practical applicability in real-world scenarios.

In summary, these challenges vary slightly across forensic domains, with scalability and resource constraints being particularly pronounced in all forensics domains, while legal and jurisdictional issues predominantly affect cross-border investigations on data stored in distinct locations. Integration difficulties and evidence management challenges further highlight the complexity of adopting blockchain in existing forensic systems. Addressing these limitations will require ongoing research to develop scalable, interoperable, and legally compliant solutions, ensuring that blockchain technology can effectively enhance digital forensic investigations.

7. Open Issues and Future Research Direction

Despite the significant progress in integrating blockchain technology into digital forensics, the reviewed studies highlight several open issues that warrant further investigation. These open issues are distinct from the challenges currently faced by blockchain-based forensic solutions discussed in Section 6.2. They represent gaps in research and unexplored opportunities in applying blockchain technology to digital forensics.

7.1. Narrowed Focus of Existing Research

While it has been established by many studies that the existence of a trusted chain of custody can "make or break" a digital investigation, it is a bit concerning that most of the existing studies that explore the use of blockchain focus on provisioning a chain of custody with smart contracts in one way or the other. This begs the question that in what other ways can blockchain or smart contracts be used to solve other pertinent issues in digital forensics? When it comes to the problem of vast data in digital forensics, the heterogeneity of evidence coming from multiple evidence sources or organizations is one of the most prominent real-life challenges [8,30,125], but beyond exploring solutions to issues in the collection, preservation, and reporting phases such as transparency, security, and immutability alone, as most studies have, how can we extend current frameworks to tackle issues in the identification and examination phases. For example, in most solutions from our review, it could be difficult to identify the co-relationship between the incoming and existing evidence in a heterogeneous environment using a manual approach. Finding a way to automate the process of definitely categorizing incoming evidence as complementary or unrelated evidence in a particular case or scenario with smart contracts is crucial in enhancing blockchain as a comprehensive solution for digital investigations beyond the standard CoC issues that have been continually researched.

7.2. Lack of Studies in Malware Forensics

Cyber-attackers are becoming increasingly sophisticated in their creation of malware to avoid detection, obstruct meaningful analysis, and leave no traces behind. This is an important field because this analysis of the malware helps digital investigators provide reports that can be used by other stakeholders to combat the malware and potentially create anti-malware software that will automatically defend systems from similar malware in the future [60]. Despite this importance, Malware Forensics remains an underexplored domain in the context of blockchain technology as we could not find any approaches for this area. Given the evolving sophistication of malware and its increasing use in cyberattacks [126], there is a critical need for blockchain-based frameworks that enhance malware forensics by ensuring tamper-proof evidence management, traceability, and real-time collaboration for malware analysis or even exploration of smart contracts for automation of malware identification in the case of incident prevention. The absence of studies in this domain suggests a missed opportunity to address one of the most dynamic challenges in digital forensics.

7.3. Lack of Studies in Blockchain Forensics

Blockchain Forensics, which involves the analysis of blockchain data to identify evidence of unlawful activities, including fraud, money laundering, and cybercrimes, which are increasingly conducted via cryptocurrencies and decentralized platforms [12], remains another domain with little to no representation in the reviewed studies. Future research could explore how blockchain itself can serve as both the domain and the tool of forensic investigations; developing tools and frameworks that can analyze blockchain activities despite the pseudonymity of users to uncover patterns related to fraudulent or criminal behavior. Artificial intelligence could be useful in this area to identify and stop fraudulent activity in real-time using machine learning [127].

7.4. Neglect of Operational Requirements in Digital Forensics

The operational requirements of digital forensics as identified in Section 2, such as ensuring effective incident preparedness through policy enforcement, addressing training gaps of investigators and secure and efficient communication among stakeholders, remain largely unaddressed in the reviewed studies. Fulfilling these requirements will go a long way in the integration of forensic workflows into organizational and investigative processes. Future research should explore how blockchain can address some of these operational requirements, such as by automating incident response protocols or employing immutable ledgers to validate policy adherence by staff.

7.5. Ethical Implications of Blockchain in Digital Forensics

The use of blockchain in digital forensics raises important ethical concerns, such as the risk of privacy violations [66], the potential misuse of immutable records, and challenges in balancing transparency with confidentiality. Public blockchains, while offering transparency, can inadvertently expose sensitive information, including metadata or even pseudonym identities, which could compromise the privacy of individuals involved in forensic investigations [100]. Conversely, permissioned blockchains provide controlled access but may raise concerns about accountability and trust as restricted access could create opportunities for bias or manipulation by a few stakeholders. These issues are particularly critical in investigations involving vulnerable populations or sensitive legal proceedings where protecting privacy and maintaining trust are paramount.

Additionally, the immutability of blockchain records [97,98,109,111], while valuable for ensuring evidence integrity, introduces ethical dilemmas in cases of incorrect or malicious data entries. Immutable records cannot be altered or deleted, even when errors are

identified, potentially undermining the fairness of investigations or legal outcomes. This raises questions about how forensic systems should handle such scenarios and whether general mechanisms for ethical redaction or annotation of blockchain entries should be developed like [98] where they used new transactions to make unneeded evidence as "deleted" in the ledger. Moreover, the use of blockchain to automate forensic processes via smart contracts could inadvertently perpetuate biases or errors if the underlying algorithms are not carefully designed and validated. Future research should not only address these ethical concerns but also explore how blockchain-based forensic systems can integrate principles of fairness, accountability, and privacy by design to align with legal and societal expectations.

8. Limitations of Research

While this SLR aims to provide a comprehensive overview of blockchain applications in digital forensics, it is possible that a few distinct approaches or studies in this area were inadvertently omitted. The active nature of the field and the sheer volume of ongoing research may have contributed to gaps in the coverage, particularly in emerging or niche domains. Also, as we have conducted the review process manually (by the authors) without the use of automated tools, there is a slight possibility that interpretations or inferences made during data extraction and analysis may not fully align with the intentions of the cited studies. However, every effort was made to minimize such risks through multiple rigorous critical review by the authors and use of generative artificial intelligence for further validation of the findings only.

9. Conclusions

Blockchain technology has emerged as a transformative force in digital forensics, addressing challenges related to securing, analyzing, and preserving digital evidence. Its immutable and decentralized nature enhances transparency and trust, making it a valuable tool in strengthening forensic processes. This study systematically reviews the integration of blockchain into digital forensics, highlighting its applications, challenges, and future research directions. By analyzing 39 primary studies, this work maps blockchain's role across various forensic domains, particularly in IoT, cloud, and storage forensics, where it enhances data provenance, access control, and chain of custody management.

While blockchain has demonstrated its potential in forensic investigations, challenges such as scalability, computational overhead, integration barriers, and jurisdictional complexities remain significant hurdles to adoption. Additionally, gaps persist in its application to malware forensics, blockchain forensics, and the identification and examination phases of forensic investigations, signaling areas for future exploration. Moreover, scalability issues, computational overhead, integration challenges, and jurisdictional complexities remain key barriers to overcome for blockchain-based solutions in the field. This study also identifies open issues that extend beyond the challenges faced by existing solutions.

As part of our future work, we aim to investigate solutions for improving blockchain's role in the identification and examination phases of digital forensics, addressing the gaps identified in this study. As part of this, we plan to expand on blockchain applications beyond the chain of custody by exploring how blockchain and smart contracts can facilitate more advanced forensic processes, particularly in evidence categorization, correlation, and automation in heterogeneous forensic environments. Our next goal is to develop a framework and use-case scenario to prove this concept.

Supplementary Materials: The following supporting information can be downloaded at https://www.mdpi.com/article/10.3390/blockchains3010005/s1. Figure S1: Phases of review protocol (authors' elaboration).

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

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

References

1. Dasaklis, T.K.; Casino, F.; Patsakis, C. Sok: Blockchain solutions for forensics. In *Technology Development for Security Practitioners*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 21–40.
2. 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]
3. 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: Securing Patient Data*; Springer: Cham, Switherland, 2019; pp. 149–168.
4. Kumar, M. Applications of blockchain in digital forensics and forensics readiness. In *Blockchain for Cybersecurity and Privacy*; CRC Press: Boca Raton, FL, USA, 2020; pp. 339–364.
5. Sarmah, S.S. Understanding blockchain technology. *Comput. Sci. Eng.* **2018**, *8*, 23–29.
6. Hasselgren, A.; Kralevska, K.; Gligoroski, D.; Pedersen, S.A.; Faxvaag, A. Blockchain in healthcare and health sciences—A scoping review. *Int. J. Med. Inform.* **2020**, *134*, 104040. [CrossRef]
7. Du, M.; Chen, Q.; Xiao, J.; Yang, H.; Ma, X. Supply chain finance innovation using blockchain. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1045–1058. [CrossRef]
8. 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]
9. 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*, 301470. [CrossRef]
10. 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]
11. Batista, D.; Mangeth, A.L.; Frajhof, I.; Alves, P.H.; Nasser, R.; Robichez, G.; Silva, G.M.; Miranda, F.P.d. Exploring blockchain technology for chain of custody control in physical evidence: A systematic literature review. *J. Risk Financ. Manag.* **2023**, *16*, 360. [CrossRef]
12. 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. [CrossRef]
13. Årnes, A. *Digital Forensics*; John Wiley & Sons: Hoboken, NJ, USA, 2017.
14. Sachowski, J. *Implementing Digital Forensic Readiness: From Reactive to Proactive Process*; CRC Press: Boca Raton, FL, USA, 2019.
15. Cook, M.; Marnerides, A.; Johnson, C.; Pezaros, D. A survey on industrial control system digital forensics: Challenges, advances and future directions. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 1705–1747. [CrossRef]
16. Lee, H.C.; Palmbach, T.; Miller, M.T. *Henry Lee's Crime Scene Handbook*; Academic Press: Cambridge, MA, USA, 2001.
17. Carrier, B.; Spafford, E. An event-based digital forensic investigation framework. In Proceedings of the Digital Forensic Research Conference, Baltimore, MD, USA, 11–13 August 2004.
18. Cohen, F.B. *Digital Forensic Evidence Examination*; Asp Press Livermore: Livermore, CA, USA, 2010.
19. Martini, B.; Choo, K.-K.R. An integrated conceptual digital forensic framework for cloud computing. *Digit. Investig.* **2012**, *9*, 71–80. [CrossRef]
20. Kohn, M.D.; Eloff, M.M.; Eloff, J.H. Integrated digital forensic process model. *Comput. Secur.* **2013**, *38*, 103–115. [CrossRef]
21. Perumal, S.; Norwawi, N.M.; Raman, V. Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology. In Proceedings of the 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC), Sierre, Switzerland, 7–9 October 2015; pp. 19–23.
22. Prayudi, Y.; Riadi, I. Digital Forensics Workflow as A Mapping Model for People, Evidence, and Process in Digital Investigation. *Int. J. Cyber-Secur. Digit. Forensics* **2018**, *7*, 294–305.
23. Atlam, H.F.; Hemdan, E.E.-D.; Alenezi, A.; Alassafi, M.O.; Wills, G.B. Internet of things forensics: A review. *Internet Things* **2020**, *11*, 100220. [CrossRef]
24. Du, X.; Le-Khac, N.-A.; Scanlon, M. Evaluation of digital forensic process models with respect to digital forensics as a service. *arXiv* **2017**, arXiv:1708.01730.
25. Ajijola, A.; Zavarsky, P.; Ruhl, R. A review and comparative evaluation of forensics guidelines of NIST SP 800-101 Rev. 1: 2014 and ISO/IEC 27037: 2012. In Proceedings of the World Congress on Internet Security (WorldCIS-2014), London, UK, 8–10 December 2014; pp. 66–73.
26. Horsman, G. The COLLECTORS ranking scale for 'at-scene'digital device triage. *J. Forensic Sci.* **2021**, *66*, 179–189. [CrossRef] [PubMed]

27. Horsman, G.; Sunde, N. Unboxing the digital forensic investigation process. *Sci. Justice* **2022**, *62*, 171–180. [CrossRef] [PubMed]
28. Von Solms, S.; Louwrens, C.; Reekie, C.; Grobler, T. A control framework for digital forensics. In Proceedings of the Advances in Digital Forensics II: IFIP International Conference on Digital Forensics, National Center for Forensic Science, Orlando, FL, USA, 29 January–1 February 2006; pp. 343–355.
29. Saleem, S. Protecting the Integrity of Digital Evidence and Basic Human Rights During the Process of Digital Forensics. Ph.D. Thesis, Department of Computer and Systems Sciences, Stockholm University, Stockholm, Sweden, 2015.
30. 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]
31. Roussev, V. Hashing and data fingerprinting in digital forensics. *IEEE Secur. Priv.* **2009**, *7*, 49–55. [CrossRef]
32. 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.
33. Karie, N.M.; Venter, H.S. Taxonomy of challenges for digital forensics. *J. Forensic Sci.* **2015**, *60*, 885–893. [CrossRef] [PubMed]
34. Tiwari, A.; Mehrotra, V.; Goel, S.; Naman, K.; Maurya, S.; Agarwal, R. Developing trends and challenges of digital forensics. In Proceedings of the 2021 5th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 22–23 October 2021; pp. 1–5.
35. Casino, F.; Dasaklis, T.K.; Spathoulas, G.P.; Anagnostopoulos, M.; Ghosal, A.; Borocz, I.; Solanas, A.; Conti, M.; Patsakis, C. Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access* **2022**, *10*, 25464–25493. [CrossRef]
36. Ferrazzano, M.; Brighi, R. Digital Forensics: Best Practices and Perspective. In *Digital Forensic Evidence: Towards Common European Standards in Antifraud Administrative and Criminal Investigations*; Collezione di Giustizia Penale; Wolters Kluwer/CEDAM: Milano, Italy, 2021; pp. 13–48.
37. Al-Dhaqm, A.; Ikuesan, R.A.; Kebande, V.R.; Abd Razak, S.; Grispos, G.; Choo, K.-K.R.; Al-Rimy, B.A.S.; Alsewari, A.A. Digital forensics subdomains: The state of the art and future directions. *IEEE Access* **2021**, *9*, 152476–152502. [CrossRef]
38. Joseph, P.D.; Norman, J. An analysis of digital forensics in cyber security. In Proceedings of the First International Conference on Artificial Intelligence and Cognitive Computing: AICC 2018, Hyderabad, India, 2–4 February 2018; pp. 701–708.
39. Yaacoub, J.-P.A.; Noura, H.N.; Salman, O.; Chehab, A. Digital forensics vs. Anti-digital forensics: Techniques, limitations and recommendations. *arXiv* **2021**, arXiv:2103.17028.
40. Case, A.; Richard, G.G., III. Memory forensics: The path forward. *Digit. Investig.* **2017**, *20*, 23–33. [CrossRef]
41. Daghmehchi Firoozjaei, M.; Habibi Lashkari, A.; Ghorbani, A.A. Memory forensics tools: A comparative analysis. *J. Cyber Secur. Technol.* **2022**, *6*, 149–173. [CrossRef]
42. Ligh, M.H.; Case, A.; Levy, J.; Walters, A. *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory*; John Wiley & Sons: Hoboken, NJ, USA, 2014.
43. Malin, C.; Casey, E.; Aquilina, J. *Malware Forensics Field Guide for Windows Systems*; Syngress: Waltham, MA, USA, 2012.
44. Carrier, B. *File System Forensic Analysis*; Addison-Wesley: New York, NY, USA, 2005.
45. Al-Dhaqm, A.; Abd Razak, S.; Othman, S.H.; Ali, A.; Ghaleb, F.A.; Rosman, A.S.; Marni, N. Database forensic investigation process models: A review. *IEEE Access* **2020**, *8*, 48477–48490. [CrossRef]
46. Fowler, K. *Data Breach Preparation and Response: Breaches Are Certain, Impact Is Not*; Syngress: Rockland, MA, USA, 2016.
47. Sutherland, I.; Davies, G.; Pringle, N.; Blyth, A. The impact of hard disk firmware steganography on computer forensics. *J. Digit. Forensics Secur. Law* **2009**, *4*, 5. [CrossRef]
48. Pilli, E.S.; Joshi, R.C.; Niyogi, R. Network forensic frameworks: Survey and research challenges. *Digit. Investig.* **2010**, *7*, 14–27. [CrossRef]
49. Qureshi, S.; Tunio, S.; Akhtar, F.; Wajahat, A.; Nazir, A.; Ullah, F. Network Forensics: A Comprehensive Review of Tools and Techniques. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 887–889. [CrossRef]
50. Yaacoub, J.-P.A.; Noura, H.N.; Salman, O.; Chehab, A. Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations. *Internet Things* **2022**, *19*, 100544. [CrossRef]
51. Riadi, I.; Umar, R.; Firdonsyah, A. Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method. *Int. J. Comput. Sci. Inf. Secur. (IJCSIS)* **2017**, *15*, 3–8.
52. Brunty, J. Mobile device forensics: Threats, challenges, and future trends. In *Digital Forensics*; Elsevier: Amsterdam, The Netherlands, 2016; pp. 69–84.
53. Verdoliva, L. Media forensics and deepfakes: An overview. *IEEE J. Sel. Top. Signal Process.* **2020**, *14*, 910–932. [CrossRef]
54. Sencar, H.T.; Verdoliva, L.; Memon, N. *Multimedia Forensics*; Springer: Berlin/Heidelberg, Germany, 2022.
55. Bourouis, S.; Alroobaea, R.; Alharbi, A.M.; Andejany, M.; Rubaiee, S. Recent advances in digital multimedia tampering detection for forensics analysis. *Symmetry* **2020**, *12*, 1811. [CrossRef]

56. Janarthanan, T.; Bagheri, M.; Zargari, S. IoT forensics: An overview of the current issues and challenges. In *Digital Forensic Investigation of Internet of Things (IoT) Devices*; Springer: Cham, Switzerland, 2021; pp. 223–254.
57. Stoyanova, M.; Nikoloudakis, Y.; Panagiotakis, S.; Pallis, E.; Markakis, E.K. A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1191–1221. [CrossRef]
58. Manral, B.; Somani, G.; Choo, K.-K.R.; Conti, M.; Gaur, M.S. A systematic survey on cloud forensics challenges, solutions, and future directions. *ACM Comput. Surv. (CSUR)* **2019**, *52*, 1–38. [CrossRef]
59. Purnaye, P.; Kulkarni, V. A comprehensive study of cloud forensics. *Arch. Comput. Methods Eng.* **2022**, *29*, 33–46. [CrossRef]
60. Casey, E.; Malin, C.H.; Aquilina, J.M. *Malware Forensics: Investigating and Analyzing Malicious Code*; Syngress: Burlington, MA, USA, 2008.
61. Lohachab, A.; Garg, S.; Kang, B.; Amin, M.B.; Lee, J.; Chen, S.; Xu, X. Towards interconnected blockchains: A comprehensive review of the role of interoperability among disparate blockchains. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–39. [CrossRef]
62. Gupta, M. *Blockchain for Dummies (2nd IBM Li)*; Wiley: Hoboken, NJ, USA, 2018.
63. Wüst, K.; Gervais, A. Do you need a blockchain? In Proceedings of the 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, Switzerland, 20–22 June 2018; pp. 45–54.
64. Alqahtany, S.S.; Syed, T.A. ForensicTransMonitor: A Comprehensive Blockchain Approach to Reinvent Digital Forensics and Evidence Management. *Information* **2024**, *15*, 109. [CrossRef]
65. Ali, M.S.; Vecchio, M.; Putra, G.D.; Kanhere, S.S.; Antonelli, F. A decentralized peer-to-peer remote health monitoring system. *Sensors* **2020**, *20*, 1656. [CrossRef] [PubMed]
66. 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]
67. Kamal, R.; Hemdan, E.E.-D.; El-Fishway, N. A review study on blockchain-based IoT security and forensics. *Multimed. Tools Appl.* **2021**, *80*, 36183–36214. [CrossRef]
68. Ferdous, M.S.; Chowdhury, M.J.M.; Hoque, M.A. A survey of consensus algorithms in public blockchain systems for crypto-currencies. *J. Netw. Comput. Appl.* **2021**, *182*, 103035. [CrossRef]
69. Yao, W.; Ye, J.; Murimi, R.; Wang, G. A survey on consortium blockchain consensus mechanisms. *arXiv* **2021**, arXiv:2102.12058.
70. Le, T.-V.; Hsu, C.-L. A systematic literature review of blockchain technology: Security properties, applications and challenges. *J. Internet Technol.* **2021**, *22*, 789–802.
71. Habib, G.; Sharma, S.; Ibrahim, S.; Ahmad, I.; Qureshi, S.; Ishfaq, M. Blockchain technology: Benefits, challenges, applications, and integration of blockchain technology with cloud computing. *Future Internet* **2022**, *14*, 341. [CrossRef]
72. Mohanta, B.K.; Panda, S.S.; Jena, D. An overview of smart contract and use cases in blockchain technology. In Proceedings of the 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bangalore, India, 10–12 July 2018; pp. 1–4.
73. Schuhknecht, F. Talking blockchains: The perspective of a database researcher. In Proceedings of the 2021 IEEE 37th International Conference on Data Engineering Workshops (ICDEW), Chania, Greece, 19–22 April 2021; pp. 72–75.
74. Zhang, R.; Xue, R.; Liu, L. Security and privacy on blockchain. *ACM Comput. Surv. (CSUR)* **2019**, *52*, 1–34. [CrossRef]
75. Guo, H.; Yu, X. A survey on blockchain technology and its security. *Blockchain: Res. Appl.* **2022**, *3*, 100067. [CrossRef]
76. Zhao, Y.; Li, Y.; Mu, Q.; Yang, B.; Yu, Y. Secure pub-sub: Blockchain-based fair payment with reputation for reliable cyber physical systems. *IEEE Access* **2018**, *6*, 12295–12303. [CrossRef]
77. Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
78. Stephen, R.; Alex, A. A review on blockchain security. In *IOP Conference Series: Materials Science and Engineering*; IOP: Bristol, UK, 2018; p. 012030.
79. Khan, S.N.; Loukil, F.; Ghedira-Guegan, C.; Benkhelifa, E.; Bani-Hani, A. Blockchain smart contracts: Applications, challenges, and future trends. *Peer-Peer Netw. Appl.* **2021**, *14*, 2901–2925. [CrossRef] [PubMed]
80. Kassen, M. Blockchain and e-government innovation: Automation of public information processes. *Inf. Syst.* **2022**, *103*, 101862. [CrossRef]
81. Eggers, J.; Hein, A.; Weking, J.; Böhm, M.; Krcmar, H. Process automation on the blockchain: An exploratory case study on smart contracts. In Proceedings of the 54th Hawaii International Conference on System Sciences, Kauai, HI, USA, 5 January 2021.
82. Zhou, S.; Li, K.; Xiao, L.; Cai, J.; Liang, W.; Castiglione, A. A systematic review of consensus mechanisms in blockchain. *Mathematics* **2023**, *11*, 2248. [CrossRef]
83. Wei, Q.; Li, B.; Chang, W.; Jia, Z.; Shen, Z.; Shao, Z. A survey of blockchain data management systems. *ACM Trans. Embed. Comput. Syst. (TECS)* **2022**, *21*, 1–28. [CrossRef]
84. Zhu, C.; Li, J.; Zhong, Z.; Yue, C.; Zhang, M. A Survey on the Integration of Blockchains and Databases. *Data Sci. Eng.* **2023**, *8*, 196–219. [CrossRef]

85. Kang, P.; Yang, W.; Zheng, J. Blockchain private file storage-sharing method based on IPFS. *Sensors* **2022**, *22*, 5100. [CrossRef] [PubMed]
86. Khatal, S.; Rane, J.; Patel, D.; Patel, P.; Busnel, Y. Fileshare: A blockchain and ipfs framework for secure file sharing and data provenance. In *Advances in Machine Learning and Computational Intelligence: Proceedings of ICMLCI 2019*; Springer: Singapore, 2021; pp. 825–833.
87. Keele, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; EPSRC: Swindon, UK, 2007.
88. 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]
89. 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]
90. 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]
91. 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]
92. Rane, S.; Dixit, A. BlockSLaaS: Blockchain Assisted Secure Logging-as-a-Service for Cloud Forensics. In *Security and Privacy: Second ISEA International Conference, Proceedings of the ISEA-ISAP 2018, Jaipur, India, 9–11 January 2019*; Springer: Singapore, 2019; pp. 77–88.
93. Ragu, G.; Ramamoorthy, S. A blockchain-based cloud forensics architecture for privacy leakage prediction with cloud. *Healthc. Anal.* **2023**, *4*, 100220.
94. Pourvahab, M.; Ekbatanifard, G. Digital forensics architecture for evidence collection and provenance preservation in iaas cloud environment using sdn and blockchain technology. *IEEE Access* **2019**, *7*, 153349–153364. [CrossRef]
95. Yan, W.; Shen, J.; Cao, Z.; Dong, X. Blockchain based digital evidence chain of custody. In Proceedings of the 2020 2nd International Conference on Blockchain Technology, Hilo, HI, USA, 12–14 March 2020; pp. 19–23.
96. Liu, G.; He, J.; Xuan, X. A data preservation method based on blockchain and multidimensional hash for digital forensics. *Complexity* **2021**, *2021*, 5536326. [CrossRef]
97. 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]
98. Lone, A.H.; Mir, R.N. Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. *Digit. Investig.* **2019**, *28*, 44–55. [CrossRef]
99. Billard, D.; Bartolomei, B. Digital forensics and privacy-by-design: Example in a blockchain-based dynamic navigation system. In *Privacy Technologies and Policy: 7th Annual Privacy Forum, APF 2019, Rome, Italy, 13–14 June 2019, Proceedings 7*; Springer: Heidelberg, Germany, 2019; pp. 151–160.
100. Li, M.; Chen, Y.; Lal, C.; Conti, M.; Alazab, M.; Hu, D. Eunomia: Anonymous and secure vehicular digital forensics based on blockchain. *IEEE Trans. Dependable Secur. Comput.* **2021**, *20*, 225–241. [CrossRef]
101. Menard, T.; Abouyoussef, M. Towards Privacy-Preserving Vehicle Digital Forensics: A Blockchain Approach. In Proceedings of the 2024 12th International Symposium on Digital Forensics and Security (ISDFS), San Antonio, TX, USA, 29–30 April 2024; pp. 1–6.
102. Philip, A.O.; Saravanaguru, R.K. Smart contract based digital evidence management framework over blockchain for vehicle accident investigation in IoV era. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 4031–4046. [CrossRef]
103. Hu, S.; Zhang, S.; Fu, K. Tfchain: Blockchain-based trusted forensics scheme for mobile phone data whole process. In Proceedings of the 2022 IEEE 6th Information Technology and Mechatronics Engineering Conference (ITOEC), Chongqing, China, 4–6 March 2022; pp. 155–165.
104. Liang, G.; Xin, J.; Wang, Q.; Ni, X.; Guo, X. Research on IoT Forensics System Based on Blockchain Technology. *Secur. Commun. Netw.* **2022**, *2022*, 4490757. [CrossRef]
105. Tsai, F.-C. The application of blockchain of custody in criminal investigation process. *Procedia Comput. Sci.* **2021**, *192*, 2779–2788. [CrossRef]
106. 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]
107. 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]
108. Tyagi, R.; Sharma, S.; Mohan, S. Blockchain enabled intelligent digital forensics system for autonomous connected vehicles. In Proceedings of the 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT), Chennai, India, 10–11 March 2022; pp. 1–6.

109. Rao, S.; Fernandes, S.; Raorane, S.; Syed, S. A novel approach for digital evidence management using blockchain. In Proceedings of the International Conference on Recent Advances in Computational Techniques (IC-RACT), Raigad, India, 27–28 March 2020.
110. 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]
111. Yunianto, E.; Prayudi, Y.; Sugiantoro, B. B-DEC: Digital evidence cabinet based on blockchain for evidence management. *Int. J. Comput. Appl.* **2019**, *181*, 22–29. [CrossRef]
112. Duy, P.T.; Do Hoang, H.; Khanh, N.B.; Pham, V.-H. Sdnlog-foren: Ensuring the integrity and tamper resistance of log files for sdn forensics using blockchain. In Proceedings of the 2019 6th NAFOSTED Conference on Information and Computer Science (NICS), Hanoi, Vietnam, 12–13 December 2019; pp. 416–421.
113. Pourvahab, M.; Ekbatanifard, G. An efficient forensics architecture in software-defined networking-IoT using blockchain technology. *IEEE Access* **2019**, *7*, 99573–99588. [CrossRef]
114. Mothukuri, V.; Cheerla, S.S.; Parizi, R.M.; Zhang, Q.; Choo, K.-K.R. BlockHDFS: Blockchain-integrated Hadoop distributed file system for secure provenance traceability. *Blockchain Res. Appl.* **2021**, *2*, 100032. [CrossRef]
115. Nyaletey, E.; Parizi, R.M.; Zhang, Q.; Choo, K.-K.R. BlockIPFS-blockchain-enabled interplanetary file system for forensic and trusted data traceability. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 18–25.
116. Sakshi; Malik, A.; Sharma, A.K. Blockchain-based digital chain of custody multimedia evidence preservation framework for internet-of-things. *J. Inf. Secur. Appl.* **2023**, *77*, 103579. [CrossRef]
117. Zarpala, L.; Casino, F. A blockchain-based forensic model for financial crime investigation: The embezzlement scenario. *Digit. Financ.* **2021**, *3*, 301–332. [CrossRef]
118. 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]
119. Fu, X.; Ma, H.; Ding, B.; Wang, H.; Shi, P. Subtraction of Hyperledger Fabric: A blockchain-based lightweight storage mechanism for digital evidences. *J. Syst. Archit.* **2024**, *153*, 103182. [CrossRef]
120. Lawrence, L.; Shreelekshmi, R. Edwards curve digital signature algorithm for video integrity verification on blockchain framework. *Sci. Justice* **2024**, *64*, 367–376. [CrossRef]
121. Apirajitha, P.; Devi, R.R. A novel blockchain framework for digital forensics in cloud environment using multi-objective krill Herd Cuckoo search optimization algorithm. *Wirel. Pers. Commun.* **2023**, *132*, 1083–1098. [CrossRef]
122. Akhtar, M.S.; Feng, T. Using blockchain to ensure the integrity of digital forensic evidence in an iot environment. *EAI Endorsed Trans. Creat. Technol.* **2022**, *9*, e2. [CrossRef]
123. Rani, D.; Gill, N.S.; Gulia, P.; Yahya, M.; Ahanger, T.A.; Hassan, M.M.; Abdallah, F.B.; Shukla, P.K. A secure digital evidence preservation system for an iot-enabled smart environment using ipfs, blockchain, and smart contracts. *Peer–Peer Netw. Appl.* **2025**, *18*, 5. [CrossRef]
124. Ghaderi, M.R.; Ghahyazi, A.E. A Conceptual Blockchain-Based Framework for Secure Industrial IoT Remote Monitoring: Proof of Concept. *Wirel. Pers. Commun.* **2024**, *139*, 1071–1101. [CrossRef]
125. Brotsis, S.; Kolokotronis, N.; Limniotis, K.; Shiaeles, S.; Kavallieros, D.; Bellini, E.; Pavué, C. Blockchain solutions for forensic evidence preservation in IoT environments. In Proceedings of the 2019 IEEE Conference on Network Softwarization (NetSoft), Paris, France, 4–28 June 2019; pp. 110–114.
126. Ferdous, J.; Islam, R.; Mahboubi, A.; Islam, M.Z. A State-of-the-Art Review of Malware Attack Trends and Defense Mechanism. *IEEE Access* **2023**, *11*, 121118–121141. [CrossRef]
127. Rani, T.M.; Suresh, A.; Bhargavi, S.; Reddy, M.H.V.; Nikhil, K.S.; Priya, G.C. Enhancing Crypto Transaction Security: A Machine Learning Approach. In Proceedings of the 2024 10th International Conference on Electrical Energy Systems (ICEES), Chennai, India, 22–24 August 2024; pp. 1–7.