Journal of
Risk and Financial Management

MDPI

Systematic Review

Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review

Danielle Batista [1], Ana Lara Mangeth [2], Isabella Frajhof [2], Paulo Henrique Alves [2,*], Rafael Nasser [2], Gustavo Robichez [2], Gil Marcio Silva [3] and Fernando Pellon de Miranda [3]

[1] School of Information, Faculty of Arts, Vancouver, University of British Columbia (UBC), Vancouver, BC V6T 1Z1, Canada; malelo36@mail.ubc.ca
[2] ECOA Institute, Pontifical Catholic University of Rio de Janeiro (PUC-Rio), Rio de Janeiro 22451-900, Brazil; analara-mangeth@puc-rio.br (A.L.M.); isabellazfrajhof@puc-rio.br (I.F.); nasser@puc-rio.br (R.N.); robichez@puc-rio.br (G.R.)
[3] Petrobras, Rio de Janeiro 20031-912, Brazil; gilmarcio@petrobras.com.br (G.M.S.); fmiranda@petrobras.com.br (F.P.d.M.)
* Correspondence: ph.alves@puc-rio.br

Abstract: Blockchain technology, initially known for its applications in the financial industry, has emerged as a promising solution for various other domains. One prominent area for the use of blockchain-based solutions is forensics, specifically the chain of custody maintenance and control. While there have been numerous research projects exploring the use of blockchain technology in digital forensics, limited attention has been given to its application in controlling of the physical evidence chain of custody. In this research, we aim to explore the literature on the use of blockchain technology to solve problems related to the physical evidence chain of custody. Through a systematic literature review (SLR), we analyzed 26 resources discussing blockchain-based solutions for evidence chain of custody issues, based on requirements that could be applied to both physical and digital evidence. The results showed that there is a lack of studies involving the use of blockchain technology to solve problems related to the physical evidence chain of custody, and future research should focus on solving the issue.

Keywords: chain of custody; blockchain; smart contracts; physical evidence; forensics

Citation: Batista, Danielle, Ana Lara Mangeth, Isabella Frajhof, Paulo Henrique Alves, Rafael Nasser, Gustavo Robichez, Gil Marcio Silva, and Fernando Pellon de Miranda. 2023. Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review. *Journal of Risk and Financial Management* 16: 360. https://doi.org/10.3390/jrfm16080360

Academic Editor: Thanasis Stengos

Received: 9 June 2023
Revised: 14 July 2023
Accepted: 14 July 2023
Published: 2 August 2023

1. Introduction

Chain of custody in the forensics field is the procedure of properly handling evidence in an investigation process. It is an essential component of evidence collection and analysis, and it is critical for evidence to be accepted in judicial courts. The issues involving the chain of custody of material evidence are mainly related to the chain of custody integrity and accuracy, which are necessary to ensure that evidence cannot be refuted or rejected in court.

Blockchain is a disruptive technology, providing resources to solve problems not only in the financial industry but also in different fields, such as ESG (Environmental, Social, and Governance), voting, taxes, record keeping, identity management, and forensics (Alves et al. 2022; Miranda et al. 2023; Owens and Hodžić 2022; Robichez et al. 2021). As a result of its immutability and distribution characteristics, blockchain has the potential to solve problems of trust in different procedures. Blockchain technology can also reduce costs and increase efficiencies (Attaran and Gunasekaran 2019). In this study, we aimed to conduct a literature review focusing on examining research papers related to the chain of custody of evidence and the use of blockchain technology to support the chain of custody's trustworthiness. Our specific goal was to identify proposals that could be applied to the control and management of the chain of custody of physical evidence.

In this sense, this paper is a systematic literature review (SLR) that aims to provide an overview of how blockchain has been applied to preserve and control the chain of custody of evidence in forensic research. The objective was to identify the different approaches to solving chain of custody problems using the different blockchain platforms and their features. The study was conducted according to the description in Section 5 and fills the lack of systematic literature reviews of blockchain application to the chain of custody of evidence. More precisely, this study aimed to answer two Research Questions (RQs):

- (RQ1) How have blockchain and smart contracts been used in the chain of custody of physical evidence?
- (RQ2) What does blockchain offer to control the chain of custody of physical evidence?

The review was based on resources from four established scientific databases. A total of 72 resources were found in these databases, of which 26 resources were fully analyzed and provided evidence of the status of the research of blockchain-based solutions to solve problems related to the chain of custody of physical evidence and of how the current literature relates to the concept of physical evidence. The final selected resources (37%) sufficiently represented a diverse range of perspectives and findings, enabling this article to draw relevant conclusions and to contribute to the existing knowledge on the topic.

The other sections of this paper are organized as follows. Section 2 provides the main concepts discussed in this paper, and Section 3 highlights current literature reviews focusing on the use of blockchain in the forensic field. Section 4 explains the research methodology. Section 5 provides the results, and Section 6 the discussion. Finally, Section 7 presents the limitations and proposed future research and Section 8 concludes the paper.

2. Background

Blockchain technology has emerged as a disruptive innovation, providing a decentralized and transparent environment across various domains. Blockchain can be understood as a distributed ledger technology that enables secure and immutable record-keeping of digital transactions. It comprises a chain of blocks, each containing a list of validated and time-stamped transactions. An interesting feature of blockchain is its decentralized nature, where multiple participants, or nodes, maintain copies of the ledger. This distributed consensus mechanism ensures that no single entity has control over the entire network, making it resistant to tampering and censorship. Thus, blockchain is ripe for contexts involving multiple parties with a need for a reliable and trustworthy ambiance in the registering of sensitive information, since it can "allow for an audit trail of all operations carried out between peers without the need for a centralized authority" (Grima et al. 2021).

Blockchains can be classified as public, private/permissioned, or hybrid. Public blockchain allows any interested party to be a node in the network and to participate in the consensus. Registered data can be viewed by members or non-members. In its turn, private or permissioned blockchains only allow the participation of authorized members, limiting data access to such participants. Lastly, hybrid blockchains embed characteristics of both public and private blockchains.

The key features of blockchain include transparency, immutability, security, and decentralization of recorded data in the ledger data. In public blockchains, transparency is achieved by its public nature, allowing members and non-members to view and verify transactions. In private or permissioned blockchains, data availability is limited to participants of the network; hence, transparency is restricted to such members. Immutability ensures that once a transaction is recorded on the blockchain, it cannot be altered retroactively. Security is enforced through advanced cryptographic algorithms, ensuring the integrity and confidentiality of data. Moreover, decentralization eliminates the need for intermediaries, reducing costs and enhancing trust among participants.

Due to its disruptive characteristics, blockchain technology has had positive effects in diverse sectors, establishing the foundation for a new economy (Grima et al. 2021). This technology has brought significant advancements to various domains, including supply chain management (Kramer et al. 2021), since blockchain provides transparent and secure

information sharing. This, in turn, enhances trust among consumers and stakeholders (Kramer et al. 2021). Likewise, the field of digital forensics stands to benefit greatly from the implementation of blockchain technology. In particular, the application of blockchain in the context of chain of custody has garnered substantial attention. This is due to its potential to address the challenges associated with the management and preservation of digital evidence.

Chain of custody refers to the chronological documentation and accountability of the custody, control, transfer, analysis, and disposition of assets or evidence (Chopade et al. 2019). It plays a crucial role in legal, forensic, and regulatory contexts, since it ensures the integrity and admissibility of evidence in court proceedings.

The chain of custody establishes a clear and auditable trail. It demonstrates uninterrupted custody and handling of assets from their origin to their final destination. Maintaining an accurate chain of custody is essential to prevent unauthorized access, tampering, or loss of assets and the respective evidence. It involves documenting relevant information, such as date, time, location, individuals involved, and any changes in custody. To achieve such a purpose, chain of custody protocols typically require strict adherence to standard operating procedures, with a focus on maintaining the integrity and authenticity of the assets throughout their life cycles.

Therefore, chain of custody plays a crucial role in managing and validating evidence in digital forensics investigations. It ensures the collection, tracking, and protection of evidence from the point of collection to its utilization in a court of law (Bonomi et al. 2018). While chain of custody is not mandatory in forensic analysis, it is extensively employed to establish the integrity of evidence and ensure its admissibility in legal proceedings. A robust chain of custody process should adhere to certain requirements, including integrity, traceability, authentication, verifiability, and security against tampering (Bonomi et al. 2018).

Digital evidence is inherently fragile and susceptible to unexpected alterations. This can compromise its reliability and admissibility in legal proceedings. Traditional chains of custody primarily operated through paper-based systems, often involving physical handovers of evidence. In this process, documentation is filled out and signed at each step, relying on physical signatures and documented delivery routes to ensure the authenticity and traceability of evidence. However, this conventional approach is insufficient to guarantee the provenance and integrity of digital evidence, given its volatile nature and the speed of digital transactions (Tsai 2021).

To overcome these limitations, researchers have explored the potential of blockchain technology to enhance the chain of custody in digital forensics investigations (Chopade et al. 2019; Tsai 2021). As mentioned before, blockchain exhibits essential features, such as decentralization, integrity, traceability, and consistency, which align with the requirements of traditional chain of custody (Tsai 2021). By leveraging these features, blockchain-based solutions offer a promising framework for the efficient delivery and preservation of digital evidence.

The use of blockchain technology in the chain of custody process presents several potential advantages. It holds great promise for improving the management and preservation of digital evidence, especially in forensic investigations. By leveraging the features of blockchain, such as immutability and transparency, it becomes possible to create an unalterable and auditable record of custody transfers. Each custody transfer can be securely recorded as a transaction on the blockchain, ensuring a tamper-resistant and trustworthy chain of custody.

Furthermore, the decentralized nature of blockchain eliminates the reliance on a single central authority in the maintenance of custody records. In this sense, data availability eliminates friction between parties, allowing parties to directly access datab. Multiple nodes participate in verifying and validating transactions, reducing the risk of fraud or manipulation. This decentralized consensus mechanism enhances the reliability and trustworthiness of the chain of custody.

It is worth mentioning that, due to its trustworthiness, blockchain technology has been widely used for information tracking purposes, both in the public sector (state police

systems, for example (Hingorani et al. 2020)) and private sector, serving several different industries (including healthcare (Hölbl et al. 2018) and agriculture Demestichas et al. (2020)). Thus, as blockchain technology continues to evolve, it is expected to also play a crucial role in ensuring the credibility, admissibility and reliability of digital evidence in legal proceedings.

Nevertheless, as is evident throughout this work, the implementation of blockchain technologies in the chain of custody context presents the following challenges: (i) the need to ensure the reliability of data registration carried out before the insertion of the data in the blockchain, as well as an acknowledgment of its previous immutability, (ii) the complexity of mapping a chain of custody process and identifying the most appropriate and useful way of applying blockchain technology to it, (iii) the under-explored nature of the field of research into blockchain technologies and smart contracts applied to the chain of custody context, which leaves a gap to be filled, often experimentally, and (iv) the hardship in defining a robust framework that would be able to respond to the various necessary requirements, as well as the hardship in designing the functional architecture.

3. Related Work

This SLR, unlike any other in the existing literature, set out to explore the extensive realm of blockchain and smart contracts as powerful solutions to the problem of ensuring an impeccable chain of custody of material evidence. While previous systematic reviews have touched upon the integration of blockchain and smart contracts in the forensics domain, they primarily centered around the chain of custody of evidence and emerging challenges, particularly in the realm of digital forensics, notably pertaining to IoT forensics. However, to the best of our knowledge, no previous research has delved into the depths of the specifics of using blockchain to solve problems related to the material evidence chain of custody with the precision and thoroughness demonstrated by this pioneering research.

In a systematic literature review, Akinbi et al. (2022) reported some of the most recent blockchain-based forensic investigation models for IoT evidence collection. The authors aimed to analyze how blockchain was being used to improve the forensic investigation process using IoT, and to evaluate how efficient the models appeared to be. The study focused on models and frameworks proposing the use of blockchain to secure the evidence chain of custody and preserve privacy, integrity, and maintenance of collected evidence. The resources analyzed focused on securing the evidence chain of custody, followed by data integrity, data provenance, privacy, and identity anonymity, respectively. However, the authors observed a limitation in the applicability of the study in a different context of digital evidence and IoT forensics. Moreover, the findings of this study revealed that Ethereum emerged as the most widely utilized in forensic investigations involving the application of IoT, followed by tailor-made distributed ledgers and Hyperledger.

Finally, the paper provided evidence that most of the blockchain-based IoT frameworks analyzed in the systematic literature review proposed a proof-of-concept application of blockchain. The goal of using a proof-of-concept was to ensure the chain of custody maintenance, integrity, and provenance of IoT forensic data. The authors also observed that the proposed frameworks did not change the established forensic investigation process. Nevertheless, blockchain technology was used as a tool to ensure the tamper-resistance, immutability, and security of evidence collected from IoT devices.

Akinbi et al. (2022), when investigating their research questions, concluded that the latest blockchain-based IoT forensic investigation process models prioritized the use of permissioned and private blockchains. The main motivation for this choice is the fact that public and permissionless blockchains lack privacy and anonymity features, which are important characteristics in tools developed to support a forensic investigation. Most of the studies analyzed by Akinbi et al. (2022) focused on the use of blockchain to improve the IoT forensic investigation process by refining the overall integrity of the chain of custody process, as well as the data integrity, provenance control, privacy and anonymization. They noted that the performance evaluations of proposals "vary significantly and are measured

in similar ways including the cost, privacy, and security benefit of their implementation" (p. 7). Through the performance analysis, the author concluded that "the overall performance of each proposed blockchain-based IoT forensics investigation process model could impact the choice of selection for IoT investigations. Each model has its performance characteristics under various conditions, and one way outperforms the other in terms of a specific performance metric" (p. 8).

A systematic review was conducted by Khanji et al. (2022), focusing on the readiness of blockchain in the IoT forensic investigation. The authors evaluated frameworks in the literature, which used blockchain to mitigate some of the IoT challenges, in comparison to the current IoT investigation process. Khanji et al. (2022) used the categorization proposed by Zawoad and Hasan (2015) to categorize the IoT forensics challenges. The categories were the following: device forensics, network forensics, and cloud forensics. The challenges were highlighted as follows:

- Device level: the collection of evidence by the local memory of the IoT device. Challenges: evidence varies from the traditional digital evidence; complex computing architecture; data is produced in vendor-specific format; use of proprietary storage mechanisms; limited storage on the physical device, limiting the amount of digital traces and increasing the possibility of data loss; and difficult chain of custody maintenance.
- Network level: the study of IoT device communication and which communication protocols are used. Challenges: increased amount of encrypted network traffic; use of different protocols that require additional tools, software, and expertise.
- Cloud level: the collection of additional relevant data from the cloud services associated with the IoT devices under investigation. Challenges: cross-border jurisdiction; time-consuming evidence collection; diverse data format; and data spread over different layers.

Khanji et al. (2022) divided their analysis between a review of studies in IoT forensics and a review of blockchain-based frameworks in IoT forensics. This division aimed to compare the blockchain-based proposals and how the proposals addressed the highlighted challenges in the research. The authors categorized blockchain readiness to be used with IoT forensics into the following categories: data integrity, distributed storage, legality and regulations, management, transparency, authenticity, and security. They concluded that the resources analyzed in their systematic review provided evidence of blockchain integration readiness. However, the authors emphasized that blockchain is an emergent technology. As a consequence, it increases the complexity and costs involved in integrating this technology into digital forensics legacy systems. According to the authors, security issues regarding permissionless blockchain must also be considered in digital forensics use cases.

Two other papers (Ariffin and Ahmad 2021; Stoyanova et al. 2020) were partially considered in this analysis, even though they were not systematic reviews investigating the use of blockchain to solve problems related to the chain of custody. Stoyanova et al. (2020) conducted a survey on IoT forensics, which examines the state-of-the-art of digital forensics approaches to solve problems related to IoT systems from a forensics perspective. Part of their analysis focused on blockchain applications for IoT forensics. The findings showed that blockchain's features, such as immutability and distribution, suit the demands of IoT forensics through the use of the timestamp as a means of maintaining the integrity of the digital evidence. Other works analyzed in the paper proposed evidence of storage distribution eliminating single points of failure, the use of blockchain to secure the chain of custody of digital evidence and to track changes made to IoT devices, and the use of a public digital ledger to find facts in criminal incidents in IoT-based systems.

Ariffin and Ahmad (2021) identified the indicators for the maturity and readiness of digital forensics organizations in the era of industrial revolution 4.0, through a systematic literature review. Although this study involved the application of other technologies besides blockchain over digital forensics procedures, there was a specific analysis involving the advantages and limitations of using blockchain in the forensics field. The authors

highlighted that public blockchains do not ensure privacy, and might not be adequate for digital forensics procedures.

Therefore, as evidenced in this section, there is a lack in the literature of a systematic review that approaches the use of blockchain technology to address the challenges of preserving the trustworthiness of the chain of custody of physical evidence.

4. Methodology

The present SLR aimed to research the literature in light of RQ1, concerning how blockchain and smart contracts have been used in the chain of custody of physical evidence, and of RQ2, concerning what the technologies offer to the control of the chain of custody of physical evidence. In order to answer the research questions, extensive research was conducted to discover if, and how, blockchain-based tools offer a solution to the problem of maintaining the evidence chain of custody. To achieve this goal, the research was conducted on four established scientific databases: Scopus, IEEE Explore Digital Library, ACM Digital Library, and Elsevier Science Direct. The search strings used were blockchain AND "chain of custody", smart contract AND "chain of custody", and DLT AND "chain of custody", both in the title and the abstract. The research encompassed works published between 2013 and 2022.

The exclusion criteria of the results were grey literature, newspaper articles, and review articles. However, review articles were considered for the related work section, but not for the SLR, since such work usually does not propose a specific solution. Thus, they were out of the scope of this research. In turn, the resources considered in this SLR included book chapters, conference papers, and journal articles published in the past ten years. The criteria for selecting which literature was to be included in the review was the presentation of blockchain-based solutions to solve problems in the chain of custody of evidence. In a more specific scope, papers were selected based on their presentation of discussions and propositions for solutions addressing challenges related to both material and digital evidence. Additionally, the inclusion criteria considered the relevance and applicability of the features for digital evidence in addressing physical evidence chain of custody problems.

The first stage of research resulted in 71 references. During the study selection we identified 26 duplicated studies, which reduced the total references to 44. The second stage of selection involved reading the abstracts and analyzing the relevance of the work according to the proposed research questions. During this stage, 15 studies were rejected. Three of the 15 studies were not accessible through the accounts the authors held. One of the works (Prieto et al. 2022) comprised a summary of conference proceedings exploring blockchain and its applications. Two papers were rejected because they presented solutions focusing on aspects that would exclusively solve problems related to digital evidence. In both papers, the proposed solution could not be applied to physical evidence, such as the solutions suggested by Ali et al. (2022) and Awuson-David et al. (2021). The first focused only on digital evidence integrity, and the second focused on the maintenance of systems logs.

Among the 15 works rejected, seven references discussed the use of blockchain technology to solve problems related to the chain of custody in contexts other than forensics. Most of the works rejected at this stage focused on the use of blockchain for supply chain provenance issues, such as the works presented by Parkin and Prescott (2017), Ahmadi-Assalemi et al. (2019), Bager et al. (2022), and Mugurusi and Ahishakiye (2022).

Mugurusi and Ahishakiye (2022) focused on issues regarding the supply chain of cobalt and how blockchain can be used to preserve the chain of custody of the mineral as a means to guarantee the mineral's provenance and responsible commerce. Parkin and Prescott (2017) discussed "how different DLT platforms are being commercially used to build trust, data consistency and persistence through the chain of custody for materials as they transform along the supply chain from source to end-use" (p. 7) using two specific supply chain use cases to illustrate the discussion. Bager et al. (2022) focused on the use

of blockchain to control the coffee supply chain and solve some of the problems related to provenance information and sustainability assurance. Finally, Ahmadi-Assalemi et al. (2019) focused on the use of blockchain for network traffic control and threat detection in environments with diverse IoT devices. In this context, Lourinho et al. (2021) also proposed the use of blockchain to protect the privacy and identity of whistleblowers.

Furthermore, other works were rejected during the review stage. One of them focused on using blockchain to support the command chain and on controlling decision-making (Blowers et al. 2019), and the other used blockchain to control access to genetic data in the chain of custody (Zarchi et al. 2022). Two other papers consisted of systematic reviews regarding the use of blockchain in chain of custody solutions (Jahankhani et al. 2021), and the application of resources of Industrial Revolution 4.0 to the chain of custody (Ariffin and Ahmad 2021). Both papers are better explored in Section 2. At the end of the second stage, 29 papers were selected to be part of this SLR and were further analyzed in-depth according to our RQs.

In this sense, the described steps of the analysis, regarded as the quality assessment, were based on the following questions:

- Does this work mention which blockchain platform was used?
- Does this work use smart contracts as part of the solution?
- Does this work describe the motivation for using blockchain as a technological solution?
- Does this work describe the motivation for using the specific blockchain platform?
- Is the blockchain platform still in use?
- Does this work propose a framework for a blockchain-based solution for the chain of custody context?
- Does this work use a(n) standard/established chain of custody framework for the solution?
- Does the solution proposed in this work apply to the material evidence use cases?
- Are the components of the solution specified in this work?
- Does this work present an illustration of the solution?

These questions were considered relevant for the study analysis and the research questions guiding this research because they supported quality analysis of the resources and led to answers to the two research questions, RQ1 and RQ2. Resources that mentioned the blockchain platform used, presented the use of smart contracts as part of the solution, and proposed a framework for the blockchain-based solution would provide the support to answer RQ1, pertaining to how blockchain and smart contracts have been used in the chain of custody of physical evidence. Papers describing the motivation for using blockchain, the use of specific blockchain platforms, and the resources using an established chain of custody framework, would inform the answer to RQ2, pertaining to what blockchain technology offers to the control of the chain of custody of physical evidence. We considered it relevant to know the motivations for using blockchain and smart contracts, the platform applied for the blockchain solution proposed, and whether the platform was still in use, and how the solution was designed and proposed to solve issues related to the chain of custody. To each of these questions, there were three possible answers with the following grading: (1) yes, 1 point, (2) partially, 0.5 of a point; and (3) no, 0 points. Table 1 shows the grading of the 29 papers analyzed.

Table 1. Papers' Score.

Paper	Grade	Year
(Alruwaili 2021)	9.5	2021
(Gupta and Mishra 2021)	9	2021
(Li et al. 2021)	9	2021
(Olukoya 2021)	9	2021
(Sathyaprakasan et al. 2021)	9	2021

Table 1. *Cont.*

Paper	Grade	Year
(Bonomi et al. 2018)	9	2020
(Douladiris et al. 2020)	9	2020
(Chopade et al. 2019)	9	2019
(Chandramouli et al. 2022)	8.5	2022
(Wang et al. 2022)	8.5	2022
(Khan et al. 2021)	8.5	2021
(Kumar et al. 2021)	8.5	2021
(Liu et al. 2021)	8.5	2021
(Tsai 2021)	8.5	2021
(Elgohary et al. 2022)	8	2022
(Jung and Tsai 2020)	8	2020
(Lone and Mir 2019)	8	2019
(Malamas et al. 2019)	7.5	2019
(Pourvahab and Ekbatanifard 2019)	7	2019
(Ahmad et al. 2020)	6.5	2020
(Burri et al. 2020)	6.5	2020
(Silva and Garcia 2021)	5.5	2021
(Yan et al. 2020)	5	2020
(Al-Khateeb et al. 2019)	4.5	2019
(Zhang et al. 2017)	4.5	2017
(Jaquet-Chiffelle et al. 2020)	3	2020
(Calvão and Archer 2021)	0	2021

After the quality assessment, 28 references remained, to be extracted at the data extraction stage. Paper (Calvão and Archer 2021) was excluded during this stage due to the absence of a concrete solution, despite discussing intriguing aspects of utilizing blockchain for the chain of custody of the mineral supply chain. Once the papers were separated and analyzed, the following data were extracted from each work: the blockchain model, the blockchain platform, the chain of custody requirements, the jurisdiction, types of publication, year of publication, reference standards, and proposed solution. The data extraction is structured in Table 2.

Table 2. Data Extraction Properties.

Description	Values
Blockchain model	Hybrid Private Public
Blockchain platform	Besu Bitcoin Corda Ethereum Hyperledger Hyperledger Fabric Other Quorum Solana

Table 2. *Cont.*

Description	Values
Chain of custody requirement	Access control Auditability Authenticity/ Integrity Data/ evidence provenance Immutability Privacy/ Confidentiality Process automation Recordkeeping Security Storage Transparency
Jurisdiction	Asia EU Latin America Middle East N/A North America
Type of publication	Book chapter Conference paper Journal article Workshop
Year	Number
Reference Standard	Framework International standard Ontology Requirements
Proposed Solution	Architecture Framework Model Prototype System

The results were refined to a final total of 26 references. The refining process is represented in Figure 1. The final references were divided into two book chapters, eight conference papers, and 17 journal articles. After analyzing all the references, the data was refined to present the research findings discussed in Section 5.

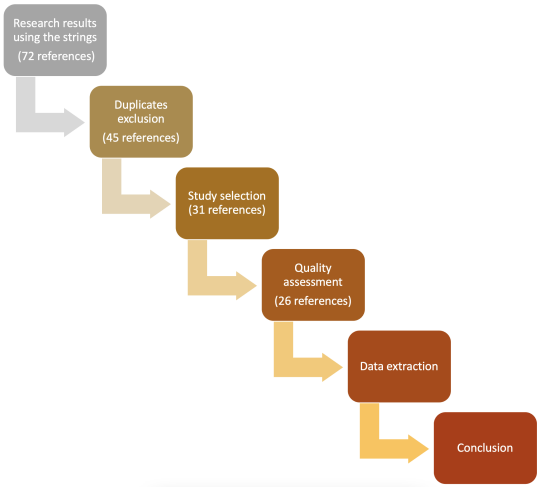

Figure 1. Methodology Model.

5. Results

The growth of published papers on the subject of blockchain and chain of custody is testament to an increased interest in this field of study. In 2017, only one paper that fit our criteria was published, indicating a relatively low level of research output for that year. Similarly, in 2018, the number of publications remained low, with only one paper.

In subsequent years, a significant interest in the subject of this SLR was observed, reflected in a relevant increase in publications. In 2019, the publication quantity reached four papers, marking a notable rise compared to the previous years. The upward trend continued in 2020, with a further increase of six papers, reflecting continued growth in the research output.

In 2021, there was a remarkable surge in publication activity, resulting in the release of ten new published papers. This notable spike suggests a substantial boost in research productivity during that period. However, it should be noted that three of the papers were marked as N/A in our analysis. This possibly indicates potential missing data or unreported publications. In 2022, the publication quantity decreased to two papers, showcasing a decline in research output compared to the previous year. Figure 2 shows the evolution of publications.

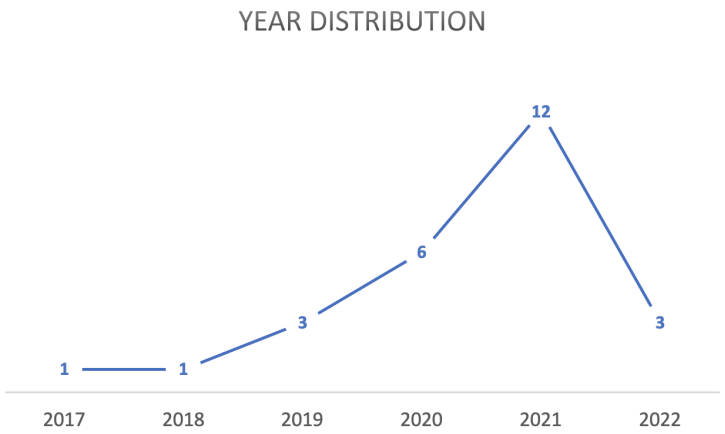

Figure 2. Year Distribution.

Among the 26 papers analyzed, three were under the jurisdiction of the European Union, indicating a European legal context (Al-Khateeb et al. 2019; Bonomi et al. 2018; Chandramouli et al. 2022). One paper was associated with the jurisdiction of North America, suggesting its grounding within the legal systems of the United States of America and Canada (Al-Khateeb et al. 2019). Similarly, one paper referred to the jurisdiction of Latin America, indicating its connection to legal frameworks within countries of this region (Silva and Garcia 2021). The majority of the analyzed papers, which constituted a significant proportion of the sample, were classified as N/A, due to their lack of explicit jurisdictional alignment.

Among the 26 papers reviewed, a significant majority (23 papers) acknowledged the utilization of blockchain platforms as a solution for chain of custody and evidence registration. As depicted in Figure 3, out of the total papers mentioning blockchain systems, 13 specifically referred to the utilization of public blockchains, whereas 10 papers mentioned the use of private blockchain systems. Additionally, four papers did not provide enough information to classify the type of blockchain employed.

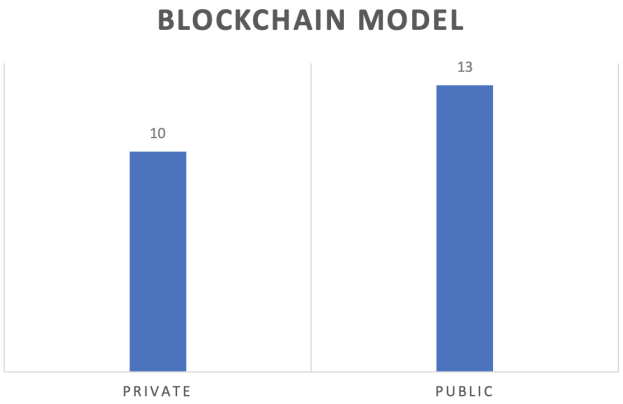

Figure 3. Blockchain Model

Regarding the identification of the blockchain platforms adopted in the 23 papers, it was found that 21 papers explicitly named the platform used. Specifically, 10 papers mentioned the employment of Hyperledger Fabric, 9 papers mentioned Ethereum, one paper mentioned Bitcoin and one paper mentioned the utilization of a non-identified blockchain platform, as depicted in Figure 4.

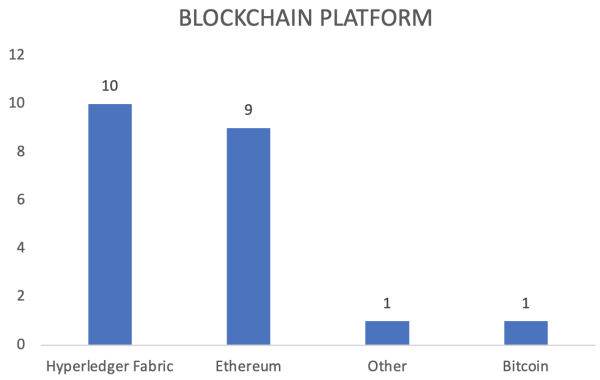

Figure 4. Blockchain Platforms.

As mentioned before, this work established key requirements in the selection of papers associated with the integration of blockchain technology and chain of custody. Within the selected papers, the most frequently mentioned requirement was "Data Provenance", which was identified in 18 out of the 26 papers, as depicted in Figure 5.

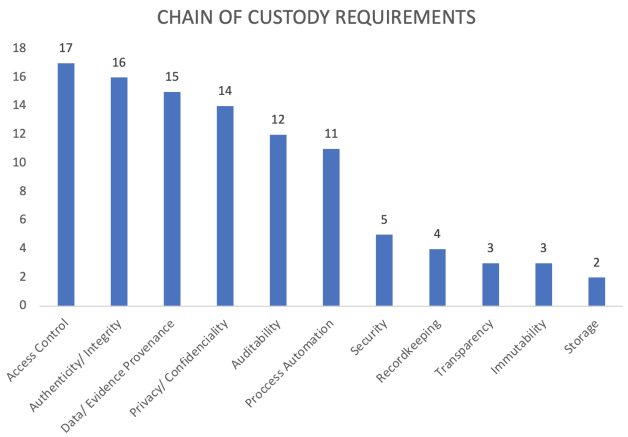

Figure 5. Chain of Custody Requirements.

The second most commonly mentioned requirement was "Access Control", identified in 16 papers. "Authenticity/Integrity" emerged as the third most frequently mentioned requirement, appearing in 14 papers. The requirement of "Auditability" was identified in 11 papers. "Privacy/Confidentiality" was mentioned in 10 papers. "Process Automation" was mentioned in 9 papers. Other requirements, such as "Immutability," "Security," and "Transparency," were mentioned in 4 papers each. Lastly, "Recordkeeping" was mentioned in only 3 papers. The review identified three mentions of both "Framework" and "International Standard", while the standard of "Requirements" was mentioned twice.

Among the analyzed papers, 13 focused solely on proposing models using blockchain to record evidence in the chain of custody process. In contrast, 17 papers proposed blockchain frameworks, while 9 papers focused on designing the architecture of blockchain systems. Finally, as depicted in Figure 6, only 10 papers overcame the design phase and presented prototypes of blockchain-based chain of custody and evidence recording systems.

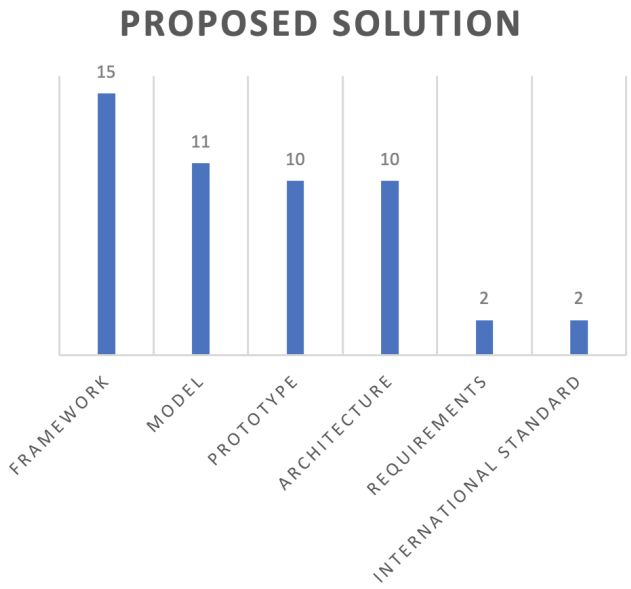

Figure 6. Proposed Solutions.

6. Discussion

In this section, we present a detailed analysis of the selected papers from the process of data extraction. Initially, it is worth noting that the use of blockchain-based smart contracts was in its nascent stage in 2017 and 2018 (Buterin 2014). During this time, the correlation between this subject and the chain of custody was not extensively discussed. This resulted in a limited number of academic publications, with only one paper published in 2017 and one in 2018.

However, in subsequent years, there was a significant increase in research productivity, with more materials being produced in both industry and academia. In 2019, the publication quantity reached four papers, marking a notable rise compared to the previous years. This upward trend continued in 2020, with a further increase to six papers, reflecting continued growth in research interest. The increase in research might have been due to the maturity of Ethereum smart contracts (Chen et al. 2020).

In 2021, there was a significant surge in publication activity, with a total of ten papers published. This spike suggests a substantial boost in research productivity during that period. A possible explanation for this increase may have been the pandemic context and the enforced social distancing. This may have contributed to high academic performance. Furthermore, many conferences exempted costs related to submission, attendance and presentation, which may have motivated publications. Another possible reason for the publication peak might be the bitcoin 'all-time high' during 2021[1]. However, it should be

noted that three articles were marked as N/A in our analysis, indicating potential missing data or unreported publications. In 2022, there was a decrease in the publication quantity, resulting in only two new papers, showcasing a decline in research results compared to the previous year.

Jurisdiction is an important concept to consider in the development of evidence chain of custody solutions, given that the chain of custody process is significantly related to the jurisdictional context. However, it is possible to assume that the jurisdictional feature was not considered relevant information by the authors, as the majority of the analyzed papers did not identify the jurisdictional context. The jurisdictional authority was identified in only five papers. Three of them stated that they were under the jurisdiction of the European Union, while both North American and Latin American jurisdictions were only mentioned once each in the papers. This finding is intriguing because several countries in the European Union and North America have emerged as leaders in the development of new technologies.

The majority of the reviewed papers acknowledged the use of blockchain platforms as a solution for chain of custody and evidence control. These findings demonstrate the substantial relevance of applying blockchain technology to enhance secure and immutable data custody. They reinforce the premise that blockchains are an efficient way of registering, tracking and protecting data. Blockchain is considered immutable, due to its inherent characteristics (Antonopoulos 2014).

Despite the small difference between the number of papers that referred to public blockchain systems (13) and those that referred to private blockchain systems (10), it is worth mentioning that the adoption of public blockchain systems tends to prevail in the chain of custody environment. Despite the prevalence of public blockchains, we observed that most of the analyzed solutions applied an extra layer of authentication to guarantee access control. As mentioned before, public blockchains are open and permissionless, meaning anyone can join the network, participate in the consensus mechanism, and validate transactions. They operate on a decentralized model, in which no single entity has control over the network. Private blockchains are restricted and permissioned, allowing only selected participants to join the network. Access and participation are controlled by an organization or a consortium of organizations. Thus, private blockchains are more centralized compared to public blockchains, and are often used for specific business applications within a closed ecosystem.

The openness and distributed nature of public blockchains make them more resistant to attacks, since they rely on cryptographic algorithms and consensus mechanisms, such as Proof-of-Work (PoW) or Proof-of-Stake (PoS). Private blockchains are also considerably safe, but may be more vulnerable to attacks if the central authority, or participating nodes, are compromised.

In general, we noticed that the main platforms used for registering the chain of custody process in blockchains are Hyperledger Fabric (mentioned in 10 papers) and Ethereum (mentioned in 9 papers). This result can be explained by the fact that these platforms offer robust smart contract functionalities, scalability, and established developer communities. Furthermore, Hyperledger Fabric is an established private blockchain, implemented in several use cases and applications. The latter already provides, by default, the necessary access control for chain of custody. This makes these platforms popular choices in the implementation of chain of custody systems.

When the requirements for selecting papers for this SLR were considered, "Data Provenance" was the most frequently mentioned requirement. This emphasizes the need to ensure the origin and history of data in the chain of custody process. This requirement is crucial to establish the integrity and reliability of the evidence throughout the custody chain and for evidence to be accepted in courts in most judicial contexts. It is worth noting that data provenance supports accountability, traceability, and trust in the custody process, as it allows for the identification of any potential tampering or unauthorized access.

The second most mentioned requirement was "Access Control". This result highlights the importance of monitoring access to information and resources within the chain of custody ecosystem. By implementing access control mechanisms, organizations can maintain transparent control over agents handling the evidence, enhancing security and integrity. Moreover, effective access control also includes mechanisms for authentication and authorization. This ensures that only authorized individuals have access to the evidence, protecting against malicious access or modifications.

"Authenticity/Integrity" emerged as the third most frequently mentioned requirement. The latter emphasizes the need to ensure that the data and records within a chain of custody remain consistent and unaltered. By preserving the authenticity and integrity of the evidence, organizations can establish the trustworthiness and admissibility of the evidence in legal proceedings. Authenticity and integrity require the implementation of cryptographic techniques, such as digital signatures and hash functions. The latter allows the detection of any unauthorized modifications or tampering attempts.

Furthermore, the identification of "Auditability" requirement in 11 papers indicates the significance of maintaining a comprehensive and verifiable trail of activities and transactions within the chain of custody. Auditability plays a crucial role in ensuring accountability and transparency. It allows for the examination of the custody process and the detection of any irregularities or potential breaches. By providing an auditable and tamper-proof trail, blockchain-based systems can enable efficient and reliable auditing of the evidence chain of custody.

In regards to "Privacy/Confidentiality", such requirements were mentioned in 10 papers. This highlights the importance of protecting sensitive information and maintaining confidentiality during the evidence chain of custody process. Although it ranked fifth in this analysis, it is worth mentioning that privacy concerns have been widely discussed in recent years, and ensuring privacy in the evidence chain of custody process is of paramount importance. By leveraging blockchain's inherent features, such as encryption and permissioned access, organizations can enhance privacy, protect sensitive data from unauthorized access and protect individuals from being exposed.

The "Process Automation" requirement was mentioned in 9 papers, indicating the potential for blockchain technology to automate and streamline various aspects of the chain of custody process. By automating tasks such as evidence tracking, documentation, and notifications, organizations can reduce manual errors, enhance efficiency, and improve overall operational effectiveness. Furthermore, process automation can also contribute to reducing the risk of improper human intervention and manipulation of evidence or data in the chain of custody process.

Other requirements, such as "Immutability," "Security," and "Transparency," were mentioned in 4 papers each. These requirements highlight the desire for a tamper-resistant, secure, and transparent framework when it comes to preserving evidence. Immutability ensures that once data is recorded on the blockchain, it cannot be altered or deleted, providing a reliable and auditable record of its chain of custody. Security measures, such as encryption and access controls, help protect against unauthorized access and ensure the confidentiality and integrity of the evidence. Transparency is important to the maintainenance of trust and accountability, allowing visibility of the chain of custody process for stakeholders and verifying its reliability and compliance.

Lastly, "Recordkeeping" was mentioned in only three papers, indicating that, while maintaining accurate records is one of the main goals of a chain of custody, the latter requirement may not have received as much attention in the context of blockchain and chain of custody. However, it is important to note that robust recordkeeping practices are essential to maintain a complete and reliable chain of custody. This assures that all relevant information and documentation are recorded and accessible throughout the process.

Regarding the standards underlying the architectures of the system, they serve as relevant parameters for identifying the most common frameworks used for chain of custody registration in blockchain. These frameworks vary from country to country or region to

region, as each has its own set of rules and guidelines. International standards, such as those established by ISO, often act as a common regulatory foundation across different countries, promoting a better understanding of the system's performance. In our SLR, we employed the standards of "Framework," "International Standard," and "Requirements."

The term "Framework" emphasizes the importance of adopting a structured approach when developing blockchain-based systems for chain of custody and evidence. It provides a systematic guide for the implementation of such systems, ensuring interoperability, security, and consistency across various deployments. Additionally, a well-defined framework can help in addressing specific challenges and requirements of the custodial chain domain, such as data privacy, scalability, and trustworthiness. By considering different frameworks, researchers and practitioners can draw upon established best practices and leverage existing knowledge to design effective and reliable systems. The use of "International Standard" reflects the authors' recognition of the necessity to adhere to globally recognized benchmarks in the development of blockchain systems for custodial chains. By following international standards, researchers and practitioners can ensure their systems meet widely accepted criteria for performance, security, and interoperability. It also facilitates knowledge exchange and collaboration across different regions, enabling advancements in the field and contributing to the establishment of a cohesive global ecosystem for custodial chain solutions.

The review identified three mentions of both "Framework" and "International Standard." This suggests a clear acknowledgment of the significance of establishing a comprehensive framework in designing blockchain systems in this domain, while also aligning with internationally accepted standards. The inclusion of "Requirements" twice in the literature indicates that further exploration and standardization efforts are needed in defining the specific requirements for blockchain-based custodial chain systems. Identifying and defining clear requirements assists in the development of more effective and reliable solutions, ensuring the successful implementation and adoption of blockchain technology in this field.

Among the analyzed papers, 13 focused solely on proposing models for utilizing blockchain systems in recording chain of custody and evidence. While these models contribute to conceptualizing the potential benefits and components of custodial chain systems, it is crucial to address the gap between theory and practice. Practical implementation and empirical validation are necessary to assess the feasibility and effectiveness of the proposed models. Future research should emphasize the importance of real-world implementations to validate the theoretical foundations presented in models.

In contrast, 17 papers presented frameworks that offered more comprehensive approaches to implementing blockchain-based systems for chain of custody and evidence recording. These frameworks aim to bridge the gap between theoretical models and practical implementation by providing guidelines and methodologies for system development. By offering a structured approach, these frameworks can assist in the successful deployment and operation of custodial chain systems, ensuring the integrity and transparency of evidence throughout the chain of custody process.

Furthermore, nine papers focused on designing the architecture of blockchain systems. These papers emphasized the structural elements and technical considerations involved in building such systems. Architectural designs contribute to the development of scalable and secure systems, ensuring the effective recording and management of chain of custody and evidentiary information. These papers recognized the importance of system architecture in supporting the core functionalities of custodial chain systems, such as the following: data immutability, transparency, and traceability.

Lastly, only 10 papers progressed beyond the design phase and presented prototypes of blockchain-based chain of custody and evidence recording systems. Prototypes serve as tangible demonstrations of the proposed concepts, allowing for practical evaluation and validation of the proposed solutions. These prototypes provide valuable insights into the

feasibility and performance of blockchain technology in custodial chain applications. They pave the way for further advancements and potential real-world implementations.

This study aimed to answer two research questions: RQ1, How have blockchain and smart contracts been used in the chain of custody of physical evidence? and RQ2, What does blockchain offer to the control of the chain of custody of physical evidence? In answering RQ1, the analysis identified a lack of studies focusing exclusively on the chain of custody of physical evidence. That gap could be explained by the fact that it is difficult to establish a link between the blockchain platform and the physical world to maintain the integrity of physical evidence. However, blockchain is a technology that offers interesting resources to control the provenance of physical materials and to improve access control to chain of custody evidence systems.

In answering RQ2, the analysis indicates that most of the requirements for the protection of digital evidence chain of custody can be applied to the physical evidence chain of custody. Data provenance is required for both types of evidence chain of custody, as much as are access control, authenticity/ integrity, auditability and privacy/confidentiality. It is important to highlight the main differences in the features that blockchain offers to solve problems, with integrity, in regard to both physical and digital evidence. In the first case, blockchain would only be useful to guarantee the integrity of the chain of custody. In regard to digital evidence, depending on the the solution model, blockchain can assure the integrity of both chain of custody and of the evidence per se.

7. Limitation and Future Research

A limitation of this study was that only English-written papers were considered. As this work was limited to a literature review, it did not propose solutions for further problems of chain of custody control and maintenance. Another limitation was that this study's perspective is somewhat restricted to the authors' background and experience with the technology. The research team comprises multidisciplinary researchers with academic backgrounds in Archival Science, Information Technology, and Law. Since the researchers' backgrounds did not cover a wider range of scientific fields this provided the study with a limited perspective.

For future research, it is worth noting that a promising field of study capable of providing valuable insights into the topics of blockchain and chain of custody is supply chain. There is a rich body of literature exploring supply chain enhanced by blockchain technology, for instance, in food safety and agriculture. While information technology has been successfully employed to enhance food safety by providing consumers with more information and transparency on labeling standards (Dospinescu and Dospinescu 2018), the benefits of blockchain in the field of agriculture are already well-known (Bermeo-Almeida et al. 2018). However, many challenges regarding the adoption of blockchain in the supply chain domain remain unaddressed, such as the inability to "determine falsification during initial data entry" (L.B. 2022) (which is also true in the chain of custody of evidence). Another challenge is the risks on privacy and cybersecurity malicious attacks (Bermeo-Almeida et al. 2018), and the lack of a technique for actively monitoring and halting early-stage information tampering (L.B. 2022). Therefore, some aspects of blockchain-based supply chain systems could provide valuable insights for further advancements in chain of custody of the evidence.

In the chain of custody analysis, no article was found that specifically deals with the use of blockchain to control the chain of custody of physical evidence. Only a few of the analyzed works in this review have mentioned the application of a solution in regard to both physical and digital evidence. Most of the resources discussed the use of blockchain to solve digital evidence chain of custody issues. Therefore, future research in this matter includes: (1) a discussion of the use of blockchain for the physical evidence chain of custody control and preservation; (2) an analysis of the limitations of the proposed blockchain solutions, to mitigate existing risks of the chain of custody and the integrity of its evidence; (3) research regarding existing problems in the control of the physical evidence chain of

custody, and (4) investigation into the benefits of using off-chain resources, such as oracles, to provide a link between blockchain and the external environment.

8. Conclusions

This research conducted a comprehensive literature review on the utilization of blockchain technology to ensure control and maintenance of the chain of custody of physical evidence. The analysis demonstrated that there is a lack of research regarding the use of blockchain technology and smart contracts to improve reliability and ensure the integrity of the physical evidence chain of custody. It must be noted that the chain of custody requirements need to be general enough to understand how solutions can be applied to both digital and physical evidence chains of custody. Therefore, an important conclusion of this work is that there is a clear research opportunity regarding the use of blockchain technology in the chain of custody of physical evidence. Since the integrity and trustworthiness of the evidence in the chain of custody are important to avoid future litigation, the use of blockchain technology is ripe for such a context. It can mitigate legal risks, as well as facilitate compliance and auditing. These features can be reinforced by the proposal of a blockchain framework in the chain of custody, which allows for data availability, and, thus, frictionless access to data.

In terms of management, the results of this study demonstrate that not only digital forensics could benefit from blockchain tools to guarantee the trustworthiness of the evidence chain of custody but also traditional forensics. An example of the beneficial aspect of blockchain is that its immutability feature increases the security of chain of custody recording. Also, blockchain allows for a complete visualization of all the registries of evidence made through the chain of custody life cycle in a more linear and organized manner. Another contribution of blockchain to the forensics field would be of economic nature. Since evidence chain of custody maintenance has a public interest and is primarily a government responsibility, using blockchain as a platform to guarantee the recording and integrity of the chain of custody could decrease government expenditures in public safety and judicial proceedings.

Through a comprehensive analysis of existing literature, this systematic review has unveiled significant prospects and notable shortcomings in utilizing blockchain technology in the chain of custody. These findings highlight the potential benefits various domains can derive from harnessing blockchain. The review has brought to light many opportunities for industries to explore through research and development initiatives, specifically by integrating blockchain into the chain of custody framework. These opportunities extend beyond criminal investigations, encompassing diverse sectors such as Oil & Gas.

Furthermore, future research work involves an in-depth discussion for ensuring control and preserving the chain of custody of physical evidence, analysis of the limitations of the proposed blockchain solutions to mitigate existing risks related to the chain of custody, and research regarding existing problems in the control of the physical evidence chain of custody.

Author Contributions: Conceptualization, D.B., A.L.M. and P.H.A.; methodology, D.B. and P.H.A.; formal analysis, B.B. and A.L.M.; investigation, D.B., P.H.A. and A.L.M.; resources, P.H.A.; writing—original draft preparation, D.B. and A.L.M.; writing—review and editing, D.A., A.L.M., P.H.A., I.F., R.N., G.R., G.M.S. and F.P.d.M.; supervision, P.H.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: This study did not report any data.

Acknowledgments: The authors are grateful to Petróleo Brasileiro S.A. (Petrobras) for supporting this study in the context of the Cooperation Agreement with the Pontifical Catholic University at Rio de Janeiro (PUC-Rio).

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

Abbreviations

The following abbreviations are used in this manuscript:

SLR	Systematic Literature Review
ESG	Environmental, Social, and Governance
RQ	Research Question
PoW	Proof-of-Work
PoS	Proof-of-Stake
MDPI	Multidisciplinary Digital Publishing Institute

Note

[1] Bitcoin Price History from 2009 to 2022. Accessed on 15 June 2023. Available at: https://www.forbes.com/advisor/in/investing/cryptocurrency/bitcoin-price-history-chart/.

References

Ahmad, Liza, Salam Khanji, Farkhund Iqbal, and Faouzi Kamoun. 2020. Blockchain-based chain of custody: Towards real-time tamper-proof evidence management. Paper presented at 15th International Conference on Availability, Reliability and Security, Virtual Event, Ireland, August 25–28 ; pp. 1–8.

Ahmadi-Assalemi, Gabriela, Haider M. Al-Khateeb, Gregory Epiphaniou, Jon Cosson, Hamid Jahankhani, and Prashant Pillai. 2019. Federated blockchain-based tracking and liability attribution framework for employees and cyber-physical objects in a smart workplace. Paper presented at 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, UK, January 16–18; pp. 1–9.

Akinbi, Alex, Áine MacDermott, and Aras M. Ismael. 2022. A systematic literature review of blockchain-based internet of things (iot) forensic investigation process models. *Forensic Science International: Digital Investigation* 42: 301470. [CrossRef]

Ali, Mohamed, Ahmed Ismail, Hany Elgohary, Saad Darwish, and Saleh Mesbah. 2022. A procedure for tracing chain of custody in digital image forensics: A paradigm based on grey hash and blockchain. *Symmetry* 14: 334. [CrossRef]

Al-Khateeb, Haider, Gregory Epiphaniou, and Herbert Daly. 2019. Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger. *Blockchain and Clinical Trial: Securing Patient Data*, 149–68. [CrossRef]

Alruwaili, Fahad F. 2021. Custodyblock: A distributed chain of custody evidence framework. *Information* 2: 88. [CrossRef]

Alves, Paulo Henrique, Isabella Z. Frajhof, Élisson Michael Araújo, Yang Ricardo Miranda, Rafael Nasser, Gustavo Robichez, Ronnie Paskin, Alessandro Garcia, Cristiane Lodi, Flavia Pacheco, and et al. 2022. Blockchain-based enterprise ballots in an oil and gas consortium. In *Enterprise Information Systems: 23rd International Conference, ICEIS 2021, Virtual Event, April 26–28. 2021, Revised Selected Papers*. Berlin and Heidelberg: Springer; pp. 211–35.

Antonopoulos, Andreas M. 2014. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Sebastopol: O'Reilly Media, Inc.

Ariffin, Khairul Akram Zainol, and Faris Hanif Ahmad. 2021. Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0. *Computers & Security* 105: 102237.

Attaran, Mohsen, and Angappa Gunasekaran. 2019. *Applications of Blockchain Technology in Business: Challenges and Opportunities*. Berlin: Springer Nature.

Awuson-David, Kenny, Tawfik Al-Hadhrami, Mamoun Alazab, Nazaraf Shah, and Andrii Shalaginov. 2021. Bcfl logging: An approach to acquire and preserve admissible digital forensics evidence in cloud ecosystem. *Future Generation Computer Systems* 122: 1–13. [CrossRef]

Bager, Simon L., Christina Singh, and U. Martin Persson. 2022. Blockchain is not a silver bullet for agro-food supply chain sustainability: Insights from a coffee case study. *Current Research in Environmental Sustainability* 4: 100163. [CrossRef]

Bermeo-Almeida, Oscar, Mario Cardenas-Rodriguez, Teresa Samaniego-Cobo, Enrique Ferruzola-Gómez, Roberto Cabezas-Cabezas, and William Bazán-Vera. 2018. Blockchain in agriculture: A systematic literature review. In *Technologies and Innovation. CITI 2018*. Cham: Springer, pp. 44–56.

Blowers, Misty, Shaun Scrafford, and Jon Williams. 2019. Blockchain technologies and distributed ledger systems as enablers for real time decision support. In *Disruptive Technologies in Information Sciences II*. Bellingham: SPIE, vol. 11013, pp. 109–13.

Bonomi, Silvia, Marco Casini, and Claudio Ciccotelli. 2018. B-coc: A blockchain-based chain of custody for evidences management in digital forensics. *arXiv* arXiv:1807.10359.

Burri, Xavier, Eoghan Casey, Timothy Bolle, and David-Olivier Jaquet-Chiffelle. 2020. Chronological independently verifiable electronic chain of custody ledger using blockchain technology. *Forensic Science International: Digital Investigation* 33: 300976. [CrossRef]

Buterin, Vitalik. 2014. A next-generation smart contract and decentralized application platform. *White Paper* 3: 1–36.

Calvão, Filipe, and Matthew Archer. 2021. Digital extraction: Blockchain traceability in mineral supply chains. *Political Geography* 87: 102381. [CrossRef]

Chandramouli, Krishna, Roxana Horincar, Charlotte Jacobe de Naurois, Dirk Pallmer, David Faure, Wilmuth Müller, and Konstantinos Demestichas. 2022. Blockchain technologies for chain of custody authentication. *Security Technologies and Social Implications*, 262–89. [CrossRef]

Chen, Jiachi, Xin Xia, David Lo, John Grundy, and Xiaohu Yang. 2020. Maintaining smart contracts on ethereum: Issues, techniques, and future challenges. *arXiv* arXiv:2007.00286.

Chopade, Mrunali, Sana Khan, Uzma Shaikh, and Renuka Pawar. 2019. Digital forensics: Maintaining chain of custody using blockchain. Paper presented at 2019 Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, December 12–14; pp. 744–47.

Demestichas, Konstantinos, Nikolaos Peppes, Theodoros Alexakis, and Evgenia Adamopoulou. 2020. Blockchain in agriculture traceability systems: A review. *Applied Sciences* 10: 4113. [CrossRef]

Dospinescu, Octavian, and Nicoleta Dospinescu. 2018. The use of information technology toward the ethics of food safety. *Ecoforum Journal* 7: 4113.

Douladiris, Kostas, Thomas Dasaklis, Fran Casino, and Christos Douligeris. 2020. A blockchain framework for reverse logistics of used medical equipment. Paper presented at 4th Pan-Hellenic Conference on Informatics, Athens, Greece, November 29–December 1; pp. 148–51.

Elgohary, Hany M., Saad M. Darwish, and Saleh Mesbah Elkaffas. 2022. Improving uncertainty in chain of custody for image forensics investigation applications. *IEEE Access* 10: 14669–79. [CrossRef]

Grima, Simon, Murat Kizilkaya, Kiran Sood, and Mehmet ErdemDelice. 2021. The perceived effectiveness of blockchain for digital operational risk resilience in the european union insurance market sector. *Journal of Risk and Financial Management* 14: 363. [CrossRef]

Gupta, Abhishek, and Preeti Mishra. 2021. Blockchain based framework to maintain chain of custody (coc) in a forensic investigation. In *Advances in Computing and Data Sciences: 5th International Conference, ICACDS 2021, Nashik, India, April 23–24. 2021, Revised Selected Papers, Part I 5*. Berlin and Heidelberg: Springer, pp. 37–46.

Hingorani, Ishwarlal, Rushabh Khara, Deepika Pomendkar, and Nataasha Raul. 2020. Police complaint management system using blockchain technology. Paper presented at 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, December 3–5; pp. 1214–19.

Hölbl, Marko, Marko Kompara, Aida Kamišalić, and Lili Nemec Zlatolas. 2018. A systematic review of the use of blockchain in healthcare. *Symmetry* 10: 470. [CrossRef]

Jahankhani, Hamid, Stefan Kendzierskyj, and Anita Colin. 2021. Blockchain as a tool for transparency and governance in the delivery of development aid. In *Strategy, Leadership, and AI in the Cyber Ecosystem*. London: Elsevier, pp. 93–111.

Jaquet-Chiffelle, David-Olivier, Eoghan Casey, and Jonathan Bourquenoud. 2020. Tamperproof timestamped provenance ledger using blockchain technology. *Forensic Science International: Digital Investigation* 33: 300977. [CrossRef]

Jung, Po-Yu, and Fu-Ching Tsai. 2020. An autotriage b-coc model in digital forensic investigation. *Procedia Computer Science* 176: 1729–35. [CrossRef]

Khan, Abdullah Ayub, Mueen Uddin, Aftab Ahmed Shaikh, Asif Ali Laghari, and Adil E. Rajput. 2021. Mf-ledger: Blockchain hyperledger sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture. *IEEE Access* 9: 103637–650. [CrossRef]

Khanji, Salam, Omar Alfandi, Liza Ahmad, Lubna Kakkengal, and Mousa Al-kfairy. 2022. A systematic analysis on the readiness of blockchain integration in iot forensics. *Forensic Science International: Digital Investigation* 42: 301472. [CrossRef]

Kramer, Michael Paul, Linda Bitsch, and Jon H. Hanf. 2021. The impact of instrumental stakeholder management on blockchain technology adoption behavior in agri-food supply chains. *Journal of Risk and Financial Management* 14: 598. [CrossRef]

Kumar, Gulshan, Rahul Saha, Chhagan Lal, and Mauro Conti. 2021. Internet-of-forensic (iof): A blockchain based digital forensics framework for iot applications. *Future Generation Computer Systems* 120: 13–25. [CrossRef]

L.B., Krithika. 2022. Survey on the applications of blockchain in agriculture. *Agriculture* 12: 1333. [CrossRef]

Li, Meng, Chhagan Lal, Mauro Conti, and Donghui Hu. 2021. Lechain: A blockchain-based lawful evidence management scheme for digital forensics. *Future Generation Computer Systems* 115: 406–20. [CrossRef]

Liu, Gongzheng, Jingsha He, and Xinggang Xuan. 2021. A data preservation method based on blockchain and multidimensional hash for digital forensics. *Complexity* 2021: 5536326. [CrossRef]

Lone, Auqib Hamid, and Roohie Naaz Mir. 2019. Forensic-chain: Blockchain based digital forensics chain of custody with poc in hyperledger composer. *Digital Investigation* 28: 44–55. [CrossRef]

Lourinho, Lynton, Stefan Kendzierskyj, and Hamid Jahankhani. 2021. Securing the digital witness identity using blockchain and zero-knowledge proofs. In *Strategy, Leadership, and AI in the Cyber Ecosystem*. Amsterdam: Elsevier, pp. 159–94.

Malamas, Vaggelis, Thomas Dasaklis, Panayiotis Kotzanikolaou, Mike Burmester, and Sokratis Katsikas. 2019. A forensics-by-design management framework for medical devices based on blockchain. Paper presented at 2019 IEEE world congress on services (SERVICES), Milan, Italy, July 8–13; vol. 2642, pp. 35–40.

Miranda, Yang R., Paulo H. Alves, Ronnie Paskin, Rafael B. Nasser, Gustavo Robichez, Luiz Faria, Roberto Trindade, Joana Silva, Leandro Peixoto, and Fernando Pellon de Miranda. 2023. Enhancing corporate social responsibility with blockchain-based trackable esg tokens. In *WBlockchain—VI Workshop Blockchain: Teoria, Tecnologia e Aplicacoes*. Porto Alegre: Sociedade Brasileira de Computação.

Mugurusi, Godfrey, and Emmanuel Ahishakiye. 2022. Blockchain technology needs for sustainable mineral supply chains: A framework for responsible sourcing of cobalt. *Procedia Computer Science* 200: 638–47. [CrossRef]

Olukoya, Oluwafemi. 2021. Distilling blockchain requirements for digital investigation platforms. *Journal of Information Security and Applications* 62: 102969. [CrossRef]

Owens, Jeffrey P., and Sabina Hodžić. 2022. Policy note: Blockchain technology: Potential for digital tax administration. *Intertax* 50: 813–23. [CrossRef]

Parkin, Avril, and Rodney Prescott. 2017. Distributed ledger technology: Beyond the hype. *Journal of Digital Banking* 2: 102–9.

Prieto, Javier, Francisco Luis Benítez Martínez, Stefano Ferretti, David Arroyo Guardeño, and Pedro Tómas Nevado-Batalla. 2022. *Blockchain and Applications, 4th International Congress on Blockchain and Applications*. Lecture Notes in Networks and Systems. Berlin: Springer, vol. 595, pp. 142–49.

Pourvahab, Mehran, and Gholamhossein Ekbatanifard. 2019. An efficient forensics architecture in software-defined networking-iot using blockchain technology. *IEEE Access* 7: 99573–88. [CrossRef]

Robichez, G, Rafael Nasser, Isabella Frajhof, Paulo Henrique Alves, Armando Cavanha, Flavia Pacheco, and Cristiane Lodi. 2021. *Blockchain Initiatives on the Oil and Gas Industry*. Technical report, Tech. rep. Rio de Janeiro: Pontifical Catholic University of Rio de Janeiro PUC-Rio.

Sathyaprakasan, Revathy, Pratheeksha Govindan, Samina Alvi, Lipsa Sadath, Sharon Philip, and Nrashant Singh. 2021. An implementation of blockchain technology in forensic evidence management. Paper presented at 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, March 17–18; pp. 208–12.

Silva, Wagner, and Ana Cristina Bicharra Garcia. 2021. Where is our data? A blockchain-based information chain of custody model for privacy improvement. Paper presented at 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Dalian, China, May 5–7; pp. 329–34.

Stoyanova, Maria, Yannis Nikoloudakis, Spyridon Panagiotakis, Evangelos Pallis, and Evangelos K. Markakis. 2020. A survey on the internet of things (iot) forensics: Challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials* 22: 1191–221.

Tsai, Fu-Ching. 2021. The application of blockchain of custody in criminal investigation process. *Procedia Computer Science* 192: 2779–88. [CrossRef]

Wang, Shan, Ming Yang, Tingjian Ge, Yan Luo, and Xinwen Fu. 2022. Bbs: A blockchain big-data sharing system. Paper presented at ICC 2022-IEEE International Conference on Communications, Seoul, Republic of Korea, May 16–20; pp. 4205–10.

Yan, Wenqi, Jiachen Shen, Zhenfu Cao, and Xiaolei Dong. 2020. Blockchain based digital evidence chain of custody. Paper presented at the 2020 The 2nd International Conference on Blockchain Technology, Hilo, HI, USA, March 12–14; pp. 19–23.

Zarchi, Gal, Maya Sherman, Omer Gady, Tomer Herzig, Ziv Idan, and Dov Greenbaum. 2022. Blockchains as a means to promote privacy protecting, access availing, incentive increasing, elsi lessening dna databases. *Frontiers in Digital Health* 4: 1028249. [CrossRef]

Zawoad, Shams, and Ragib Hasan. 2015. Faiot: Towards building a forensics aware eco system for the internet of things. Paper presented at 2015 IEEE International Conference on Services Computing, New York, NY, USA, June 27–July 2; pp. 279–84.

Zhang, Yong, Songyang Wu, Bo Jin, and Jiaying Du. 2017. A blockchain-based process provenance for cloud forensics. Paper presented at 2017 3rd IEEE international conference on computer and communications (ICCC), Chengdu, China, December 13–16; pp. 2470–73.