computers

MDPI

Systematic Review

Cyber Threat Intelligence on Blockchain: A Systematic Literature Review

Dimitrios Chatziamanetoglou * and Konstantinos Rantos

Department of Computer Science, International Hellenic University, 65404 Kavala, Greece; krantos@cs.ihu.gr
* Correspondence: diehatz@cs.ihu.gr

Abstract: Cyber Threat Intelligence (CTI) has become increasingly important in safeguarding organizations against cyber threats. However, managing, storing, analyzing, and sharing vast and sensitive threat intelligence data is a challenge. Blockchain technology, with its robust and tamper-resistant properties, offers a promising solution to address these challenges. This systematic literature review explores the recent advancements and emerging trends at the intersection of CTI and blockchain technology. We reviewed research papers published during the last 5 years to investigate the various proposals, methodologies, models, and implementations related to the distributed ledger technology and how this technology can be used to collect, store, analyze, and share CTI in a secured and controlled manner, as well as how this combination can further support additional dimensions such as quality assurance, reputation, and trust. Our findings highlight the focus of the CTI and blockchain convergence on the dissemination phase in the CTI lifecycle, reflecting a substantial emphasis on optimizing the efficacy of communication and sharing mechanisms, based on an equitable emphasis on both permissioned, private blockchains and permissionless, public blockchains, addressing the diverse requirements and preferences within the CTI community. The analysis reveals a focus towards the tactical and technical dimensions of CTI, compared to the operational and strategic CTI levels, indicating an emphasis on more technical-oriented utilization within the domain of blockchain technology. The technological landscape supporting CTI and blockchain integration emerges as multifaceted, featuring pivotal roles played by smart contracts, machine learning, federated learning, consensus algorithms, IPFS, deep learning, and encryption. This integration of diverse technologies contributes to the robustness and adaptability of the proposed frameworks. Moreover, our exploration unveils the overarching significance of trust and privacy as predominant themes, underscoring their pivotal roles in shaping the landscape within our research realm. Additionally, our study addresses the maturity assessment of these integrated systems. The approach taken in evaluating maturity levels, distributed across the Technology Readiness Level (TRL) scale, reveals an average balance, indicating that research efforts span from early to mid-stages of maturity in implementation. This study signifies the ongoing evolution and maturation of research endeavors within the dynamic intersection of CTI and blockchain technology, identifies trends, and also highlights research gaps that can potentially be addressed by future research on the field.

Keywords: cyber threat intelligence; blockchain; cybersecurity

Citation: Chatziamanetoglou, D.; Rantos, K. Cyber Threat Intelligence on Blockchain: A Systematic Literature Review. *Computers* **2024**, *13*, 60. https://doi.org/10.3390/computers13030060

Academic Editors: Yu Chen, Sachin Shetty and Shantanu Pal

Received: 3 January 2024
Revised: 22 February 2024
Accepted: 23 February 2024
Published: 26 February 2024

1. Introduction

In the modern digital landscape, the field of cyber threat intelligence (CTI) has assumed an indispensable role in safeguarding the increasingly complex digital realm against persistent and sophisticated cyber threats. As the digital interdependencies grow deeper and more intricate, expanding the attack surface of organizations, cyber adversaries continually evolve their tactics, seeking to infiltrate systems, compromise data, and undermine cybersecurity. Recognizing the dynamic nature of these threats, organizations have shifted their focus from reactive cybersecurity measures towards more proactive and predictive approaches.

In this paper, we acknowledge that while there might be many variations, CTI is generally referenced in a similar manner across different perspectives. For the context of our work, we specifically adhere to the NIST publication 800-150 definition [1], being any information related to a threat that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes, which might help an organization protect itself against a threat or detect the activities of an actor. This definition guides our exploration, ensuring a consistent and precise framework for our study.

Under this definition, CTI is interrelated among other factors, with collection, analysis, transformation, and dissemination, serving as a comprehensive framework for our research, ensuring methodological consistency. Importantly, this definition contributes significantly to the formulation of our research questions, particularly in the context of the convergence with blockchain technology. By aligning with NIST 800-150, our study not only adheres to established standards but also facilitates an in-depth exploration of the convergence between CTI and blockchain. This integration enhances the precision of our methodology, providing a robust basis for investigating this dynamic landscape of cybersecurity.

CTI, once primarily reactive in nature, has now grown as part of a proactive intelligence collection and decision-making process, aimed at enhancing preparedness against and facilitating mitigation of cyber threats. This transformation relies on the collection and analysis of timely, relevant, and actionable information about potential and existing threats, as well as the tactics and attack patterns employed by adversaries. This paradigm shift has empowered organizations to strengthen their cybersecurity defenses, identify vulnerabilities, and counter potential attacks more effectively [2]. However, with this expansion in scope and capability comes a corresponding challenge; the management, storage, analysis, and sharing of vast and sensitive threat intelligence data.

The integration of CTI with blockchain technology presents a promising solution to address these challenges. In a broader context, CTI encompasses the practice of collecting, analyzing, and disseminating data and insights related to cyber threats. The information offered in CTI varies depending on its depth and nature, encompassing an amalgamation of elements such as threat actors, attack patterns, methodologies, motives, threat severity, the broader threat landscape, Techniques–Tactics–Procedures (TTPs), and Indicators of Compromise (IoC) [3]. At every level of CTI, the mechanism for sharing such intelligence plays a pivotal role. This sharing mechanism is the focal point of dedicated endeavors by governmental institutions, private sector entities, IT security vendors, the IT industry, and security researchers. Their collective effort is geared toward establishing a dependable, timely, and accurate framework for the dissemination of CTI.

On the other hand, blockchain, renowned for its robust and tamper-resistant properties as a distributed ledger technology, introduces a transformative shift in data and transaction management. Beyond its foundational feature of immutability, blockchain shines with its exceptional attributes of availability and scalability. Its decentralized network ensures data redundancy across multiple nodes, guaranteeing accessibility even during system failures or cyberattacks. This scalability is vital as CTI accumulates vast volumes of threat-related data.

The convergence of CTI with blockchain technology has ignited growing interest within the cybersecurity community, offering the potential to revolutionize the threat intelligence landscape. By harnessing blockchain's innate attributes of immutability, availability, and scalability, CTI stakeholders are in position to follow through an era of secure, transparent, and collaborative methods for managing, analyzing, and sharing threat intelligence, enhancing data integrity, ensuring uninterrupted access to critical intelligence, and providing a trusted platform for cross-industry cooperation. In this synergy, CTI and blockchain have the potential to bolster cybersecurity efforts and overcome the persistent challenges of securely handling and disseminating critical threat information.

In light of these developments, this literature review embarks on a comprehensive exploration of the recent advancements and emerging trends that lie at the intersection

of CTI and blockchain technology. Specifically, we reviewed research papers published during the last 5 years to investigate the various proposals, methodologies, models, and implementations related to the distributed ledger technology and how this technology can be used to collect, store, analyze, and share CTI in a secured and controlled manner, as well as how this combination can further support additional dimensions such as quality assurance, reputation, and trust. Our aim is to contribute to the existing knowledge in this field by identifying and incorporating state-of-the-art methods and techniques found in the literature.

The remainder of the paper is structured and organized as follows: Section 2 presents the existing research that has been performed in the field of this review and the differences from our scope of work. Section 3 outlines the research methodology, including the scope, the objectives, the research questions, the search strategy, and the eligibility criteria of this Systematic Literature Review (SLR). Section 4 presents the results and the categorization criteria of this review. Section 5 presents the literature review of the research papers in the scope of this SLR. Section 6 discusses the results in the context of the research conducted in the field, while Section 7 provides some limitations to our study. Finally, Section 8 refers to the threats of validity of our research, and Section 9 presents the conclusions of our work.

2. Related Work

Reviewing the current landscape of related work in the field of CTI, it is evident that a rich and dynamic mass of research has been developed in response to the evolving threat landscape, contributing to a comprehensive understanding of CTI's role in enhancing cybersecurity resilience and response strategies [4,5]. In addition, similar emerging research activity applies to distributed ledger technology, which is increasingly seen as a vital component of modern cyber security with a very wide spectrum of applications [6–8]. As blockchain technology continues to mature and gain adoption, it holds the promise of reshaping how CTI is collected, stored, and shared, ultimately strengthening the collective defense against cyber threat evolution.

Furthermore, non-surprisingly, numerous studies have focused during the last years on various aspects of CTI, ranging from its fundamental concepts and data sources to advanced methodologies, sharing mechanisms, and integration with cutting-edge technologies like blockchain. By converging CTI with distributed ledger technology, and by harnessing blockchain's inherent security attributes, such as data immutability, decentralized architecture, and cryptographic safeguards, CTI stakeholders aim to create a more transparent, trustworthy, and collaborative ecosystem for threat intelligence ecosystem.

While CTI and blockchain technology have both seen substantial individual attention in the literature, the synergy arising from their convergence represents a compelling and promising area for inquiry. Nonetheless, according to our research, there have been relatively few literature reviews found in this field, scoping the evolving relationship and convergence of CTI and blockchain technology research. Specifically, the lack of studies that holistically scope and present the trajectory of research developments in these two domains combined is noticeable.

El-Kosairy et al. [9] conducted a survey on CTI sharing based on blockchain, collecting the latest research contributions that use blockchain to overcome the conventional CTI problems, comparing them for awareness about the different methods used, and pointing out uncovered areas for further research. It is important to note that this study presented the advancements in integrating CTI with blockchain technology, emphasizing pertinent challenges within the domain. However, it is crucial to acknowledge that this study does not claim to be exhaustive in encapsulating the entirety of relevant research papers published in the field up to the point of review.

Dunnett et al. [10], presented their research about the challenges and opportunities of blockchain for CTI sharing. Nevertheless, their research was conducted in early 2022, which means it does not encompass the most recent developments in the field. Furthermore, their

study appears to be more widely oriented and does not provide a comprehensive overview of the entire body of literature related to this topic.

Finally, Saxena et al. [11] presented CTI challenges in a relationship with blockchain and presented a conceptual and abstract proposal for a blockchain-based CTI sharing model. However, their study, while insightful, does not comprehensively capture the entire landscape in the subject area of our research.

The scarcity of comprehensive updated literature reviews in this intersection underscores the need for our research, as it aims to bridge this gap by providing an in-depth analysis and synthesis of the evolving CTI and blockchain landscape. In that respect, we seek to offer a comprehensive and up-to-date overview of the research in this emerging field, underpinning the potential of the amalgamation of CTI and blockchain technology.

A comparison table between existing related work and our systematic review is depicted in Table 1.

Table 1. Comparison with related work.

Study	Type	Method	Research Period	Literature Coverage
El-Kosairy et al. [9]	Survey	Not mentioned	2018–2021	Does not cover all existing literature by the time it was conducted
Dunnett et al. [10]	Survey	Not mentioned	2017–2021	Does not encompass the most recent developments in the field by the time it was conducted
Saxena et al. [11]	Survey	Not mentioned	2017–2021	Does not capture comprehensively the entire landscape
This Work	SLR	PRISMA with 6 RQs	Last 5 years	Extensive literature coverage

3. Research Methodology

In this section, we outline the procedures that we applied during our review process, emphasizing how we identified, screened, selected, and analyzed articles that incorporate the utilization of blockchain technology as a foundational component in the domain of CTI. Our methodological approach involves a systematic literature review, which was conducted in accordance with established guidelines to comprehensively survey and synthesize the existing scope of research on this specific intersection. Through this detailed review process, we aim to identify insights, trends, and potential challenges related to the use of blockchain in relation to the CTI lifecycle, contributing to a holistic understanding of its impact on the field.

3.1. Research Scope

Our research scope focuses on the dynamic interplay and overlap between blockchain technology and CTI, with a particular emphasis on their integration within the broader framework of the various other contributing factors, such as stages of the CTI lifecycle, supporting technology, CTI levels, and blockchain type. The scope of the present research is graphically shown in Figure 1.

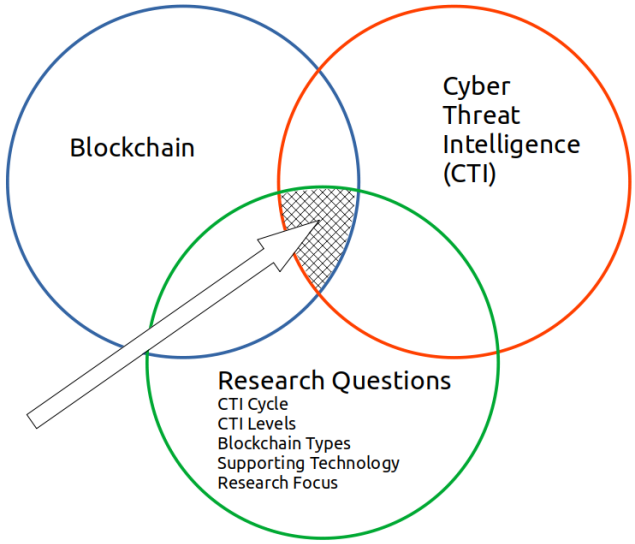

Figure 1. Scope of the research.

3.2. Research Objective and Research Questions

Taking into consideration that the research in the field of CTI and blockchain has grown during recent years, the objective of the present review is to present a comprehensive and systematic bibliographic review of related work that was published in the last five years and, if possible, identify the areas and potential trends that show increased research interest.

The research questions (RQs) that this review is focusing on answering are the following:

RQ1: Which areas of the CTI lifecycle (direction, collection, processing, dissemination) [12] have attracted more research interest?
RQ2: Which level of CTI data (strategic, operational, tactical, technical) [12] is in the scope of each research paper?
RQ3: What aspects of CTI data, like trust, reputation, privacy, quality, and sustainability, are in the scope of each study?
RQ4: Which particular supporting technology or methodology is used in each research?
RQ5: What type of blockchain technology is used (permissioned vs. permissionless and/or private vs. public)?
RQ6: What is the implementation maturity of the proposed solutions?

3.3. SLR Method

To meet the research objectives of this paper, we opted for the systematic literature review (SLR) method. SLR is a widely applied approach in various research domains, including computer science and technology [13]. It is characterized by its systematic and comprehensive nature, involving well-defined steps and methods [14]. In that respect, we specifically adopted the PRISMA methodology [15] as the research method for this paper. The aim is to ensure an unbiased selection procedure and criteria for accounting all published articles relevant to our research scope. The transparency inherent to the SLR process forms the foundation for achieving high-quality standards in both the process and the results. However, it is essential to acknowledge that the search is limited to specific databases, which entails the risk of potentially missing a portion of the published research worldwide. In the forthcoming sections, we provide a detailed account of the research and analysis steps.

The next procedural step that has to be applied is the definition of the research strategy, which encompasses the selection of data sources, research string, and the criteria for selection. Subsequently, the process involves an initial screening phase, wherein titles and

abstracts are evaluated for relevance. Following this, relevant information is extracted, and an analysis and synthesis of this data takes place. The output of this comprehensive process results in the composition of the final study report [16].

3.4. Search Strategy and Eligibility Criteria

The search strategy of the SLR included the selection of the data sources and the formation of the search criteria. It was meant to be kept as simple as possible, in order to narrow down the results as well as keep the resulting output as relevant as possible. The search was performed against the Scopus database, as it is the most comprehensive source of information in the field of the present research, referencing the main volume of published material.

The selection criteria involve careful consideration of specific factors such as relevance to the scope of the present SLR, ensuring that the chosen papers explicitly discuss or investigate the convergence of CTI with blockchain and publication recency bounded to the specified period of 5 years to maintain a contemporary focus. In addition, clarity, coherence, and methodological rigor were taken into strong consideration.

On the other hand, exclusion criteria were applied to ensure the selection of impactful research. Sources lacking clear contributions to the understanding of CTI and blockchain convergence were excluded to prioritize substantive insights. Further refinement was achieved by excluding papers with limited accessibility, ensuring that our review comprises readily available and accessible research. Irrelevant publications, not directly addressing the convergence of CTI with blockchain, were also excluded to streamline the focus of our study and enhance the relevance of the selected literature.

The search string was the following:

```
TITLE-ABS-KEY (cyber AND threat AND intelligence AND blockchain)
```

The search criteria were based on the English language and there were no exclusions since the intent was to gather first all the relevant output and then screen the content on a manual basis for more accuracy.

4. Results and Categorization

4.1. Output and Selection of Publications

Based on the search criteria applied in October 2023, a total of 158 research publications were retrieved from the Scopus database. During the initial screening process, 79 publications passed as being within the margins of the research scope and 79 were filtered out. The excluded papers, at this stage, were as follows:

- 31 papers as literature reviews not in the scope of our research;
- 25 publications as lecture notes and book chapters;
- 21 papers found out of scope;
- 1 paper in duplication;
- 1 paper published in a non-English language.

During the next stage, the 79 initially accepted papers were further manually full-text screened, and the following 32 papers were found to be further excluded:

- 10 papers not related to CTI;
- 13 found to have a general reference to CTI but with no contributing value to the present research;
- 9 found to have a general reference to the application of blockchain technology with only a very abstract approach toward CTI.

As a result, from the evaluation process, 47 research publications were found to be ultimately accepted for further analysis in the present systematic literature review. The source selection process is shown schematically in Figure 2. Furthermore, the yearly distribution of the finally included research papers in our systematic review is depicted in

Figure 3, where it is shown that from 2018 onwards, there is an increasing trend in relevant research publications.

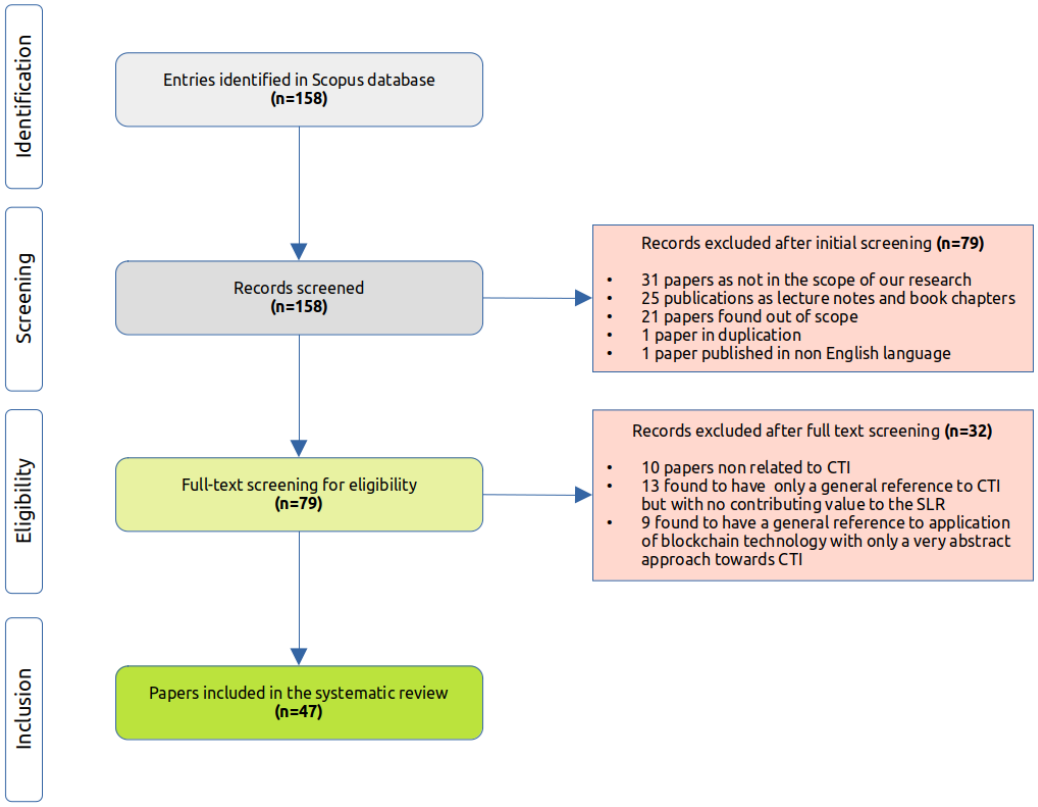

Figure 2. Source selection process from the Scopus database (PRISMA flowchart).

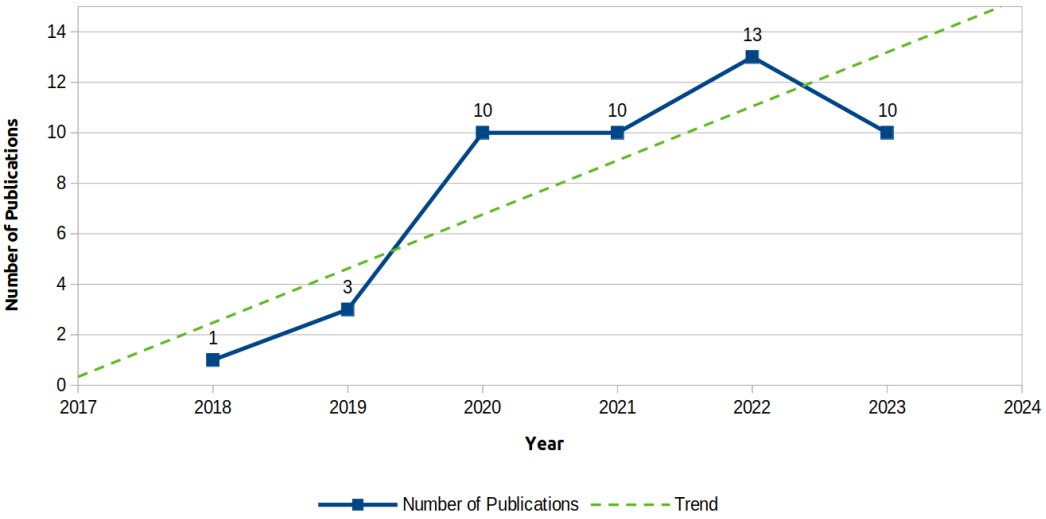

Figure 3. Yearly distribution of research papers included in our systematic review.

4.2. Categorization Criteria

This literature review will follow the approach of categorizing the reviewed papers based on the research questions addressed in Section 3. This means that the categorization will focus on the aspects shown in Table 2 and detailed below.

Table 2. Categorization criteria.

Categories	Elements
CTI Lifecycle Stage	Direction Collection Processing Dissemination
CTI Level	Strategic Operational Tactical Technical
Research Focus	Trust Privacy Reputation Quality Sustainability Performance Scalability
Supporting Technology	Artificial Intelligence Machine Learning Federating Learning Smart Contracts Consensus Algorithms Interplanetary File System
Blockchain Type	[Permissioned/Permissionless] [Public/Private/Consortium]
Implementation Maturity	TRL 1-9

4.2.1. CTI Lifecycle Stages

The CTI lifecycle is a systematic and iterative process designed to enhance an organization's cybersecurity posture by providing timely and relevant information about potential threats. This lifecycle involves several stages, for which various perspectives can be found in the literature [3,12,17]. In the context of this research, the model referred to in [12] was selected, comprising four stages: direction, collection, processing, and dissemination. This approach stems from the need for simplicity and a focus on presenting a higher-level overview. Recognizing the complexity inherent in more detailed models, the choice was made to streamline and facilitate a clearer understanding at a broader level.

4.2.2. CTI Level

CTI operates on various levels to provide comprehensive insights into the evolving threat landscape [18,19]. At the *strategic* level, it provides organizational leaders with a high-level understanding of cyber threats and their potential implications. *Operational* CTI provides real-time, actionable intelligence for immediate defensive actions and incident response. *Tactical* CTI delves into specific threats, offering details on indicators and adversary tactics, aiding in preparation and understanding. Adding a technical layer, *technical* CTI furnishes granular details on cyber threats, enabling cybersecurity professionals to implement precise and effective countermeasures. These levels collectively equip organizations to navigate and defend against cyber threats across strategic, operational, tactical, and technical dimensions [20].

4.2.3. Research Focus

Trust, privacy, reputation, quality, sustainability, performance, and scalability are integral aspects of CTI [21,22]. *Trust* is crucial in information sharing to ensure the reliability of intelligence sources and collaborative efforts. *Privacy* considerations safeguard sensitive data involved in CTI processes, promoting responsible information handling. *Reputation* and *quality* measures are essential to assess the reliability and accuracy of threat intelligence sources, influencing decision-making. *Sustainability* is vital for ensuring the longevity and

relevance of CTI frameworks amid evolving cyber landscapes. *Performance* considerations, including speed and efficiency, are paramount for timely threat detection and response. Lastly, *scalability* ensures that CTI systems can adapt to growing volumes of data and emerging threats, maintaining effectiveness over time.

4.2.4. Supporting Technology

The integration of artificial intelligence, including machine learning, deep learning, and federated learning algorithms, into blockchains [23] in combination with the usage of consensus algorithms and smart contracts, significantly advances CTI [4,19,24,25]. AI empowers CTI systems to autonomously analyze massive datasets, identify patterns, and discover complex threat behaviors, enhancing the precision and efficiency of threat detection. Federated learning introduces a collaborative dimension, enabling organizations to pool insights without compromising data privacy, thereby enhancing the collective defense against evolving threats.

Consensus algorithms ensure the integrity of information in a distributed CTI network, fostering trust among participants by validating and securing shared intelligence. Smart contracts, implemented using blockchain technology, facilitate secure and automated execution of agreements in CTI processes, ensuring transparency, trust, and the seamless enforcement of predefined rules. The amalgamation of these technologies and features fortifies CTI capabilities, providing a dynamic and adaptive framework for organizations to proactively address the ever-changing cybersecurity landscape.

In addition, the incorporation of the Interplanetary File System (IPFS) complements this integrated approach by offering decentralized and content-addressable file storage. IPFS contributes to the scalability and resilience of CTI ecosystems, allowing for efficient and secure off-chain storage of large files and data. This aligns with the decentralized nature of blockchain technology, enhancing the reliability and accessibility of critical threat intelligence information across the network.

4.2.5. Blockchain Type

Permissioned/permissionless and public/private blockchains represent distinct models within the blockchain ecosystem [26]. In a permissioned blockchain, access to the network and participation in the consensus process is restricted to a predefined set of entities, often known and trusted participants. This model is suitable for applications where a higher level of control, privacy, and regulatory compliance is required. On the other hand, permissionless blockchains operate on an open-access principle, allowing anyone to join the network, participate in consensus, and validate transactions without requiring explicit permission. Public blockchains, whether permissioned or permissionless, are accessible to anyone, fostering full decentralization. In contrast, private blockchains limit access to a specific group of participants, offering enhanced privacy and control over the network. Each model applies to different use cases, balancing factors like transparency, decentralization, access control, and regulatory compliance based on the specific requirements of the application or industry.

4.2.6. Implementation Maturity

Evaluating the implementation maturity of a research paper in a technical domain involves employing frameworks such as the Technology Readiness Level (TRL) [27]. TRL, a scale ranging from 1 to 9, assesses the progression of a technology or solution from basic principles (TRL1) to proven success in operational environments (TRL9). This framework is widely adopted across industries for its structured approach to gauging the readiness of a proposed solution. In the present literature review, this approach will be used to assess the implementation maturity of the scoped research papers, considering experimental validation, scalability, integration with existing technologies, and real-world applicability. However, this assessment will not take place on a comprehensive basis, as a detailed assessment is not one of the objectives of this review.

5. Literature Review

The research papers that were finally scoped under the present literature systematic review are summarized in Table 3, illustrating their contributions based on the defined categorization criteria of the review. The table reveals that these research papers span various criteria, indicating a multifaceted nature in their focus and content. This observation underscores the complexity and diversity of the contributions, making it challenging to neatly classify them into discrete categories. The research papers often address multiple aspects, showcasing a detailed and comprehensive exploration of the common denominator of the review, which is blockchain technology. This complexity highlights the richness and interdisciplinary nature of the literature, emphasizing the need for a holistic understanding of the research landscape within the scope of this review.

In the subsequent parts of this section, the focus will be on providing a summary of the various research papers considered within this review, organized based on the proposed types of blockchain technology. This summary aims to distill and highlight the key findings, methodologies, and insights presented in these papers while emphasizing their contributions within the specific contexts of private, public, or consortium blockchain technologies. This categorization allows for a more structured presentation of the literature, offering insights into how different blockchain implementations influence the convergence of CTI and blockchain technology. Despite the diverse nature of the contributions, categorizing them based on blockchain types provides a perspective on the various ways researchers have explored the intersection of CTI and blockchain within distinct blockchain frameworks. This approach enhances the clarity of understanding and enables readers to identify trends and patterns specific to each type of blockchain technology, contributing to a more insightful comprehension of the research landscape within the scope of this review.

The selection of blockchain types plays a pivotal role in shaping the trust and privacy dynamics within CTI and blockchain convergence. Different configurations, whether public, private, or consortium, introduce distinct considerations that shape the collaborative CTI sharing landscape. From a security perspective, the choice of blockchain type directly impacts the level of control and access within the network, influencing the confidentiality and integrity of shared threat intelligence data. Understanding the implications of these technological choices is imperative in establishing robust trust mechanisms and ensuring the privacy and security of sensitive information exchanged within the CTI ecosystem.

Public blockchains are decentralized and open to anyone, allowing universal participation, transaction validation, and ledger maintenance. They operate without a central authority, emphasizing transparency and immutability. In contrast, private blockchains are restricted to authorized entities, providing a controlled environment for transactions and data management, offering heightened privacy and control. Consortium blockchains involve a collaborative effort among a predefined group of participants, combining elements of decentralization with restricted access. Each blockchain type serves distinct purposes—public blockchains prioritize openness, private blockchains prioritize control, and consortium blockchains aim for a balance between collaboration and decentralization. The choice among these blockchain models depends on specific use case requirements, reflecting the diverse landscape of blockchain applications.

5.1. Public Blockchains

Xuan et al. [28] have developed a network threat intelligence sharing platform leveraging blockchain technology. Their experiments demonstrate that this blockchain-based network threat intelligence system can efficiently collect a broader and more extensive range of network data while maintaining security and privacy, while enhancing the overall effectiveness of sharing network threat intelligence data among various organizations.

Gong et al. [29] present a blockchain-based CTI framework aimed at enhancing trust in data sources and content while enabling swift identification and removal of malicious or inaccurate data to resist Sybil attacks. The proposed framework employs a validated procedure facilitated by smart contracts to gather CTI and records metainformation in

a blockchain network, ensuring the validity and reliability of CTI data through source traceability but also offering efficient operation and management of CTI data.

Riesco et al. [30] introduce a model in cybersecurity information exchange, aiming to encourage dynamic information sharing across all participant levels. Their proposal supports the deployment of Dynamic Risk Management frameworks to maintain risks within acceptable levels over time as well as offers unique incentives for sharing, investing, and consuming threat intelligence and risk information. They utilize standards such as Structured Threat Information Exchange and W3C semantic web standards to create a knowledge workspace for behavioral threat intelligence patterns and furthermore, they introduce Ethereum blockchain smart contracts to incentivize knowledge sharing.

Buber et al. [31] outline a decentralized cybersecurity information sharing system leveraging blockchain technology. The system incorporates a controlled decision-making mechanism, authorization termination, and rule-set maintenance to enable distributed decision-making. The decision-making process involves the use of two smart contracts on the blockchain, one for positive votes and the other for negative ones. Members access cyber threat data through company-related queries, facilitating the integration of diverse data sources into a unified cybersecurity management system. The system's design also allows for the collection of real-time cybersecurity data in a single repository, enhancing its utility for implementing real-time cybersecurity applications.

Chatziamanetoglou et al. [32,33] introduce a blockchain-based architecture for managing CTI that encompasses data collection, evaluation, storage, and sharing. This system ensures data integrity and excludes untrustworthy evaluation peers while simultaneously assessing the quality of CTI feeds against defined criteria. The evaluation process employs a reputation and trust-based mechanism, with validators rating CTI feeds based on quality parameters and preserving fairness through the "proof-of-quality" (PoQ) consensus algorithm.

Menges et al. [34] introduce a decentralized platform designed for exchanging threat intelligence information, emphasizing its capability to address legal reporting obligations for security incidents while offering additional incentives for information exchange among involved parties. The evaluation involves implementing the platform using the EOS blockchain and IPFS distributed hash table. The prototype, coupled with cost measurements, showcases the feasibility and cost-efficiency of the presented concept, underscoring the potential practicality of the proposed decentralized threat intelligence exchange system.

Dunnet et al. [35] present an innovative blockchain-based architecture designed to elevate the secure sharing of CTI data. Their framework addresses pivotal challenges related to privacy, trust, and accountability that emerge during the collaborative sharing of CTI among organizations. A notable feature of their approach is the integration of non-interactive zero-knowledge proof functionalities, demonstrating a commitment to underpin data confidentiality and integrity. The overarching goal is to showcase a more effective and efficient approach to CTI sharing, underscoring the potential of their blockchain-based architecture to enable collaborative threat intelligence efforts.

Karatisoglou et al. [36] introduce BRIDGE, an innovative tool that enhances the exchange of intelligence between CTI and cybersecurity professionals. It utilizes the Structured Threat Information eXpression (STIX) standard, leverages blockchain technology, and automates the conversion of intelligence into a format suitable for researchers and professionals, while experimental results show potential for improvements in speed and performance compared to traditional methods.

Ma et al. [37] propose a CTI sharing mechanism based on blockchain, applying game theory principles and smart contracts. Their approach is designed to motivate and promote active participation in CTI sharing, mitigate free-riding behavior among participants, and enhance enthusiasm and efficiency in the sharing process. Moreover, by leveraging blockchain technology, trust among sharing members is increased, while eliminating the need for trusted third parties, and ensuring both security and efficiency in CTI sharing.

Al-Sharu et al. [38] introduce a blockchain-based data sharing approach that focuses on safeguarding the privacy of CTI sharing entities while preventing unauthorized sharing and benefiting legitimate sharing parties. It accomplishes this by creating a comprehensive attack chain using encrypted threat intelligence and leveraging the blockchain's ability to trace back the source of threats in the attack chain. Additionally, smart contracts are employed to automatically send early warning responses to potential attack targets.

5.2. Private Blockchains

Graf et al. [39] introduce an automated system for classifying and managing incident reports to establish cyber situational awareness. It combines a deep autoencoder neural network for classification with blockchain smart contracts for incident management. The system offers real-time solutions, reducing the need for extensive human involvement in cyber incident analysis, focusing on essential information for prompt mitigation.

Zhang et al. [40] introduce an approach to enhance the distribution of intrusion rules in a private blockchain environment. The system utilizes management nodes to consolidate new rules into a designated RuleBlock, which is then broadcasted across the entire network. By updating their local RuleChain with the received RuleBlocks, all nodes swiftly acquire the latest intrusion rules, ensuring rapid dissemination and bolstering the intrusion detection system's ability to promptly detect and respond to emerging threats.

Wu et al. [41] present TITAN, a trust enhancement framework for decentralized sharing, leveraging P2P reputation systems to tackle open trust issues. The design incorporates blockchain and Trusted Execution Environment technologies to guarantee security, integrity, and privacy within the threat intelligence sharing reputation system's operations.

Cha et al. [42] present a blockchain-based architecture for sustainable computing in the context of CTI, addressing issues related to reliability, privacy, scalability, and sustainability. It deals with multiple data feeds to create a reliable dataset, reduce network load, and measure organizations' contributions to encourage participation. Experimental analysis involves measures of reliability, privacy, scalability, and sustainability.

He et al. [43] propose a theoretical and abstract CTI rating and sharing mechanism based on smart contracts. Their blockchain-based threat intelligence system includes a threat intelligence sharing module, using the blockchain to share crucial information among nodes, and a threat intelligence rating module, evaluating and assigning credibility ratings to sources while assessing their contribution rates within the network.

Hajizadeh et al. [44] present a secure distributed model for enabling the sharing of CTI among diverse participants, leveraging blockchain technology to ensure tamper-proof record-keeping and smart contracts for immutable logic. They implement this on the open-source permissioned blockchain platform, Hyperledger Fabric, integrating Software-Defined Networking (SDN) into the sharing platform to enhance defense capabilities against threats within the system.

Preuveneers et al. [45] introduce TATIS, tackling the challenge of mistrust in threat intelligence sources and the information itself by augmenting their security framework. This enhanced framework provides protection for threat intelligence platform APIs, incorporating distributed ledger capabilities to facilitate reliable and trustworthy threat intelligence sharing, along with the ability to audit the provenance of threat intelligence. The feasibility of the distributed framework has been implemented and evaluated on the Malware Information Sharing Platform (MISP) solution, with a performance assessment conducted using real-world open-source threat intelligence feeds.

Badsha et al. [46] introduce BloCyNfo-Share, a blockchain-based privacy-preserving cybersecurity information sharing system employing proxy re-encryption and attribute-based encryption. This framework allows organizations to implement fine-grained access control, delegating access to their cybersecurity information through blockchain technology. The proposed system undergoes privacy and experimental analysis, demonstrating both privacy and efficiency in its model.

Olukoya [47] suggests employing a blockchain ledger to enhance security investigative activities and store associated metadata derived from CTI. They derive cybersecurity incident response requirements by analyzing models from an open-source incident management platform. To validate their approach, they investigate evidence actions in TheHive security incident response platform (SIRP) as a case scenario, demonstrating the feasibility and practicality of their proposed techniques and methods.

Moubarak et al. [48] presented a lightweight CTI sharing platform to visualize security threats in real-time. Their proposal is based on the hyperledger blockchain, smart contracts (chaincodes), and on an embedded Certificate Authority for managing user identities and their corresponding cryptographic materials.

Ali et al. [49,50] introduce a system that ensures privacy and trust through the utilization of distributed ledger technology. The system employs smart contracts for secure decentralized operations and establishes a privacy-preserving ecosystem dedicated to the storage and sharing of threat information related to the MITRE ATT&CK framework.

Pahlevan et al. [51,52] introduce a system for secure and efficient threat information sharing, utilizing the Trusted Automated Exchange of Intelligence Information (TAXII) standard and private blockchain technology. This system automates the threat sharing process, ensuring privacy, data integrity, and interoperability.

Goncalo et al. [53] propose a solution for information credibility in a multi-participant environment through the creation and implementation of a blockchain-based architecture. Participants receive reputation levels to evaluate and authenticate information produced by other actors, and credits are assigned based on the quantity and accuracy of validations. The proposal validates this architecture through a proof-of-concept involving a three-organization scenario, showcasing its applicability and effectiveness in addressing the identified challenges.

Nguyen et al. [54] present a framework that leverages Hyperledger Fabric blockchain and IPFS distributed storage, which is designed to support organizations in meeting their legal reporting requirements and encourages collaborative CTI exchange among ICS stakeholders through the use of discount-based incentives and quality assurance mechanisms, including expert verification. Their proposal ensures confidentiality and privacy for secure, private CTI exchange within sub-groups.

Maina et al. [55] suggest an approach to share CTI by employing Ethereum smart contract blockchain technology. It involves hashing device identities and replacing them with an on-chain verifiable random function, which enhances the privacy and security of participating nodes or financial institutions within the blockchain network while transmitting information.

Sarhan et al. [56] present a hierarchical blockchain-based federated learning framework designed for secure sharing of CTI and intrusion detection heterogeneous data sources and types available at a wide range of IoT endpoints, capable of detecting a wide range of malicious activities while preserving data privacy. They, furthermore, propose the use of blockchain-based smart contracts, which overcomes the problem of limited trust, motivating and assisting the participation of organizations.

Kumar et al. [57] introduce a blockchain-based privacy-preserved threat intelligence framework (P2TIF) designed to safeguard confidential information and identify cyber-threats in Industrial Internet of Things (IIoT) environments, using a deep learning module based on a deep variational autoencoder (DVAE) to transform data and protect against inference attacks. Encoded data are then analyzed by a threat detection system employing an attention-based deep gated recurrent neural network (A-DGRNN) to recognize malicious patterns in IIoT environments.

Shi et al. [58] introduce CITAShare, a threat intelligence sharing model based on the CITA blockchain technology. This model incorporates a distributed architecture database, utilizing a consensus algorithm for data updates and addressing privacy concerns through the implementation of smart contracts. Furthermore, the proposal includes a profit distribu-

tion method based on an improved Shapley value to enhance the motivation of contributors within the threat intelligence sharing process.

5.3. Consortium Blockchains

Homan et al. [59] present a blockchain network model designed to enhance the secure dissemination of CTI data. Their study utilizes a comprehensive testbed built on the Hyperledger Fabric framework and incorporates the STIX 2.0 protocol for standardized CTI data representation. The research validates the effectiveness of the segmentation strategy, which is implemented through smart contracts and Hyperledger Fabric channels. The emphasis lies in overcoming trust barriers and addressing data privacy concerns inherent in the domain of CTI.

Purohit et al. [60,61] developed the DefenseChain platform, which harnesses blockchain technology to offer threat intelligence sharing capabilities for defending against cyber threats. DefenseChain facilitates attack detection and mitigation through distributed trust principles, allowing domains to share threat intelligence in a federation, using a quality-based approach for detection and mitigation considering factors such as accuracy, suspiciousness score, service time, attack type, and recurrence.

Huff et al. [62] propose a distributed ledger to enable the sharing of cybersecurity threat information as a mechanism for non-attributable participation in a threat-sharing community. The participating entities submit monetized threat intelligence data in the form of structured work queries as transactions on the ledger using token-based authentication based on Distributed Anonymous Payment (DAP) schemes in cryptocurrency. Their new anonymous token-based authentication scheme, applied in a permissioned blockchain, allows a consortium of semi-trusted entities to share the workload of managing CTI for the community's benefit.

Mendez et al. [63] focus their research on the Ethereum platform, employing the Proof-of-Authority consensus algorithm. Their approach involves utilizing a distributed data collection method with an abstract data model within a permissioned-based network. The study adopts a perspective aligned with Internet Service Providers (ISPs) and conducts a series of simulations to assess the efficacy of their decentralized framework.

Allouche et al. [64] introduce TRADE, a blockchain-based access control framework designed to facilitate the seamless sharing of threat intelligence across organizational boundaries. Leveraging the power of smart contracts, TRADE offers a mechanism for enforcing sharing policies, enabling organizations to maintain granular control over their sensitive data. The framework not only ensures the preservation of anonymity but also establishes a robust accountability structure within the network, fostering a secure and trust-driven environment for collaborative threat intelligence sharing.

Zhang et al. [65] introduce a blockchain-based CTI model addressing performance issues in terms of speed, scalability, and security. The model combines consortium blockchain and distributed reputation management systems to enable automated analysis and response to tactical threat intelligence. It also presents the "Proof-of Reputation" (PoR) consensus algorithm, which is tailored for CTI sharing and exchange, ensuring transaction efficiency in a credible network environment through a reputation model.

Jiang et al. [66] introduce a novel approach to threat intelligence sharing referred to as BFLS, combining blockchain-based CTI sharing platforms for security and privacy with federated learning technology to enable scalable machine learning applications, specifically for threat detection. This approach allows users to access well-trained threat detection models without the need to transmit personal data, enhancing both security and privacy.

Duy at al. [67] introduce FedChain-Hunter, a threat-hunting framework that combines blockchain and Federated Learning (FL) to collaboratively detect cyber threats while upholding data privacy and transparent data owner contributions. The framework employs Software-Defined Networking (SDN) with adaptable security orchestration to effectively monitor and collect relevant security events. Additionally, it integrates advanced security measures like Fully Homomorphic Encryption (HE) and Differential Privacy (DP) into the

FL scheme, ensuring strong security and privacy preservation during the aggregation of each Machine Learning (ML) model update.

Hosen et al. [68] present a comprehensive framework for Industrial Internet of Things (IIoT) systems, incorporating secure peer-to-peer and group communication in an edge computing environment. This framework integrates a consortium blockchain, an Interplanetary File System (IPFS)-based immutable data storage system, and an intelligent threat detection model, employing a hybrid security scheme that includes modified ECC, PUF, and Lagrange interpolation to ensure secure communications. The modified Proof-of-Vote (PoV) consensus algorithm is utilized to address latency issues during block mining, and the threat intelligence model employs an autoencoder to transform data and an RNN-DL to identify cyber-attacks.

5.4. All Blockchain Types

Dunnett et al. [69] have introduced a blockchain-based CTI sharing framework that facilitates trusted, verifiable, and differential CTI exchange between producers and consumers. The term “differential" pertains to the producer’s capability to manage the extent of information shared with consumers. Within this framework, CTI producers can partition CTI data into distinct groups, each containing sensitive information that can be selectively and differentially shared with CTI consumers.

Bandara [70] introduces Luunu, a CTI sharing platform that leverages blockchain, MISP, Model Cards, and Federated Learning technologies to enhance privacy, transparency, traceability, anonymity, and data provenance in a scalable manner. their proposal incorporates self-sovereign identity (SSI) to ensure participant anonymity within the CTI sharing network. Additionally, a blockchain-based federated learning system is proposed for the collective analysis of CTI data gathered from participating organizations.

Zhang et al. [71] propose a blockchain-enabled Threat Intelligence Integrity Audit (TIIA) scheme for Industrial Internet of Things (IIoT), ensuring the confidentiality of threat intelligence in ciphertext state on the blockchain. The TIIA scheme employs a double-chain structure, utilizing storage and audit chains for storing threat intelligence ciphertext and conducting integrity audits, respectively, with Paillier homomorphic encryption and searchable encryption for confidentiality and ciphertext retrieval. Additionally, a redundant block deletion algorithm is introduced to enhance audit-chain efficiency, and the performance analysis indicates reduced computational and communication costs, affirming the scheme’s effectiveness in maintaining high audit efficiency.

Dunnet et al. [72] introduce a blockchain-based framework for sharing CTI that relies on trustless delegates for making trust-based decisions and decentralizing trust evaluation. This framework uses attribute-based encryption to achieve access control and allows CTI producers to periodically inject false data to monitor delegate behavior, enhancing transparency and accountability. This research demonstrates that the proposed framework is secure against common privacy and trust issues and provides some evidence that the proof-of-concept prototype using Ethereum is both scalable and cost-effective.

Dhifallah et al. [73] propose a solution that integrates blockchain and AI technologies to enhance system efficiency and mitigate vulnerabilities, focusing on countering contamination and evasion attacks on intrusion detection systems (IDSs) using machine learning. Additionally, smart contracts were introduced to protect IDS results against adversarial machine learning attacks in the context of IoT devices, enabling real-time AML detection in data streams.

Mishra [74] proposes a Hybrid Intrusion Detection Tree (HIDT) system, using the machine learning hybrid decision tree method for enhancing anomaly detection accuracy in IoT IDS applications, while incorporating blockchain technology to ensure scalability, reliability, and security. Furthermore, the study evaluates the efficacy of the HIDT model by conducting a performance metric-based comparison with existing approaches.

Table 3. Research papers included in the systematic review according to their characteristics.

#	Ref	RQ1 CTI Lifecycle	RQ2 CTI Level	RQ3 Research Focus	RQ4 Supporting Technology	RQ5 Blockchain Type	RQ6 Implem. Maturity
1	Graf et al. [39] (2018)	Processing	Tactical, Technical	Performance	AI, Smart Contracts	Permissioned, Private	3–4
2	Homan et al. [59] (2019)	Dissemination	All	Trust, Privacy	Hyperledger Fabric, Smart Contracts, STIX 2.0	Permissioned, Consortium	3–4
3	Zhang et al. [40] (2019)	Dissemination	Technical	Performance	IDS	Permissioned, Private	2–3
4	Wu et al. [41] (2019)	Processing, Dissemination	All	Trust, Privacy, Reputation, Quality	TEE	Permissioned, Private	1–2
5	Xuan et al. [28] (2020)	Collection, Dissemination	Technical	Trust, Privacy	Ethereum, Smart Contracts, IPFS	Permissionless, Public	3–4
6	Gong et al. [29] (2020)	Processing, Dissemination	All	Sustainability, Trust	Smart Contracts, Ethereum	Permissionless, Public	2–3
7	Cha et al. [42] (2020)	Collection, Processing, Dissemination	Tactical, Technical	Trust, Privacy, Scalability, Sustainability		Permissioned, Private	2–3
8	He et al. [43] (2020)	Processing, Dissemination	Tactical, Technical	Quality	STIX, Smart Contracts	Permissioned, Private	2–3
9	Hajizadeh et al. [44] (2020)	Collection, Dissemination	Tactical, Technical	Sustainability	Hyperledger Fabric, STIX, SDN	Permissioned, Private	2–3
10	Riesco et al. [30] (2020)	Dissemination	All	Trust, Risk Management	Ethereum, Smart Contracts, STIX, OWL (Web Ontology Language)	Permissionless, Public	3–4
11	Purohit et al. [61] (2020)	Collection, Processing, Dissemination	Operational, Tactical	Quality, Trust	Hyperledger, IPFS, ML	Permissioned, Consortium	3–4
12	Preuveneers et al. [45] (2020)	Processing, Dissemination	Tactical, Technical	Trust, Privacy	Hyperledger Fabric, MISP, API	Permissioned, Private	3–4
13	Badsha et al. [46] (2020)	Dissemination	All	Trust, Privacy	Ethereum, Smart Contracts, Encryption	Permissioned, Private	3–4
14	Buber et al. [31] (2020)	Dissemination	All	Trust, Privacy	Voting Algorithm, CDMM, Smart Contracts	Permissionless, Public	1–2
15	Huff et al. [62] (2021)	Dissemination	Technical, Tactical	Trust	zk–SNARK, DAP, MISP, Sparse Merkle Trees	Permissioned, Consortium	3–4
16	Chatziamanetoglou et al. [33] (2021)	Processing, Dissemination	All	Reputation, Trust, Quality	Consensus Algorithms	Permissionless, Public	2–3
17	Mendez et al. [63] (2021)	Dissemination	Tactical, Technical	Sustainability	Ethereum, Consensus Algorithms	Permissioned, Consortium	3–4
18	Olukoya [47] (2021)	Processing, Dissemination	Tactical, Technical	Sustainability	Hyperledger Fabric, MISP, SIRP	Permissioned, Private	3–4
19	Moubarak et al. [48] (2021)	Dissemination	All	Sustainability	Hyperledger, STIX, Smart Contracts	Permissioned, Private	3–4
20	Ali et al. [49] (2021)	Dissemination	Tactical	Trust, Privacy	Hyperledger, IPFS	Permissioned, Private	1–2
21	Pahlevan et al. [51] (2021)	Dissemination	Tactical	Trust, Privacy	TAXII	Permissioned, Private	2–3

Table 3. *Cont.*

#	Ref	RQ1 CTI Lifecycle	RQ2 CTI Level	RQ3 Research Focus	RQ4 Supporting Technology	RQ5 Blockchain Type	RQ6 Implem. Maturity
22	Allouche et al [64] (2021)	Processing, Dissemination	Tactical, Technical	Trust, Privacy	Smart Contracts, Access Control, TAXII	Permissioned, Consortium	2–3
23	Menges et al. [34] (2021)	Collection, Processing, Dissemination	Tactical, Technical	Trust, Privacy, Quality, Sustainability	EOS, IPFS, Smart Contracts	Permissionless, Public	5–6
24	Goncalo et al. [53] (2021)	Dissemination	Tactical, Technical	Trust, Privacy	Hyperledger Fabric, Smart Contracts	Permissioned, Private	2–3
25	Nguyen et al. [54] (2022)	Direction, Dissemination	All	Trust, Privacy	Hyperledger Fabric, IPFS	Permissioned, Private	2–3
26	Dunnet et al. [35] (2022)	Dissemination	All	Trust, Privacy	Blockchain Agnostic, IPFS, Smart Contracts, NIZKP	Permissionless, Public	2–3
27	Zhang et al. [65] (2022)	Processing, Dissemination	Tactical, Technical	Reputation, Trust, Scalability	Consensus Algorithms, DFA	Permissioned, Consortium	2–3
28	Maina et al. [55] (2022)	Dissemination	Tactical, Technical	Privacy	Ethereum, Smart Contracts	Permissioned, Private	1–2
29	Dunnett et al. [69] (2022)	Processing, Dissemination	All	Trust, Privacy	STIX, Differential Sharing, Ethereum, Smart Contracts	All	3–4
30	Karatisoglou et al. [36] (2022)	Collection, Processing, Dissemination	Tactical, Technical	Sustainability, Performance	STIX, SIGMA	Permissionless, Public	2–3
31	Sarhan et al. [56] (2022)	Dissemination	Tactical, Technical	Privacy, Trust	ML, Smart Contracts, FL	Permissioned, Private	2–3
32	Bandara [70] (2022)	Dissemination	All	Privacy, Trust	FL, MISP, Model Card	All	2–3
33	Kumar et al. [57] (2022)	Processing, Dissemination	All	Privacy, Scalability	Deep Learning, DVAE, A-DGRNN, IPFS, Smart Contracts	Permissioned, Private	3–4
34	Pahlevan et al. [52] (2022)	Dissemination	Tactical	Trust, Privacy	TAXII	Permissioned, Private	2–3
35	Shi et al. [58] (2022)	Dissemination	All	Trust, Privacy	CITA, Hyperledger, Smart Contracts, Shapley	Permissioned, Private	1–2
36	Zhang et al. [71] (2022)	Processing, Dissemination	All	Privacy, Performance	Homomorphic Encryption	All	2–3
37	Ali et al. [50] (2022)	Dissemination	Tactical	Trust, Privacy, Performance	Hyperledger, IPFS	Permissioned, Private	5–6
38	Dunnet et al. [72] (2023)	Dissemination	All	Trust, Privacy	Smart Contracts, Attribute-Based Encryption, Ethereum	All	3–4
39	Ma et al. [37] (2023)	Dissemination	All	Trust	Smart Contracts, Game Theory, Ethereum	Permissionless, Public	2–3
40	Al-Sharu et at. [38] (2023)	Processing, Dissemination	Tactical, Technical	Trust	Smart Contracts, STIX	Permissionless, Public	2–3

Table 3. *Cont.*

#	Ref	RQ1 CTI Lifecycle	RQ2 CTI Level	RQ3 Research Focus	RQ4 Supporting Technology	RQ5 Blockchain Type	RQ6 Implem. Maturity
41	Jiang et al. [66] (2023)	Processing, Dissemination	All	Trust, Privacy	FL,ML, Smart Contracts	Permissioned, Consortium	3–4
42	Chatziamanetoglou et al. [32] (2023)	Processing, Dissemination	All	Reputation, Trust, Quality, Sustainability	Consensus Algorithms	Permissionless, Public	2–3
43	Purohit et al. [60] (2023)	Collection, Processing, Dissemination	Operational, Tactical	Quality, Trust	Hyperledger, IPFS, ML	Permissioned, Consortium	3–4
44	Duy at al. [67] (2023)	Collection, Processing, Dissemination	Tactical, Technical	Privacy, Trust	ML, SDN, ML, HE, Differential Privacy	Permissioned, Consortium	3–4
45	Dhifallah et al. [73] (2023)	Processing, Dissemination	Tactical, Technical	Privacy, Trust	Ethereum, ML, FL, AI	All	2–3
46	Hosen et al. [68] (2023)	Processing, Dissemination	Technical	Privacy, Performance	RNN, DL, IPFS, ECC, PUF	Permissioned, Consortium	3–4
47	Mishra [74] (2023)	Collection, Processing, Dissemination	Technical	Privacy, Reputation	ML, HDT	All	2–3

6. Discussion

In our literature review exploring CTI within the realm of blockchain technology, we have gathered statistical insights on trends in supporting technologies, characteristics, and research approaches. While these statistics offer a glimpse into the landscape, it is important to clarify that they serve as supplementary indicators, not the core focus of this review. Our primary aim is to delve into the broader themes and advancements, also providing relevant background information, while using these statistics as indicative markers to enrich the overall understanding of the intersection between CTI and blockchain technology.

In summary, the comprehensive analysis across these research questions not only shows evolving themes but also underscores the interdisciplinary and interconnected nature of research in CTI based on distributed ledger technologies. The parallel exploration of multiple aspects within individual papers enriches the depth and breadth of understanding in this evolving and complex field. An analytic depiction of the research papers' distributions per research question of this study is shown in Figure 4. The following sections provide a detailed analysis of this review's results with respect to our initial research questions.

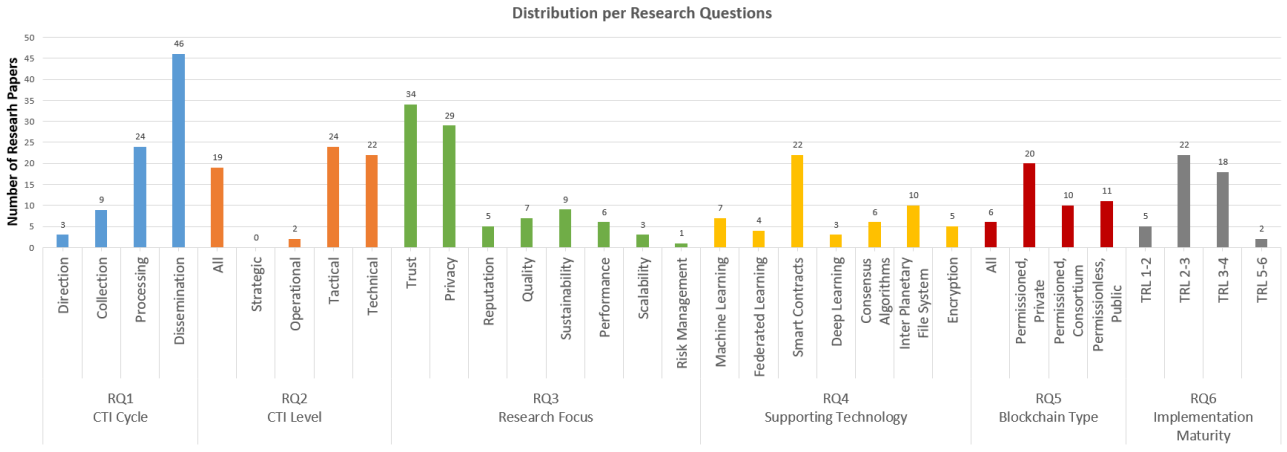

Figure 4. Distribution of research papers by research question.

6.1. RQ1: CTI Lifecycle

In regard to the research question "CTI Lifecycle", it is notable that the *dissemination* phase prominently takes center stage. A substantial emphasis, represented by 46 papers, underscores the significance attributed to the effective communication and sharing of CTI. This trend aligns with the collaborative nature of blockchain technology, where secure and transparent dissemination of intelligence is paramount. The distributed and tamper-resistant nature of blockchain facilitates the creation of a trust-enhanced environment, ensuring that CTI is shared reliably among participants.

Complementing the emphasis on dissemination, the *processing* phase emerges as another focal point within the CTI lifecycle, as evidenced by 24 papers. This observation underscores the importance attached to the analysis and interpretation of intelligence data enabled by blockchain technology. The *processing* phase assumes a pivotal role in enhancing cyber threat detection and response capabilities, emphasizing the relationship between CTI and blockchain technology. Blockchain's ability to maintain an immutable ledger, coupled with its decentralized structure, contributes to the integrity and reliability of the processed intelligence data, reinforcing its role in fortifying cybersecurity measures.

In contrast, the *direction* and *collection* phases of the CTI lifecycle do not emerge as key focal points within the literature. This observation aligns with our expectations, considering the inherent nature of these phases. *Direction* and *collection* involve activities that are often more centralized and unilateral, focusing on the acquisition and orientation of intelligence data. In the collaborative and decentralized paradigm of blockchain technology, these phases may not play as central a role, reflecting the prioritization of shared dissemination and processed analysis in the context of CTI and blockchain convergence.

6.2. RQ2: CTI Level

Concerning the research question "CTI Level", the analysis of the results sheds light on the distribution of emphasis across different levels, with a predominant focus on the *tactical* and *technical* dimensions. Notably, a substantial number of papers refrain from explicitly referencing a specific CTI level. This observation, coupled with an in-depth exploration of the content of these research works, suggests that these proposals hold applicability across the entire spectrum of CTI levels, spanning from the *strategic*, which addresses broader organizational goals, down to the most *technical*, which are concerned with specific threat indicators and vulnerabilities.

The absence of explicit level references in a significant portion of the literature implies a versatility that transcends the conventional delineations of CTI levels. Rather than being confined to a particular layer, these proposals showcase adaptability and relevance throughout the full scope of CTI operations. This flexibility is particularly noteworthy in the context of blockchain technology, where the collaborative and decentralized nature of the platform lends itself to addressing a broad array of CTI challenges at various operational levels.

This diverse coverage not only underscores the adaptability of proposed solutions but also points towards a comprehensive potential for exploration in the integration of CTI and blockchain technology. The holistic coverage across different CTI levels reflects a nuanced understanding of the multifaceted nature of cybersecurity threats and the need for solutions that can address *strategic*, *operational*, and *technical* aspects. It reinforces the notion that the convergence of CTI and blockchain holds promise for providing comprehensive and adaptable solutions that can effectively enhance cybersecurity across a spectrum of organizational requirements and threat landscapes.

6.3. RQ3: Research Focus

In view of the review findings related to the research question "Research Focus", a nuanced landscape emerges within the domain of CTI and blockchain technology convergence. *Trust* emerges as a foundational factor steering collaborative efforts. However, it is essential to acknowledge that while trust might be seen as a primary driver in this

convergence, *privacy* stands as a critical characteristic that such solutions must effectively address. Rather than being a driving force, privacy assumes a pivotal role in shaping the dynamics of CTI and blockchain integration. Blockchain technology, with its decentralized and tamper-resistant ledger, establishes a foundation of trust by offering transparency and immutability in CTI transactions. The cryptographic principles embedded in blockchain contribute to the confidentiality of shared data, ensuring that participants have control over their information and share only what is necessary.

Moreover, the application of *smart contracts* within the blockchain framework introduces an automated mechanism for enforcing privacy rules. By encoding the conditions under which specific threat intelligence data are shared, smart contracts provide an enabling approach to privacy that complements the trust-driven nature of CTI and blockchain convergence.

Selective disclosure mechanisms inherent in blockchain, such as *access controls*, further contribute to privacy considerations, as this is highlighted in [46,58,64,67,72]. This feature allows for the controlled sharing of specific threat intelligence data, aligning with the need for granular control over information dissemination. While trust remains a central theme, the emphasis on privacy is crucial in ensuring that sensitive data are shared judiciously and securely.

Additionally, the dimension of *reputation* plays a pivotal role in enabling trust-based architectures within CTI and blockchain integration [32,33,41,65,74]. Reputation mechanisms within the blockchain ecosystem can enhance the reliability of participants and the information they share. This further fortifies the foundation of trust by introducing a reputational aspect that adds an extra layer of assurance to collaborative efforts in the CTI landscape.

In addition to trust, reputation, and privacy considerations, the *quality* of CTI assumes paramount importance in the overall context of CTI and blockchain integration [32–34,41,43,60,61]. The effectiveness of collaborative efforts hinges on the accuracy, relevance, and timeliness of the intelligence shared. Ensuring high-quality CTI not only enhances the efficacy of threat detection and response but also reinforces the foundation of trust by promoting a shared understanding of the threat landscape. Along with quality, other significant factors that are increasingly explored are the scalability and performance of the proposed solutions [36,39,40,42,50,57,71]. Scalability ensures that the system can accommodate a growing volume of CTI transactions effectively. Performance, on the other hand, is vital for timely and reliable processing of CTI data.

Trust and privacy stand out as predominant themes, with 34 and 29 papers dedicated to these aspects, respectively. The cross-cutting nature of these dimensions is noteworthy, as several papers contribute concurrently to both trust and privacy considerations. This suggests a holistic approach to addressing the fundamental pillars of security and confidentiality within blockchain-based CTI frameworks. In addition, scalability and performance are addressed in nine and six papers respectively, while the enabling factors of reputation and quality are addressed accordingly by five and seven papers, respectively.

6.4. RQ4: Supporting Technology

Examining the findings pertaining to the research question of "Supporting Technology", a multifaceted landscape emerges. The reviewed papers reflect a diversified approach, with various aspects of supporting technologies concurrently contributing to the overarching framework. Notably, smart contracts exhibit prominence, featured in 22 papers, highlighting their pivotal role in enhancing the security and efficiency of CTI processes. Machine learning, with seven papers, and federated learning, with four papers, underscore the significance of advanced analytics and collaborative learning in enabling threat detection capabilities. The utilization of specific consensus algorithms (six papers) emphasizes the need for establishing trust and integrity in a distributed CTI network. The incorporation of the Interplanetary File System (IPFS), addressed in 10 papers, signals a trend toward decentralized and secure storage solutions for large datasets. Moreover, the

modest representation of deep learning (three papers) suggests a nascent exploration of more intricate neural network architectures within the intersection of blockchain and CTI. Finally, the aspects of encryption, mostly homomorphic encryption, introduce a critical dimension, emphasizing the role of secure communication and data protection in the fusion of blockchain and CTI.

This analysis not only sheds light on the prevalence of various supporting technologies but also underscores the interconnected and interdisciplinary nature of research in this evolving field. Smart contracts stand out as integral components, playing a pivotal role in not only enhancing security but also streamlining the processes of CTI operations. Machine learning, along with federated learning, underscores the critical importance of advanced analytics and collaborative learning, enriching the capabilities of threat detection in real time. Specific consensus algorithms contribute to establishing trust and maintaining integrity within the decentralized networks of CTI and blockchain integration. The adoption of the Interplanetary File System (IPFS) reflects a progressive shift towards decentralized and secure storage solutions, crucial for handling the ever-expanding datasets associated with threat intelligence. The modest exploration of deep learning indicates a promising avenue for the development of intricate neural network architectures, potentially advancing the sophistication of threat analysis. Finally, the emphasis on encryption, especially homomorphic encryption, introduces a crucial layer of secure communication and data protection, ensuring the confidentiality, privacy and integrity of shared threat intelligence. Together, these technologies form a robust foundation, enhancing the collaborative, secure, and efficient nature of CTI operations within the dynamic landscape of blockchain technology.

6.5. RQ5: Blockchain Type

It is also imperative to extend our exploration to the usage of different blockchain types in underpinning trust and privacy within the convergence of CTI and blockchain technology, addressing the research question "Blockchain Type", with an observation of the dual focus on permissioned, private, or consortium blockchains (in total 30 papers) and permissionless, public blockchains (11 papers). This reflects a dynamic exploration of different blockchain architectures for CTI applications. The subset of six research papers addressing blockchain technology across all types of blockchain, indicating an abstract approach, emphasizing the importance of a flexible and adaptable approach to blockchain solutions in the cybersecurity domain.

The choice between permissioned and permissionless blockchains, and further classifications into public, private, or consortium models, significantly influences the trust and privacy dynamics in CTI and blockchain integration. Permissioned blockchains, such as private or consortium blockchains, often offer controlled access, making them conducive to fostering trust among known entities. These models, by design, enable more granular control over participant identity, contributing to a heightened sense of trust in the CTI sharing ecosystem.

On the other hand, permissionless blockchains, particularly public models, promote a decentralized approach where participation is open to any entity. While this openness aligns with the principles of transparency, it introduces complexities concerning privacy. Striking a balance between maintaining transparency, a hallmark of trust, and safeguarding sensitive information is a crucial consideration in the context of CTI and blockchain integration.

6.6. RQ6: Implementation Maturity

Expanding the analysis to include the aspects of "Implementation Maturity", viewed through Technology Readiness Levels (TRLs) metrics, adds a layer of insight into the developmental stages of blockchain-based CTI implementations. The distribution across TRLs reveals a notable emphasis on early-to-mid-stages of maturity, with 5 papers falling within TRL 1-2, 22 papers within TRL 2-3, and 18 papers within TRL 3-4. Additionally, there is a modest representation in the more advanced stages, specifically TRL 5-6, with two papers. It is crucial to highlight that the TRL assessment was not conducted systematically

and in depth, serving as a broad indicator rather than an exhaustive analysis. This suggests a need for more comprehensive evaluations in future research to provide a thorough understanding of the maturity trajectories in blockchain-based CTI implementations. The presence of papers across various TRLs hints at an evolving landscape, signaling potential advancements in maturity levels as the field continues to progress.

7. Study Limitations

This systematic review carries certain limitations, primarily tied to the maturity of existing publications and the specific search engine employed for publication retrieval. Our reliance on Scopus, a robust scientific literature indexing system encompassing major digital libraries like Elsevier, Springer, ACM, IEEE, and MDPI, was our choice to ensure a comprehensive coverage of scholarly work. However, it is important to acknowledge that this decision inherently limits the review to the maturity and depth of publications available within the selected databases.

Furthermore, the scope of our study focused solely on the scientific literature, excluding the exploration of the gray literature and real-world implementations. This deliberate exclusion was a decision made in alignment with the study's overarching objectives, emphasizing only a thorough examination of scholarly contributions and insights. While this approach ensures a rigorous analysis of theoretical and academic perspectives, it may overlook valuable insights and experiences found in the gray literature or practical, real-world scenarios. It is essential for readers to be mindful of these constraints when interpreting the findings, recognizing that the study's design reflects a deliberate choice in pursuit of specific research goals.

8. Threats to Validity

As we delve into the convergence of CTI and blockchain technology in this systematic literature review, it is essential to acknowledge the dynamic and multifaceted nature of this evolving field. While our analysis has highlighted critical insights into recent advancements, emerging trends, and the interconnected nature of CTI and blockchain, it is crucial to recognize potential threats to the validity of our conclusions.

One potential threat to validity lies in the generalization of our conclusions. The reviewed literature primarily focuses on recent advancements and emerging trends, and the rapidly evolving nature of both CTI and blockchain technology may introduce variability over time. Additionally, the diverse methodologies employed across the reviewed papers could contribute to variations in results and interpretations.

Another consideration is the potential publication bias within the literature review. The inclusion of published papers may lead to an overemphasis on positive results or successful implementations, potentially neglecting negative outcomes or unsuccessful applications of CTI and blockchain convergence. Addressing this bias ensures a more balanced representation of the field.

Moreover, the evolving landscape of blockchain technology and the diverse use cases within CTI introduce complexities that might not be fully captured in the current literature. As these technologies continue to advance, new developments may challenge the relevance and completeness of our findings.

To mitigate the potential threat related to generalization, future research efforts should consider incorporating longitudinal studies that track the evolution of CTI and blockchain technology over time, using the presented research questions or even an evolution of them. This approach would enable a more comprehensive understanding of trends and variations through the progress of time, offering insights into the persistence or transformation of the research field.

To address potential publication bias, researchers can actively seek out and include implementation results, white papers, study cases, and even negative results. This inclusive approach ensures a more accurate and unbiased portrayal of the challenges and limitations associated with the convergence of CTI and blockchain. Moreover, researchers can synthe-

size results across studies while accounting for methodological variations. This method enhances the robustness of conclusions by identifying patterns and trends that transcend individual study nuances.

Considering the evolving landscape of blockchain technology and the dynamic nature of CTI, researchers should establish a framework for continuous monitoring and updates. Regularly revisiting the recent literature, while incorporating the latest developments, ensures that the findings remain relevant and reflective of the current state of the field.

9. Conclusions

This systematic literature review provides a comprehensive analysis of the convergence between CTI and blockchain technology. Examining key research questions related to the CTI lifecycle, CTI level, CTI research area focus, supporting technology, blockchain type, and implementation maturity, this review unveils the interconnected nature of this evolving field. Trust and reputation emerge as driving forces essential for underpinning the privacy of CTI data. This study emphasizes the significance of factors such as CTI data quality, scalability, and performance in ensuring timely, reliable, and actionable threat intelligence. Notably, permissioned and private blockchain schemas are favored, as well as the usage of permissionless and public schemas with the required access control mechanisms to ensure security and confidentiality, reflecting a dynamic exploration of diverse blockchain architectures for CTI applications.

The future convergence of CTI and blockchain technology is the subject of steadily growing significant advancements, with several key trajectories shaping the landscape. Interoperability standards are anticipated to play a significant role, enabling seamless data exchange across diverse blockchain implementations. Establishing common frameworks will foster a more collaborative cybersecurity ecosystem, enhancing the effectiveness of threat intelligence sharing. Privacy preservation is expected to evolve through the integration of advanced cryptographic techniques within blockchain frameworks. Innovations like zero-knowledge proofs and differential privacy are already being explored, elevating the confidentiality and protection of sensitive CTI data.

Furthermore, the integration of CTI and blockchain with emerging technologies holds considerable promise. The incorporation of quantum computing, artificial intelligence, and edge computing could revolutionize threat analysis, introducing unprecedented speed, security, performance, scalability, accuracy, and quality. These synergies would empower cybersecurity efforts to adapt more effectively to the dynamic and sophisticated nature of evolving cyber threats. Additionally, decentralized threat intelligence marketplaces may emerge, leveraging blockchain's capabilities to facilitate secure and automated transactions through smart contracts. This could redefine how organizations acquire and exchange threat intelligence, promoting efficiency, transparency, and trust in the process.

In addition, we highlight the importance of an alternate angle, focusing on the need for a more in-depth exploration of the specific impact on distinct security team roles, including Security Analysts, Security Operations Center (SOC) teams, Computer Security Incident Response Teams (CSIRTs), and Executive Management. Further scientific inquiry could be directed towards comprehensively understanding how the integration of CTI and blockchain shapes the unique interests, requirements, and responsibilities inherent to the aforementioned roles within the domain of cybersecurity operations, enhancing the applicability and relevance of our findings, ensuring a more tailored and effective implementation across a spectrum of organizational contexts.

In conclusion, the future of CTI and blockchain convergence is characterized by the pursuit of interoperability, enhanced privacy techniques, and the integration of cutting-edge technologies to preserve trust, which is one of the fundamental aspects of the domain. These developments underpin the landscape of cybersecurity, introducing new dimensions of collaboration, security, and efficiency in the face of an ever-evolving threat landscape.

Author Contributions: Conceptualization, D.C. and K.R.; methodology, K.R. and D.C.; validation, K.R. and D.C.; formal analysis, D.C.; investigation, D.C.; data curation, D.C. and K.R.; writing—original draft preparation, D.C.; writing—review and editing, K.R.; visualization, D.C. and K.R.; supervision, K.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are derived from publicly available research papers.

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

References

1. Johnson, C.; Badger, L.; Waltermire, D.; Snyder, J.; Skorupka, C. *Guide to Cyber Threat Information Sharing*; NIST Special Publication 800-150; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2016.
2. ENISA. *ENISA Threat Landscape 2023*; Technical Report; ENISA: Athens, Greece, 2023.
3. Brown, R.; Nickels, K. *2023 SANS Cyber Threat Intelligence (CTI) Survey*; Technical Report; SANS Institute: North Bethesda, MD, USA, 2023.
4. Saeed, S.; Suayyid, S.A.; Al-Ghamdi, M.S.; Al-Muhaisen, H.; Almuhaideb, A.M. A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. *Sensors* **2023**, *23*, 7273. [CrossRef] [PubMed]
5. Sun, N.; Ding, M.; Jiang, J.; Xu, W.; Mo, X.; Tai, Y.; Zhang, J. Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives. *IEEE Commun. Surv. Tutorials* **2023**, *25*, 1748–1774. [CrossRef]
6. Li, X.; Cheng, J.; Shi, Z.; Liu, J.; Zhang, B.; Xu, X.; Tang, X.; Sheng, V.S. Blockchain Security Threats and Collaborative Defense: A Literature Review. *Comput. Mater. Contin.* **2023**, *76*, 2597–2629. [CrossRef]
7. Saxena, R.; Gayathri, E.; Surya Kumari, L. Semantic analysis of blockchain intelligence with proposed agenda for future issues. *Int. J. Syst. Assur. Eng. Manag.* **2023**, *14*, 34–54. [CrossRef]
8. Saeed, S.; Altamimi, S.A.; Alkayyal, N.A.; Alshehri, E.; Alabbad, D.A. Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors* **2023**, *23*, 6666. [CrossRef] [PubMed]
9. El-Kosairy, A.; Abdelbaki, N.; Aslan, H. A survey on cyber threat intelligence sharing based on Blockchain. *Adv. Comput. Intell.* **2023**, *3*, 10. [CrossRef]
10. Dunnett, K.; Pal, S.; Jadidi, Z., Challenges and Opportunities of Blockchain for Cyber Threat Intelligence Sharing. In *Secure and Trusted Cyber Physical Systems: Recent Approaches and Future Directions*; Pal, S., Jadidi, Z., Foo, E., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 1–24. [CrossRef]
11. Saxena, R.; Gayathri, E. Cyber threat intelligence challenges: Leveraging blockchain intelligence with possible solution. *Mater. Today Proc.* **2022**, *51*, 682–689. [CrossRef]
12. Ainslie, S.; Thompson, D.; Maynard, S.; Ahmad, A. Cyber-Threat Intelligence for Security Decision-Making: A Review and Research Agenda for Practice. *Comput. Secur.* **2023**, *132*, 103352. [CrossRef]
13. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Keele University: Newcastle, UK, 2007.
14. Fink, A. *Conducting Research Literature Reviews: From the Internet to Paper*; Sage Publications: Los Angeles, CA, USA, 2019.
15. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G.; PRISMA Group. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *Ann. Intern. Med.* **2009**, *151*, 264–269. [CrossRef]
16. Boland, A.; Dickson, R.; Cherry, G. *Doing a Systematic Review: A Student's Guide*; Sage Publications: London, UK, 2017; pp. 1–304.
17. Sakellariou, G.; Fouliras, P.; Mavridis, I.; Sarigiannidis, P. A reference model for cyber threat intelligence (CTI) systems. *Electronics* **2022**, *11*, 1401. [CrossRef]
18. Chismon, D.; Ruks, M. *Threat Intelligence: Collecting, Analysing, Evaluating*; MWR InfoSecurity Ltd.: Basingstoke, UK, 2015; Volume 3, pp. 36–42.
19. Montasari, R.; Carroll, F.; Macdonald, S.; Jahankhani, H.; Hosseinian-Far, A.; Daneshkhah, A. Application of artificial intelligence and machine learning in producing actionable cyber threat intelligence. In *Digital Forensic Investigation of Internet of Things (IoT) Devices*; Springer: Cham, Switzerland, 2021; pp. 47–64.
20. Tounsi, W.; Rais, H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Comput. Secur.* **2018**, *72*, 212–233. [CrossRef]
21. Wagner, T.D.; Mahbub, K.; Palomar, E.; Abdallah, A.E. Cyber threat intelligence sharing: Survey and research directions. *Comput. Secur.* **2019**, *87*, 101589. [CrossRef]
22. Asante, M.; Epiphaniou, G.; Maple, C.; Al-Khateeb, H.; Bottarelli, M.; Ghafoor, K.Z. Distributed ledger technologies in supply chain security management: A comprehensive survey. *IEEE Trans. Eng. Manag.* **2021**, *70*, 713–739. [CrossRef]
23. Girdhar, K.; Singh, C.; Kumar, Y. AI and Blockchain for Cybersecurity in Cyber-Physical Systems: Challenges and Future Research Agenda. In *Blockchain for Cybersecurity in Cyber-Physical Systems*; Springer: Cham, Switzerland, 2023; pp. 185–213.

24. Dutta, A.; Kant, S. An overview of cyber threat intelligence platform and role of artificial intelligence and machine learning. In Proceedings of the Information Systems Security: 16th International Conference, ICISS 2020, Jammu, India, 16–20 December 2020; pp. 81–86.
25. Sarhan, M.; Layeghy, S.; Moustafa, N.; Portmann, M. Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection. *J. Netw. Syst. Manag.* **2023**, *31*, 3. [CrossRef]
26. Liu, Y.; Lu, Q.; Zhu, L.; Paik, H.Y.; Staples, M. A systematic literature review on blockchain governance. *J. Syst. Softw.* **2023**, *197*, 111576. [CrossRef]
27. Mankins, J.C. *Technology Readiness Levels, White Paper*; Space Propulsion Synergy Team: Seal Beach, CA, USA, 1995; Volume 6.
28. Xuan, S.; Tang, H.; Wang, W.; Yang, W. Application of Block Chain Technology in Constructing Network Threat Intelligence System. In Proceedings of the 2020 the 2nd International Conference on Blockchain Technology, Hilo, HI, USA, 12–14 March 2020; pp. 144–149.
29. Gong, S.; Lee, C. Blocis: Blockchain-based cyber threat intelligence sharing framework for sybil-resistance. *Electronics* **2020**, *9*, 521. [CrossRef]
30. Riesco, R.; Larriva-Novo, X.; Villagrá, V.A. Cybersecurity threat intelligence knowledge exchange based on blockchain: Proposal of a new incentive model based on blockchain and Smart contracts to foster the cyber threat and risk intelligence exchange of information. *Telecommun. Syst.* **2020**, *73*, 259–288. [CrossRef]
31. Büber, E.; Şahingöz, Ö.K. Blockchain based information sharing mechanism for cyber threat intelligence. *Balk. J. Electr. Comput. Eng.* **2020**, *8*, 242–253. [CrossRef]
32. Chatziamanetoglou, D.; Rantos, K. Blockchain-Based Cyber Threat Intelligence Sharing Using Proof-of-Quality Consensus. *Secur. Commun. Netw.* **2023**, *2023*, 3303122. [CrossRef]
33. Chatziamanetoglou, D.; Rantos, K. CTI blockchain-based sharing using Proof-of-Quality consensus algorithm. In Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 26–28 July 2021; pp. 331–336.
34. Menges, F.; Putz, B.; Pernul, G. DEALER: Decentralized incentives for threat intelligence reporting and exchange. *Int. J. Inf. Secur.* **2021**, *20*, 741–761. [CrossRef]
35. Dunnett, K.; Pal, S.; Jadidi, Z.; Putra, G.D.; Jurdak, R. A Democratically Anonymous and Trusted Architecture for CTI Sharing using Blockchain. In Proceedings of the 2022 International Conference on Computer Communications and Networks (ICCCN), Honolulu, HI, USA, 25–28 July 2022; pp. 1–7.
36. Karatisoglou, M.; Farao, A.; Bolgouras, V.; Xenakis, C. BRIDGE: BRIDGing the gap bEtween CTI production and consumption. In Proceedings of the 2022 14th International Conference on Communications (COMM), Bucharest, Romania, 16–18 June 2022; pp. 1–6.
37. Ma, X.; Yu, D.; Du, Y.; Li, L.; Ni, W.; Lv, H. A Blockchain-Based Incentive Mechanism for Sharing Cyber Threat Intelligence. *Electronics* **2023**, *12*, 2454. [CrossRef]
38. Al-Sharu, W.N.; Qabalin, M.K.; Naser, M.; Saraerh, O.A. A secure framework for blockchain transactions protection. *Comput. Syst. Sci. Eng.* **2023**, *45*, 1095–1111. [CrossRef]
39. Graf, R.; King, R. Neural network and blockchain based technique for cyber threat intelligence and situational awareness. In Proceedings of the 2018 10th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 29 May–1 June 2018; pp. 409–426.
40. Zhang, F.; Li, W.; Li, T.; Wang, Y.; Li, Z. RuleChain: A Novel Intrusion Rules Distribution Method Based on Blockchain. In Proceedings of the 2019 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 5–7 December 2019; pp. 60–66.
41. Wu, Y.; Qiao, Y.; Ye, Y.; Lee, B. Towards improved trust in threat intelligence sharing using blockchain and trusted computing. In Proceedings of the 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Granada, Spain, 22–25 October 2019; pp. 474–481.
42. Cha, J.; Singh, S.K.; Pan, Y.; Park, J.H. Blockchain-based cyber threat intelligence system architecture for sustainable computing. *Sustainability* **2020**, *12*, 6401. [CrossRef]
43. He, S.; Fu, J.; Jiang, W.; Cheng, Y.; Chen, J.; Guo, Z. BloTISRT: Blockchain-based threat intelligence sharing and rating technology. In Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies, Guangzhou, China, 4–6 December 2020; pp. 524–534.
44. Hajizadeh, M.; Afraz, N.; Ruffini, M.; Bauschert, T. Collaborative cyber attack defense in SDN networks using blockchain technology. In Proceedings of the 2020 6th IEEE Conference on Network Softwarization (NetSoft), Ghent, Belgium, 29 June–3 July 2020; pp. 487–492.
45. Preuveneers, D.; Joosen, W.; Bernal Bernabe, J.; Skarmeta, A. Distributed security framework for reliable threat intelligence sharing. *Secur. Commun. Netw.* **2020**, *2020*, 8833765. [CrossRef]
46. Badsha, S.; Vakilinia, I.; Sengupta, S. Blocynfo-share: Blockchain based cybersecurity information sharing with fine grained access control. In Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 January 2020; pp. 0317–0323.
47. Olukoya, O. Distilling blockchain requirements for digital investigation platforms. *J. Inf. Secur. Appl.* **2021**, *62*, 102969. [CrossRef]

48. Moubarak, J.; Bassil, C.; Antoun, J. On the dissemination of cyber threat intelligence through hyperledger. In Proceedings of the 2021 17th International Conference on the Design of Reliable Communication Networks (DRCN), Milano, Italy, 19–22 April 2021; pp. 1–6.
49. Ali, H.; Papadopoulos, P.; Ahmad, J.; Pitropakis, N.; Jaroucheh, Z.; Buchanan, W.J. Privacy-preserving and Trusted Threat Intelligence Sharing using Distributed Ledgers. In Proceedings of the 2021 14th International Conference on Security of Information and Networks (SIN), Edinburgh, UK, 15–17 December 2021; Volume 1, pp. 1–6.
50. Ali, H.; Ahmad, J.; Jaroucheh, Z.; Papadopoulos, P.; Pitropakis, N.; Lo, O.; Abramson, W.; Buchanan, W.J. Trusted Threat Intelligence Sharing in Practice and Performance Benchmarking through the Hyperledger Fabric Platform. *Entropy* **2022**, *24*, 1379. [CrossRef]
51. Pahlevan, M.; Voulkidis, A.; Velivassaki, T.H. Secure exchange of cyber threat intelligence using TAXII and distributed ledger technologies-application for electrical power and energy system. In Proceedings of the 16th International Conference on Availability, Reliability and Security, Vienna, Austria, 17–20 August 2021; pp. 1–8.
52. Pahlevan, M.; Ionita, V. Secure and Efficient Exchange of Threat Information Using Blockchain Technology. *Information* **2022**, *13*, 463. [CrossRef]
53. Gonçalo, R.; Pedrosa, T.; Lopes, R.P. An architecture for sharing cyber-intelligence based on blockchain. In Proceedings of the Blockchain and Applications: 2nd International Congress, L'Aquila, Italy, 17–19 June 2020; pp. 71–80.
54. Nguyen, K.; Pal, S.; Jadidi, Z.; Dorri, A.; Jurdak, R. A blockchain-enabled incentivised framework for cyber threat intelligence sharing in ics. In Proceedings of the 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), Pisa, Italy, 21–25 March 2022; pp. 261–266.
55. Maina, W.; Nderu, L.; Mwalili, T. A Smart Contract Approach to Cyber Threat Intelligence Sharing in Kenya. In Proceedings of the 2022 IST-Africa Conference (IST-Africa), Virtual Conference, 16–20 May 2022; pp. 1–10.
56. Sarhan, M.; Lo, W.W.; Layeghy, S.; Portmann, M. HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection. *Comput. Electr. Eng.* **2022**, *103*, 108379. [CrossRef]
57. Kumar, P.; Kumar, R.; Gupta, G.P.; Tripathi, R.; Srivastava, G. P2tif: A blockchain and deep learning framework for privacy-preserved threat intelligence in industrial iot. *IEEE Trans. Ind. Inform.* **2022**, *18*, 6358–6367. [CrossRef]
58. Shi, H.; Wang, W.; Liu, L.; Lin, Y.; Liu, P.; Xie, W.; Wang, H.; Zhang, Y. Threat intelligence sharing model and profit distribution based on blockchain and smart contracts. In Proceedings of the 11th International Conference on Computer Engineering and Networks, Beijing, China, 9–11 December 2022; pp. 645–654.
59. Homan, D.; Shiel, I.; Thorpe, C. A new network model for cyber threat intelligence sharing using blockchain technology. In Proceedings of the 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Canary Islands, Spain, 24–26 June 2019; pp. 1–6.
60. Purohit, S.; Neupane, R.; Bhamidipati, N.R.; Vakkavanthula, V.; Wang, S.; Rockey, M.; Calyam, P. Cyber threat intelligence sharing for co-operative defense in multi-domain entities. *IEEE Trans. Dependable Secur. Comput.* **2023**, *20*, 4273–4290. [CrossRef]
61. Purohit, S.; Calyam, P.; Wang, S.; Yempalla, R.; Varghese, J. DefenseChain: Consortium blockchain for cyber threat intelligence sharing and defense. In Proceedings of the 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 28–30 September 2020; pp. 112–119.
62. Huff, P.; Li, Q. A distributed ledger for non-attributable cyber threat intelligence exchange. In Proceedings of the Security and Privacy in Communication Networks: 17th EAI International Conference, SecureComm 2021, Virtual Event, 6–9 September 2021; pp. 164–184.
63. Mendez Mena, D.; Yang, B. Decentralized actionable cyber threat intelligence for networks and the internet of things. *IoT* **2020**, *2*, 1–16. [CrossRef]
64. Allouche, Y.; Tapas, N.; Longo, F.; Shabtai, A.; Wolfsthal, Y. Trade: Trusted anonymous data exchange: Threat sharing using blockchain technology. *arXiv* **2021**, arXiv:2103.13158.
65. Zhang, X.; Miao, X.; Xue, M. A Reputation-Based Approach Using Consortium Blockchain for Cyber Threat Intelligence Sharing. *Secur. Commun. Netw.* **2022**, *2022*, 7760509. [CrossRef]
66. Jiang, T.; Shen, G.; Guo, C.; Cui, Y.; Xie, B. BFLS: Blockchain and Federated Learning for sharing threat detection models as Cyber Threat Intelligence. *Comput. Netw.* **2023**, *224*, 109604. [CrossRef]
67. Duy, P.T.; Quyen, N.H.; Khoa, N.H.; Tran, T.D.; Pham, V.H. FedChain-Hunter: A reliable and privacy-preserving aggregation for federated threat hunting framework in SDN-based IIoT. *Internet Things* **2023**, *24*, 100966. [CrossRef]
68. Hosen, A.S.; Sharma, P.K.; Puthal, D.; Ra, I.H.; Cho, G.H. SECBlock-IIoT: A Secure Blockchain-enabled Edge Computing Framework for Industrial Internet of Things. In Proceedings of the Third International Symposium on Advanced Security on Software and Systems, Melbourne, Australia, 10–14 July 2023; pp. 1–14.
69. Dunnett, K.; Pal, S.; Putra, G.D.; Jadidi, Z.; Jurdak, R. A Trusted, Verifiable and Differential Cyber Threat Intelligence Sharing Framework using Blockchain. In Proceedings of the 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Wuhan, China, 9–11 December 2022; pp. 1107–1114.
70. Bandara, E.; Shetty, S.; Mukkamala, R.; Rahaman, A.; Liang, X. LUUNU—Blockchain, MISP, Model Cards and Federated Learning Enabled Cyber Threat Intelligence Sharing Platform. In Proceedings of the 2022 Annual Modeling and Simulation Conference (ANNSIM), San Diego, CA, USA, 18–20 July 2022; pp. 235–245.

71. Zhang, W.; Bai, Y.; Feng, J. TIIA: A blockchain-enabled threat intelligence integrity audit scheme for IIoT. *Future Gener. Comput. Syst.* **2022**, *132*, 254–265. [CrossRef]
72. Dunnett, K.; Pal, S.; Jadidi, Z.; Jurdak, R. A Blockchain-Based Framework for Scalable and Trustless Delegation of Cyber Threat Intelligence. In Proceedings of the 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Dubai, United Arab Emirates, 1–5 May 2023; pp. 1–9.
73. Dhifallah, W.; Moulahi, T.; Tarhouni, M.; Zidi, S. Intellig_block: Enhancing IoT security with blockchain-based adversarial machine learning protection. *Int. J. Adv. Technol. Eng. Explor.* **2023**, *10*, 1167–1183.
74. Mishra, S. Blockchain and Machine Learning-Based Hybrid IDS to Protect Smart Networks and Preserve Privacy. *Electronics* **2023**, *12*, 3524. [CrossRef]