

Review

Supply Chain Disruption Risk Management with Blockchain: A Dynamic Literature Review

Niloofer Etemadi ^{1,*}, Yari Borbon-Galvez ^{1,2}, Fernanda Strozzi ¹ and Tahereh Etemadi ³

¹ Centro Sulla Logistica e il Supply Chain Management, LIUC Università Carlo Cattaneo, 21053 Castellanza, Italy; yborbon@liuc.it (Y.B.-G.); fstrozzi@liuc.it (F.S.)

² Department of Transport and Regional Economics, University of Antwerp, 2000 Antwerpen, Belgium

³ Department of Computer Engineering, Mazandaran Institute of Technology, Babol 734, Iran; etemadi.ta@gmail.com

* Correspondence: netemadi@liuc.it

Abstract: The purpose of this review is to describe the landscape of scientific literature enriched by an author's keyword analysis to develop and test blockchain's capabilities for enhancing supply chain resilience in times of increased risk and uncertainty. This review adopts a dynamic quantitative bibliometric method called systematic literature network analysis (SLNA) to extract and analyze the papers. The procedure consists of two methods: a systematic literature review (SLR) and bibliometric network analysis (BNA). This paper provides an important contribution to the literature in applying blockchain as a key component of cyber supply chain risk management (CSR), manage and predict disruption risks that lead to resilience and robustness of the supply chain. This systematic review also sheds light on different research areas such as the potential of blockchain for privacy and security challenges, security of smart contracts, monitoring counterfeiting, and traceability database systems to ensure food safety and security.

Keywords: blockchain technology; cyber risks; supply chain disruptions; supply chain management; resilience; systematic literature review



Citation: Etemadi, N.; Borbon-Galvez, Y.; Strozzi, F.; Etemadi, T. Supply Chain Disruption Risk Management with Blockchain: A Dynamic Literature Review. *Information* **2021**, *12*, 70. <https://doi.org/10.3390/info12020070>

Academic Editor: Nelly Leligou
Received: 6 November 2020
Accepted: 4 February 2021
Published: 7 February 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Disruption has always existed in the supply chain even before the term supply chain management (SCM) became part of our world. Disruptions have evolved over centuries from supply chain disruptions due to ecosystem changes, business model transformation, to cyberattacks by emerging technologies. (Deloitte). The fragility of international supply chains is increasing due to disruption risks that directly or indirectly endanger the stability and security of society. As an example, the spread of COVID-19 around the world has affected the movement of people and materials globally. The resulting supply chain disruptions have led to delivery delays and shortages of products and items. Simultaneously, requests for specific items utilized for epidemic control have increased dramatically, and the forecasting of demand patterns for many consumer goods has become more challenging. After the disruptions caused by the need to control the spread of the virus, the biggest challenge facing companies is restarting their supply chains. Of the many different types of risk involved in supply chain disruptions, those related to cyberattacks have gained the attention of the research community over recent years. The vulnerability of the supply chain is evidenced by cyber-attacks, for example, companies engaged in counterfeiting, theft, fraud, data manipulation, or falsification. As an example of a cybersecurity breach [1], reported Stuxnet computer worm externally taking control of Iran's Natanz uranium enrichment plant's controllers in November 2010. As stated by [2], "A cyber—event is any disturbance to this interdependent network that leads to loss of functionality, connectivity, or capacity" [2]. Based on another definition by [3], "Cyber risk is an issue that exists at the intersection of business risk, regulation, and technology". Deloitte reported that the

potential consequences of cyber-incidents are varied from massive financial losses due to operational disruptions and regulatory fines, to intangible expenditures, for instance, the loss of the customer and loss of reputation of the company. Over the past decades, our knowledge and awareness of supply chain risk management (SCRM) have been extended; with the advent of digitalization and data analytics, companies have acquired significant capabilities for providing complete solutions in SCRM. Digitalization as a part of the Industry 4.0 revolution can enable real-time SCRM and enhance collaboration, communication, and trust among supply chain parties because of real-time information sharing and improving the integration of systems and processes [4]. However, these new technologies come with new disruptions to productivity or operations, such as malicious electronic event threatening the safety of goods, the trust of customers, the brand image of companies, or a weakened market position [3]. In this vein, as a potential solution to mitigate the above-mentioned issues, academic institutions and practitioners have recently conducted several theoretical and practical projects with blockchain technology for preserving the integrity of data and systems, transparency, safety, and security [5,6].

Blockchain technology is a novel technology that has been promoted in recent years and which has a potential benefit for exploring and controlling supply chain risks. “The blockchain is a new organizing paradigm for the discovery, valuation, and transfer of all quanta (discrete units) of anything, and potentially for the coordination of all human activity on a much larger scale than has been possible before” [7]. Moreover, blockchain technology applied to the supply chain seems to be an interesting research stream for future studies, especially in the era of cybersecurity [8,9]. Although some reviews analyzed the current applications of blockchain in the supply chain, there is still a need for clarity about whether blockchain and emerging technologies can manage and predict disruptions and lead to more resilience and robustness of the supply chain, and about how these technologies can play a crucial role in privacy and security challenges, the implementation of smart contracts, monitoring counterfeiting, and tracking and tracing to ensure food safety and security.

Following on from the above discussion, this study will attempt to advance the understanding by gathering information from a literature review using bibliometric tools, namely, the analysis of the citation network and the analysis of the authors’ keywords co-occurrence network. These tools are quantitative-based methods that have been used to analyze literature in several contexts, such as supply chain, smart factory, and blockchain [10–12]. This widespread use shows their importance in describing the evolutionary trajectory and main streams of a topic in a more objective method than traditional descriptive reviews [10] and proposes the most interesting research directions for the future. The rest of the paper is structured as follows: In Section 2, study material and methods are discussed, while Section 3 is devoted to the results of the first phase of SLNA methodology with the results of SLR. Section 4 contains the results of the second phase, comprising the citation network, Louvain community analysis, main path extraction, Global citation score, and co-occurrence of author keywords. Discussion of findings and future research directions are presented in Section 6, while the article concludes with conclusions in Section 7.

2. Materials and Methods

A systematic literature review analysis (SLNA) was chosen to extract and analyze the papers. The procedure was of two stages: a systematic literature review (SLR) and bibliometric network analysis (BNA). The process of SLNA consisted of two stages, as shown in Figure 1.

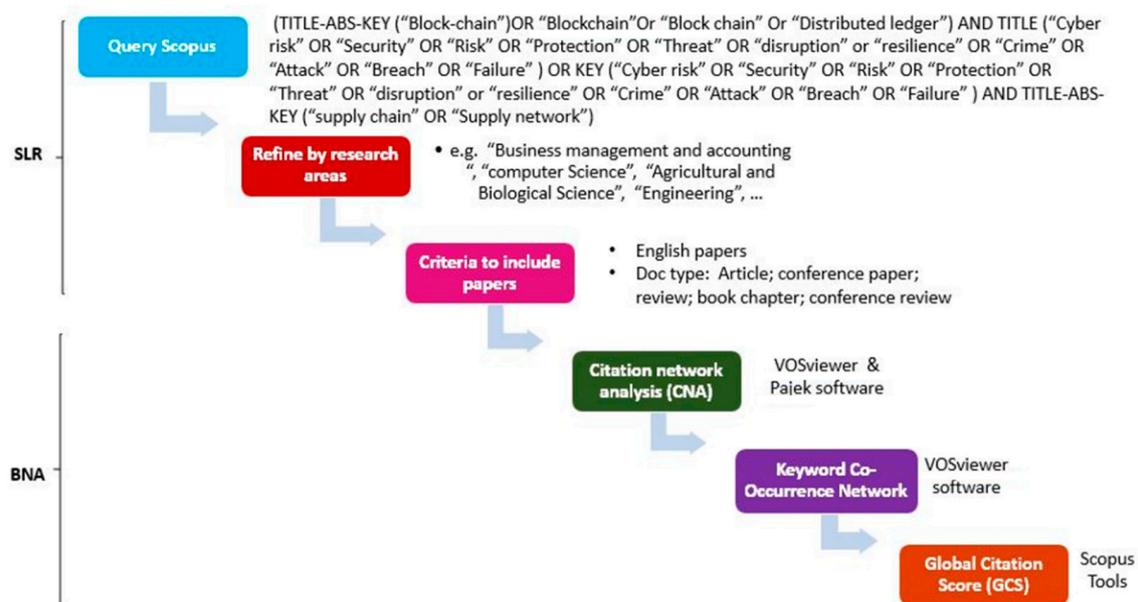


Figure 1. Systematic literature network analysis (SLNA).

In the first phase, SLR can be defined as “a specific methodology that locates existing studies, selects and evaluates contributions, analyses and synthesizes data” [13].

It was conducted through three steps, which defined the scope of the analysis to have a niche for the literature review. Second, the literature was located by tools of identified keywords, time of the retrieved papers, language, and document type in Scopus. Third, a literature selection was carried out, based on explicit criteria to include and exclude papers, which will form the input for the second phase (BNA). The BNA phase implies a bibliographic network analysis and visualization, which in this paper produces a citation network, a global citation score, and a keywords co-occurrence network.

The building networks were the product of the software VoSviewer (<https://www.vosviewer.com/> (accessed on 7 February 2021)), which was used to create bibliometric networks, and, in this study, this software was applied to study author keywords analysis [14]. Pajek [15] is another software for social network analysis (<http://mrvar.fdv.uni-lj.si/pajek/> (accessed on 7 February 2021)), and in this study, it was applied for creating, visualizing, and exploring citation networks following the method proposed by [16].

As a result, a dataset of selected papers was collected to construct an exhaustive literature review in the area of blockchain implications in managing cyber and disruption risks in the supply chain. The papers are available on the Scopus bibliographic database, which is the largest abstract and citation database in academia, covering the most important publishers, such as Springer, Elsevier, Taylor and Francis, IEEE, and Emerald. Moreover, Scopus encompasses a wider range of journals and thus offers a greater possibility for citation analysis in comparison to its peers [17].

3. First Phase of SLNA Methodology: SLR

3.1. Scope of the Analysis

In this paper, all the literature reviews include conference papers, articles, review papers, book chapters, were analyzed based on all types of applications of blockchain technology that can be used to manage cyber and disruption risks in the supply chain. It tries to capture meaningful information from a systematic literature network analysis (SLNA). It uncovers the current trends regarding cyber risks, disruptions, and blockchain paradigms and paves the way for newcomers in aiming to adopt any of the identified themes as their research focus. The trends of research in this area started in 2018 and have gained attention and interest from scientific communities in recent years. Through this paper, the research questions were addressed in the following:

RQ1: What are the latest blockchain applications focused on disruption risk management?
 RQ2: How is blockchain solutions used to identify potential disruption risks?

3.2. Locating Studies

All the search terms and their combinations were selected to promote the emergence of concepts, issues, and trends that would help address the research questions. A set of different synonyms of “blockchain”, “risks”, “supply chain” was created in Scopus and then confirmed by a team of academics and industrial communities. This step of the analysis is very crucial, as where different sets of an applied query are used, this may affect the results.

In order to have wide coverage, database research string was obtained in the following: TITLE-ABS-KEY (“block-chain” OR “blockchain” OR “block chain” OR “distributed ledger”) AND TITLE (“cyber risk” OR “security” OR “risk” OR “protection” OR “threat” OR “disruption” OR “resilience” OR “crime” OR “attack” OR “breach” OR “failure”) OR KEY (“cyber risk” OR “security” OR “risk” OR “protection” OR “threat” OR “disruption” OR “resilience” OR “crime” OR “attack” OR “breach” OR “failure”) AND TITLE-ABS-KEY (“supply chain” OR “supply network”).

3.3. Study Selection and Evaluation

The identified keywords were used as search terms in Scopus at the end of July 2020 to find relevant publications. In addition, only articles in different reference types, such as conferences, journals, review papers, and book chapters, were included in the document type. We do not consider the limitation on publication year while setting “all years” in the data range field. The search with unique keywords led to obtaining 192 English publications from 2017 to 2020. Satoshi Nakamoto [18] invented the term blockchain with Bitcoin in 2008, but no primary research papers were retrieved before 2017. This may highlight the novelty of ideas in the field of the potential of blockchain technology and its implications for cyber risk and disruption risk management.

Figure 2 shows the distribution over time of the retrieved papers by publication year. As can be seen, most studies were published after the year 2018 in either theoretical or practical applications of blockchain to supply chain management. In fact, an increasing number of contributions published in recent years also shows that the field under study experienced a growth in popularity in different sectors.

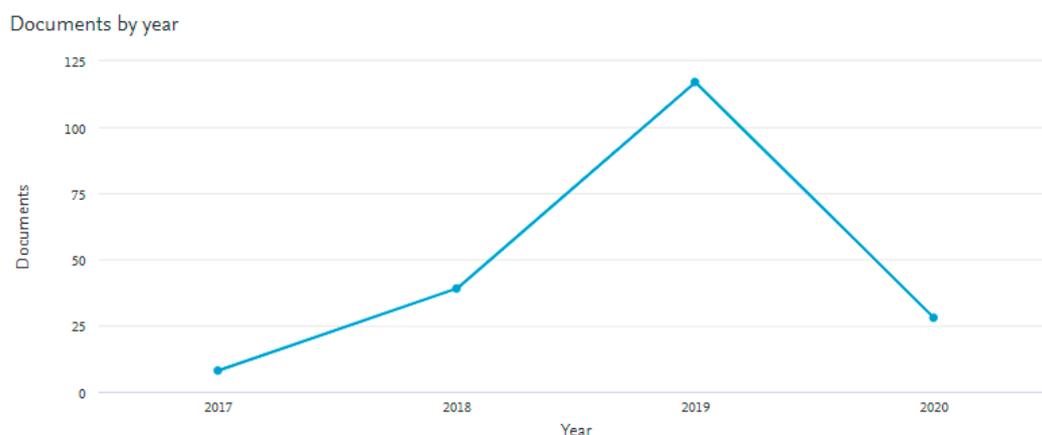


Figure 2. Distribution of articles over time by year of publication.

4. Second Phase of SLNA Methodology: BNA

The method used in this work is a bibliometric analysis; it consists of two different parts of the SLNA, which were introduced by [16] and further developed by [10], these being a citation network analysis and author keywords co-occurrence network analysis. The SLR allowed for identifying a set of papers and helped to examine the procedure of

main concepts and search strings. The 192 works resulting from the SLR phase constituted the input in the CNA to build and study bibliometric networks.

5. Results

5.1. Citation Network Analysis (CNA)

A citation network is a network in which the nodes are articles and the connections being their citations [10,16]. In this case, the flow of knowledge is depicted by arrows from the cited to citing papers. From Figure 3, a network consisting of 192 nodes was constructed with the software Pajek composed of 131 isolated nodes and four connected components. The biggest connected component includes 54 papers, and the other four include three and two papers. Based on more structured information from the biggest component, only the biggest connected component was analyzed, and the “isolated” nodes, which are papers not connected in the network, were excluded from analyses.

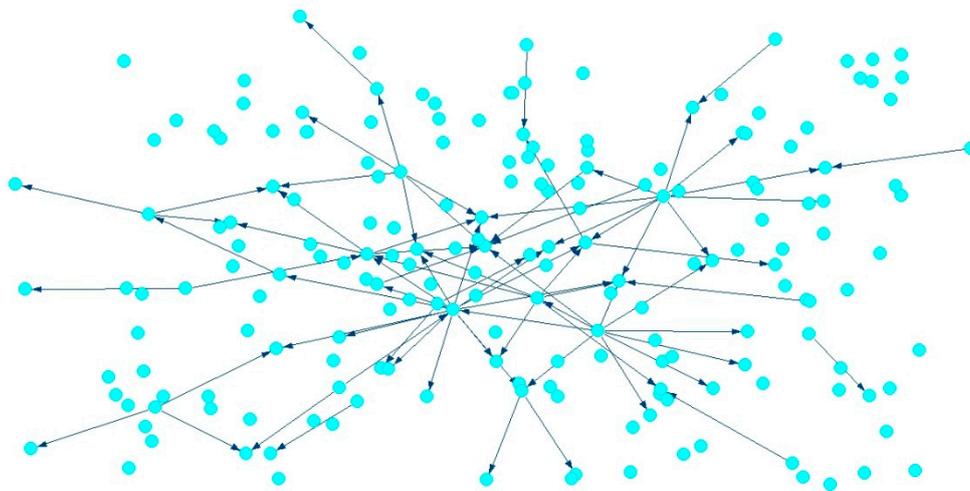


Figure 3. Citation network of 192 papers.

5.1.1. The Biggest Connected Component

As shown in Figure 4, the biggest connected component consists of 54 nodes exists. The layout of the nodes is obtained through the Kamada–Kawai algorithm [19] available in the Pajek software package.

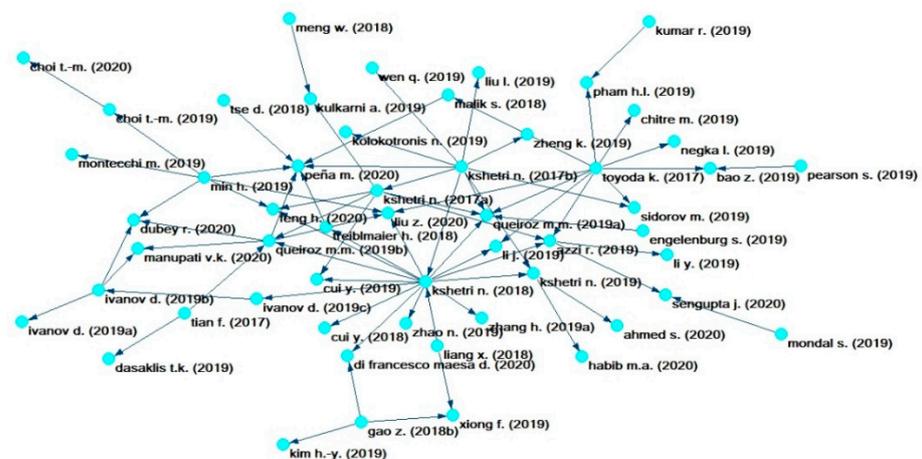


Figure 4. Main connected components of the citation network.

For holistic analysis of the components, two different analyses were selected: the Louvain community detection method and the main path analysis. Louvain community

detection method is an efficient algorithm to identify and map groups of papers into smaller sub-units or communities that allow us to study the structure of large networks [20]. The results from this algorithm are visualized through a graphical representation of the network of eight communities with different colors, which each color represents one community.

The main path analysis detects the existence of a main development trend of the field, extracting the main path component [21]. The main path represents the “backbone of the research tradition” [16,21]. As mentioned by [10], “the main path highlights the articles that build on prior articles, but continue to act as hubs in reference to later works”. Indeed, in this work, the connection was on the key-route main path, where key-route is the link that has the highest transversal weights [22]. Its extraction was performed by setting the rank numbers of key routes from 1 to 10 and using Pajek.

The eight Louvain community (Figure 5), as well as the main path (Figure 6) of the connected components, are discussed in the subsequent subsections.

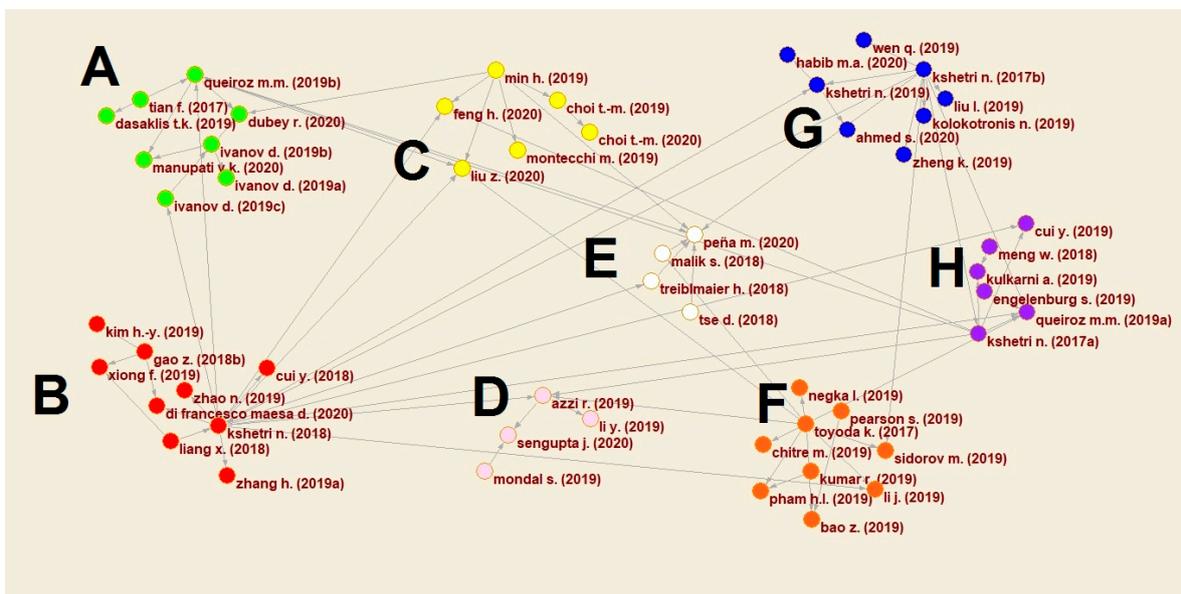


Figure 5. The Louvain communities.

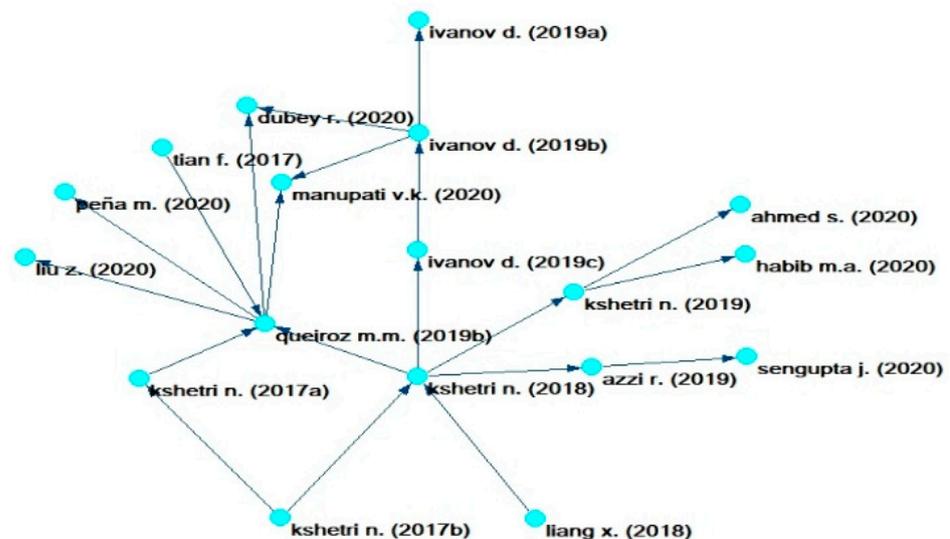


Figure 6. Main path biggest connected component of the citation network.

5.1.2. The Louvain Communities' Analysis

As stated earlier, this analysis enabled us to obtain eight communities labeled A–H in Figure 5.

Community A—Disruption Risk Management by Blockchain

The majority of papers in this community are connected with providing insights into the supply chain (SC) disruption risk management and examines how to combine blockchain technology with other digital technologies that can manage and predict disruptions and lead to resilience and robustness of the supply chain. Despite a few efforts to explore new insights into the effect of digital technologies on supply chain risks, our understanding of the human contribution and interplay of various digital technologies in terms of their impact on SC disruption risk management is still not clear.

Reference [23] Noted that the advent of digital technologies (e.g., big data analytics, artificial intelligence, blockchain, and Internet of things) brings a potential new benefit in increasing quality in the real-time flow of data and material in order to manage severe disruptions, resilience, and the ripple effect. The ripple effect in the supply chain occurs if severe disruptions affect SC performance such as demand, sales, stock return, service level, and costs [24]. In addition, Reference [25] continued their research at a more proactive level in order to evaluate severe SC risks and the ripple effect by presenting an SC digitalization framework in four important SC stages, including planning, manufacturing, sourcing, and logistics. Their findings indicate that cutting-edge technologies like blockchain and AI techniques are becoming increasingly important in response to outbreak-related disruptions by increasing operational supply chain flexibility and improving response traceability, real-time coordination, and the ability to reconfigure resources at the recovery stages and provide a robust and resilient supply chain.

From the perspective of environmental concerns, Reference [26] also developed a blockchain framework for a multi-echelon sustainable supply chain within a policy of carbon taxation in monitoring supply chain performance. Smart contracts enabled consumers to access information and details about standards and environmental concerns exhibited in the product, with the effect of diminishing costs and time and increasing the efficiency of the entire supply chain. Their proposed model can be applied to other sectors, including transportation networks, pharmaceutical services, and government services. For instance, blockchain, in conjunction with proper algorithms, can manage patient data and prescriptions.

Since blockchain has achieved significant success in the financial sectors, practitioners and researchers have started deploying blockchain in other sectors. Currently, humanitarian logistics and supply chains are increasingly adopting advanced technologies to support operations; however, the use of blockchain in this sector is at the beginning stages. Food supply chain, healthcare sectors, and government institutions are increasingly calling for more collaboration among various humanitarian actors in both the public and private sectors for real-time response to demands in order to facilitate the transparency and traceability on the flow of material, information, and financing in the supply chain. Finally, within a humanitarian setting, Reference [27] presented a theoretical model to explore the influence of blockchain on the transparency of the operational supply chain and improve collaboration by building swift trust between key partners who participated in disaster relief supply chains. Indeed, collaboration encourages joint efforts among stakeholders, contributes to effective and efficient real-time information sharing between partners, and brings several advantages such as higher transparency, flexibility, and reduces lead-time, and finally helps to enhance supply chain resilience [27].

Community B—Shared and Trusted Information by Blockchain Technology

Reference [28] Submitted the idea of blockchain adoption in terms of improvements in the entire supply chain, ranging from safe, efficient, and transparent transactions to the improvement of the level of trust and reliability between supply chain members by

sharing all transactions and related information across all the network. Reference [29] focused on weakening the resilience of the supply chain in the era of information asymmetry, which means that one of the members in the supply chain has a large amount of efficient information than the others [30]. They acknowledged that this inaccuracy or inconsistency of information could lead to take wrong decisions and increase technical risks such as cybercrime, hacking, and theft that damage the reputation of the company [29]. Among these problems, the authors emphasized the establishment of “trust” among participants in the supply chain with a decentralized information sharing mechanism based on blockchain technology.

The other papers in this community predominantly presented different mechanisms and models of blockchain technology, their adoption as well as the impact on SC performance outcomes in terms of enhancing security, trust, and information sharing. For example, to overcome some challenges such as low-performance and lack of ability to protect recorded information on the ledger, Reference [31] proposed a unified distributed ledger that satisfies the requirements of a distributed supply chain system for cargo tracing capability and different supply chain management tasks. Reference [32] conducted their studies by proposing a “blockchain-based construction supply chain framework” to eliminate some limitations in traditional systems such as extra delays, transmission costs, and information wastages and create a new mechanism towards guarantee security of share transmission and private-key protection. To mitigate the concerns associated with security threats arising from distributed ledgers, Reference [33] proposed a new architecture of the “FPGALedger” based decentralized ledger platform by relying on its security features such as bitstream encryption and tamper-resistant feature to prevent unauthorized access to sensitive data. The authors also evaluated its performance to show it is practical for enterprise applications.

In exploratory survey research, Reference [34] investigated the security and trust challenges, including software attack, i.e., stealing information stored on the servers, or other devices, installing malware code on a server for malicious activities, and hardware attacks, i.e., modifying the blueprint design, or inserting the spy chips into the hardware. The authors discussed the improvement of total performance into the supply chain management, i.e., transparency, visibility, accountability, traceability, and reliability, by applying some smart technologies such as the Internet of things, cloud computing and blockchain by participating the validated users in transactions.

Community C—A Digital Record of Every Transaction and Interaction

Papers in this community talk basically about the security and privacy of all the information of products stored in a shared and transparent system. Blockchain technology [35] has received attention from both practitioners and academics since the creation of Bitcoin. Reference [36] revealed some applications to supply chain security and a multitude of managerial benefits behind blockchain technology. For example, blockchain can contribute to lowering the cost of transactions, visibility of supply chain via open platforms, and improved the integrity of the global network of partners through digital and physical connectivity. They also discussed to show the potential of this technology in times of increased risks and uncertainty for enhancing supply chain resilience. In the recent paper, Reference [37] discussed how blockchain technology could be applied to explore risks in air-logistics operations. The authors proposed the literature from different areas, including “demand management”, “supply management”, “air-logistics operations”, “supply–demand coordination”. They also proposed the implementation of mean-variance risk analysis, which can be supported by blockchain technology. Observations show that blockchain technology is also related to information disclosure [38–40]. In fact, Reference [41] established that blockchain technology-based information disclosure can make use of rental service platforms to achieve the attractions of consumers. Reference [42] by developing a provenance knowledge framework demonstrated how blockchain technology could enhance assurance and authenticity in a transparent way through information visi-

bility for all involved parties and traceability of the products and consequently decrease perceived risks while protecting data privacy. Similar to the above study, the paper by [43] also focused on the application of blockchain technology for improving traceability performance by providing all transaction information about the origin of products with security and transparency.

Community D—Integration of Blockchain with IoT to Solve Privacy and Security Vulnerabilities

The focus of the papers in this community is on attacks, security issues, and blockchain solutions with the combination of IoT. For example, Reference [44], while attempting to describe a better comprehension of how blockchain can be integrated with IoT and real-time sensors into the pharmaceutical supply chain, studied a set of benefits and challenges of deploying the blockchain in the supply chain. Their results corroborated not only consideration of a suitable blockchain platform is important before choosing it for our business, but also we need to take into account the reliability of collected data. In the paper by [45], an RFID-based end-to-end blockchain architecture is proposed for creating a transparent food supply chain. The authors employed a new IoT-based food monitoring architecture, which updates a real-time tamper-proof of information at different retailing, logistics, and warehouse stages, to guarantee immunity against cyber attacks and making blockchain efficient from a cost perspective due to removing unnecessary transactions. Furthermore, Reference [46] conducted a comprehensive survey on security vulnerabilities and attacks in an IoT system and highlighted the advantages of integrating blockchain with different IoT and Industrial IoT applications containing cryptographic transactions, the robustness of decentralized systems, the provenance of data, and the trustworthiness of the entire system.

Community E—Transparency and Traceability in Information Exchange by Blockchain Technology

Several works in this community suggested that the exchange of information is one of the most important benefits of blockchain adoption. The study conducted by [47] discussed transparency and traceability in information exchange and the use of blockchain technology as an innovative solution to record and transfer transactions with authenticity, safety, and security among relevant parties in the SC. Reference [48] examined the relationship between SCM and blockchain from a theoretical perspective to provide relevant topics from frequently used theories such as principle agent theory (PAT) and transaction cost analysis (TCA) in the implications of blockchain on SCM and logistics. In this regard, for example, based on the PAT theory, the problem of information asymmetry between the principal and agent can be improved by blockchain technology, and the design, execution, and supervision of contracts can be done efficiently by the principle. Simultaneously, Reference [49] proposed a permissioned blockchain framework that facilitates transparent information sharing across the whole supply chain due to its remarkable features, namely immutability, auditability, and decentralization. In analyzing the applications of blockchain in the food sector, Reference [50] also reported the high level of coordination and collaboration of all supply chain participants in guaranteeing exchanges of information, security, reliability, transparency, and traceability.

Community F—Anti-Counterfeiting by Blockchain

Central to this community is the consideration of monitoring counterfeited products in the supply chain. In this vein, some authors have recently focused on counterfeiting in the medicine supply chain. For instance, one blockchain-based traceability system with RFID tags was proposed in the post supply chain by [51]. Authors tried to keep ownership information of manufactured products on the blockchain with RFID tags to prevent counterfeiting during the traceability process from manufacture to retailers. Reference [52] proposed a new solution using blockchain and encrypted QR (quick response) for traceability of drugs, all information from manufacture to end consumer is transmitted to the

chain, where smart contracts are applied to completely assess and identify the properties of medicines. Technical research based on blockchain Ethereum and IPFS networks for the traceability of medicine proposed by [53], their implementation on a small-scale showed that the proposed system in this work could be useful for the anti-counterfeit medicine supply chain. As presented by [54], the concept of “physically unclonable functions” used along with blockchain for preventing counterfeits and strengthen the security of IoT devices. The contribution of the paper by [55] is to present a secure ultralightweight RFID protocol and blockchain technology together to track attacks across the supply chain and prevent counterfeiting.

Community G—Information Privacy by Blockchain

The papers in this community mainly conducted research on blockchain from security perspectives and presented schemes on information privacy protection based on blockchain technology. In this respect, Reference [28], in a research about the security of information in IoT devices, established that through blockchain technology, IoT security challenges such as those related to IP spoofing and forgery attacks could be prevented. Because it is difficult to alter records in the approved blockchains, and it is impossible for malicious devices to connect to a network. Similarly, Reference [56] presented a scheme for data sharing in the supply chain by the industrial Internet of things (IIoT). They tried to show the ability of blockchain in avoiding data leakage among unauthorized members in the supply chain and the privacy protection of the chain. Likewise, Reference [57] for spacecraft supply chain, established that the use of blockchain is necessary for security and overall profit of the supply chain to address the issue of information asymmetry among the supply chain members and to mitigate costs of transactions. In addition, Reference [58], in a study on the use of blockchain technology in risk avoidance and coordination of supply chain, found that this technology has real potential to reduce transaction costs among members of the supply chain and improve information sharing among supply chain members.

Community H—Safety and Security Aspects of the Blockchain

The papers in this community predominantly focus on privacy and security issues and review the security aspects of the blockchain. In the paper by [6], blockchain is considered as an opportunity for enhancing the security aspects and mitigating cyber risks in end-to-end supply chains. In the paper by [59], the authors presented a review regarding the intrusion detection systems (IDSs) in conjunction with blockchain to manage data and trust. Reference [60] declared that safety and security are motivational drivers to blockchain adoption. To this purpose, they extended blockchain technology with other methods like encryption and business rules for improving the information available for risk analysis, safety, and security control in cross border activities. Some scholars [61,62] incorporated resilient and trusted security technologies with blockchain approaches while presenting integrated models/frameworks to avoid the complexity and vulnerability of the whole supply chain so that reliability and trustworthiness of processes can be achieved and the defects of a centralized network will be solved.

5.1.3. Main Path Analysis

Figure 6 depicts the main path of the biggest connected component, which includes 18 nodes from 2017 to 2020. Table 1 shows the analyses of the papers of the main path in order to highlight the main current research trends and the gaps that need to be addressed.

Table 1. Analysis of the most relevant documents belonging to the main path.

Authors	Topic	Main Issues	Contribution
[6,28]	Integration of blockchain and the Internet of things (IoT)	<ul style="list-style-type: none"> IoT security challenges 	<ul style="list-style-type: none"> Analysis and description of a trustless and decentralized system with a combination of blockchain and cloud-based IoT platform for executing cryptographic transactions through smart contracts and tracking supply chains sources of insecurity in IoT devices
[63,64]	Use of blockchain for supply chain securityblockchain-enabled supply chain activities	<ul style="list-style-type: none"> Attacks via manufacturer source code or product Attack via vendor remote access Lack of access to key supply chain objectives, including cost, quality, speed, dependability, risk reduction, sustainability, and flexibility 	<ul style="list-style-type: none"> Specified different benefits and advantages of blockchain technology such as overall system transparency; software, hardware, and firmware traceable and tamper-resistant records; accessibility and visibility of data provenance; and reliability and accountability of cyber supply chain assets Analysis and description of blockchain's roles in improving reliability, accountability, and transparency by shared and trusted information and real-time accessibility between stakeholders in the supply chain
[44]	Adoption, benefits, and challenges	<ul style="list-style-type: none"> Visibility and transparency of supply chain assets 	<ul style="list-style-type: none"> Evaluated different blockchain case studies to determine what supply chain problems can be addressed using blockchain and developed one theory about the necessity to build a blockchain-based supply chain
[46]	Blockchain solutions for IoT and IIoT	<ul style="list-style-type: none"> Security vulnerabilities and attacks in Industrial IoT- and IIoT-based systems 	<ul style="list-style-type: none"> Review attacks and highlight blockchain solutions for the IoT systems
[65]	Adoption, drivers, and challenges	<ul style="list-style-type: none"> Blockchain adoption challenges in the logistics and supply chain 	<ul style="list-style-type: none"> Contributed to the literature on blockchain adoption and developed a research model based on a unified theory of acceptance and use of technology (UTAUT)
[66]	Cross-border e-commerce supply chain and traceability	<ul style="list-style-type: none"> Recover problem, clone attack, counterfeit tag attack, and counterfeit product attack 	<ul style="list-style-type: none"> Proposed a blockchain-based framework with a multichain structure model for traceability of information and product
[67]	Food supply chain and traceability	<ul style="list-style-type: none"> Current centralized traceability systems Lack of trusted information between actors in the supply chain 	<ul style="list-style-type: none"> A food supply chain traceability system based on hazard analysis and critical control point (HACCP), blockchain, and Internet of things, for guaranteeing safety and quality of food and reducing problems, such as tampering and falsifying of information
[68,69]	Automation of the transaction process	<ul style="list-style-type: none"> Security and trust issues in the transaction process 	<ul style="list-style-type: none"> Proposed a blockchain-based framework through smart contracts for the security of transactions
[23,25]	Digital technologies and resilient supply chain	<ul style="list-style-type: none"> Ripple effect, resilience and disruption risks 	<ul style="list-style-type: none"> Proposed a conceptual framework for exploring the relationships between digitalization and SC disruptions risks
[26]	Sustainability and traceability	<ul style="list-style-type: none"> Carbon emission levels and operational costs in the supply chain 	<ul style="list-style-type: none"> Proposed a blockchain framework for a multi-echelon sustainable supply chain, which enables monitoring of the entire supply chain and total operational costs and carbon emissions reductions
[27]	Humanitarian logistics and supply chain	<ul style="list-style-type: none"> Lack of collaboration and swift-trust between supply chain key partners 	<ul style="list-style-type: none"> Proposed a theoretical model to explore the influence of blockchain on improving swift-trust, collaboration, and supply chain resilience

The first stream was addressed by focusing on a considerable number of studies that appeared from 2017 and which started to investigate the capabilities and strategies of

supply chains in using blockchain as a key component of cyber supply chain risk management (CSRM) across various sectors, such as agriculture, livestock, food processing, energy systems, and e-commerce. The oldest paper in this stream focuses on the combination of blockchain with cloud-based IoT platforms for improving cybersecurity in supply chain networks; this happens through the development of a trustless and decentralized system, which executes cryptographic transactions autonomously in a secure environment through smart contracts or via the detection and prevention of malicious actions with interlocked devices [6]. A potential solution to mitigate cyber risks in end-to-end supply chains is the implementation of blockchain into IoT devices to securely store information about the provenance of products, identity, credentials, and digital rights, with the aim to prevent safety and security vulnerabilities [28].

Following [6,28], the emerging literature on blockchain began to expound on different benefits and advantages of this technology which can have a direct effect on the supply chain, including a range of features, such as overall system transparency; software, hardware, and firmware traceable and tamper-resistant records; accessibility and visibility of data provenance; reliability and accountability of cyber supply chain assets [63]. In particular, a seminal work or milestone on the impacts of blockchain on various supply chain activities is that by [28]. This is the most frequently cited paper and has been cited by other authors among the selected papers in the main path. This paper focuses on the potential of blockchain on the elements such as cost, quality, risk reduction, and flexibility, and sustainability in meeting key supply chain management purposes. Moreover, many achievements are reachable by blockchain's ability in terms of improvements in the entire supply chain, ranging from safe, efficient, and transparent transactions to the improvement of the level of trust and reliability between supply chain members by sharing all transactions and related information across the entire network [64].

The following studies by [44,46] continued the involvement stream, focusing on the advantages of applying the blockchain for controlling cyber attacks and security vulnerabilities in the supply chain and also the new challenges posed by integrating the blockchain into the supply chain ecosystem. The authors in [44] have developed a blockchain platform with the combination of IoT and real-time sensors for the reliability of collected data during the pharmaceutical supply chain. The proposed system also ensures the transparency and tracking of products' information to enable counterfeiting detection. Furthermore, Reference [46] conducted a comprehensive survey on security vulnerabilities and attacks in Industrial IoT based systems, including (i) tampering; (ii) malicious code injection; (iii) Sybil attack; (iv) denial/distributed denial of service (Dos/DDOS); (v) data breach; (vi) malware and the countermeasures adopted to deal with each of these attacks.

The emerging literature on the blockchain, risks, and supply chain marked the development of blockchain research focused on the models, conceptual frameworks, and methods used to deal with protecting against typical problems and critical attacks. In this context, the paper by [65] presented an empirical investigation in India and the USA while taking into account the behavior of users regarding the adoption of blockchain in the supply chain field. Their results showed significant differences in performance expectancy, social influence, facilitating conditions, transparency, and trust of supply chain stakeholders in user behavior intentions towards this advanced technology across the countries under study. This paper is a source of various literature reviews [26,50,66] and a sink to [67] from the food sector.

The year 2017 is also marked by a scholarly interest in the application of blockchain technology in the agri-food chain through the work of [67]. This involves real-time food tracing with a traceability system based on hazard analysis and critical control point (HACCP), blockchain, and the Internet of things for guaranteeing safety and quality of the food and reducing many problems, such as tampering and falsifying of information. The proposed decentralized distributed system integrated with other technologies, such as WSN, GPS, RFID, to share and transfer information through the BigchainDB for data storage of products in food supply chains. The additional papers continue the debate

on the application of blockchain to the food sector and agriculture from a traceability perspective. For example, Reference [66] introduced a blockchain-based framework, with a multichain structure model, focusing on product traceability problems in the field of “cross-border e-commerce supply chain management”. The research analysis results show that the proposed framework can effectively tackle critical recovery problems and defend against attacks such as clone attack, counterfeit tag attack, and counterfeit product attack. Simultaneously [50] reported the high-level of coordination and collaboration of all supply chain participants in guaranteeing security, reliability, transparency, and traceability through the adoption of blockchain technology. In the considered time window, other contributions appeared to deal with information sharing and trust issues in the supply chain through smart contracts. Reference [68] grasped the impact of information sharing on security issues and trust in data accessing processes between stakeholders in the supply chain by presenting a conceptual framework based on blockchain technology and automation of transaction processes through smart contracts. In the transaction process, the payment will be done automatically with the confirmation of the buyer to the supplier with the details of an order ID, time, and date of shipment, and the data accessing process can be stored on-chain or off-chain for tracking purposes. Subsequently, Reference [69] proposed a framework with the use of blockchain technology to improve the level of truthful information shared across users while interacting with the fertilizer distribution systems for ensuring soil fertility and crop production.

Currently, the supply chain is becoming more sensitive to disruptions than in the past due to the growth of sophistication in the supply chain processes, or poor coordination, fraud, complex deals, different government policies, cultural and behavioral diversifications among supply chain entities. For example, the rapid spread of COVID-19 caused serious vulnerabilities in demand and disruptions in international supply chains. First, there was the big issue of supplying medical equipment, including special devices for diagnostic tests and personal protective supplies, such as masks and protective clothing, etc., to address the challenges related to treatment, protection, and control [70]. Second, it was similarly difficult to meet the daily needs of customers for food and other necessary items under lockdown during the COVID-19 pandemic [71].

The second stream of research referred to a new perspective in the supply chain (SC) disruption risk management and examines how to combine blockchain technology with other digital technologies can manage and predict disruptions and lead to resilience and robustness of the supply chain.

This stream of the main path is, as earlier discussed, in community A.

5.1.4. General Comments on the Connected Components’ Analyses

In conclusion, the two analyses conducted allowed a comprehensive review of the connected component. Specifically, an overview of the main path analysis enabled us to see how the applications, integration, and implementation of blockchain technology are connected and collaborative for an effective, secure supply chain. Similarly, the Louvain communities allowed us to uncover further research streams that are not considered by the works in the main path analysis, e.g., a digital record of every transaction and interaction, transparency and traceability in information exchange by blockchain technology, anti-Counterfeiting by blockchain, etc.

As mentioned in the citation network, some papers among the retrieved set of scientific works were excluded from the analysis because they are not connected in the network, and no citations are linking them. To overcome this drawback, the forthcoming additional analyses such as GCS and Co-occurrence of author keywords compensated for this limitation.

5.2. Global Citation Score Analysis

The information provided by the citation network must be expanded by an additional analysis, which is called global citation score analysis (GCS). Recent main studies can be

identified using GCS analysis. The whole number of citations to a paper in the Scopus database will appear with this analysis, regardless of their belonging to a connected component of a citation network. The most cited papers with high GCS retrieved from the Scopus database are considered as seminal or prominent papers in the evolution of knowledge [10,72]. The ten most cited papers ranked based on their GCS in Table 2. Indeed, 4 out of the 10 most cited papers that are not present in the main path analysis are found to belong to one of the Louvain community earlier discussed, and this supports the capability of the CNA to detect recent chief tendencies for conducting works in the era of blockchain. It is thus safe to state that both the main path analysis and the Louvain community affirm the significance of CNA analysis.

Table 2. Global citation score analysis (GCS) of the 10 most cited papers.

Title	Author	Source	Year	GCS	Main Path	Louvain Community
Can Blockchain Strengthen the Internet of Things?	[28]	IT Professional	2017	213	YES	G
Blockchain's roles in meeting key supply chain management objectives	[64]	International Journal of Information Management	2018	175	YES	B
A supply chain traceability system for food safety based on HACCP, blockchain and the Internet of things	[67]	14th International Conference on Services Systems and Services Management, ICSSSM 2017—Proceedings	2017	120	YES	A
Blockchain's roles in strengthening cybersecurity and protecting privacy	[6]	Telecommunications Policy	2017	110	YES	H
When intrusion detection meets blockchain technology: A review	[59]	IEEE Access	2018	108	NO	H
A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain	[51]	IEEE Access	2017	98	NO	F
The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics	[25]	International Journal of Production Research	2019	81	YES	A
Blockchain adoption challenges in the supply chain: An empirical investigation of the main drivers in India and the USA	[65]	International Journal of Information Management	2019	54	YES	A
Blockchain application in food supply information security	[47]	IEEE International Conference on Industrial Engineering and Engineering Management	2018	51	NO	E
The impact of the blockchain on the supply chain: a theory-based research framework and a call for action	[48]	Supply Chain Management	2018	41	NO	E

5.3. Co-Occurrence Analysis of Author Keywords

“The co-occurrence of a similar word or couple of words may signify a research theme. This perhaps implies the presence of patterns and trends in a particular field” [11,73]. The network map (Figure 7) and the cluster items (Table 3) are the results of the VoSviewer software that performed this method. The software created seven clusters, with different colors, grouping a set of 29 keywords, which was the result of the initial 465 keywords after setting a threshold of the minimum number of occurrences of a keyword at 4. We selected this threshold because the expected results of a too low value of threshold would not be enough significance in the analysis. In addition, selecting a too high value of threshold would cause the elimination of a number enough of keywords.

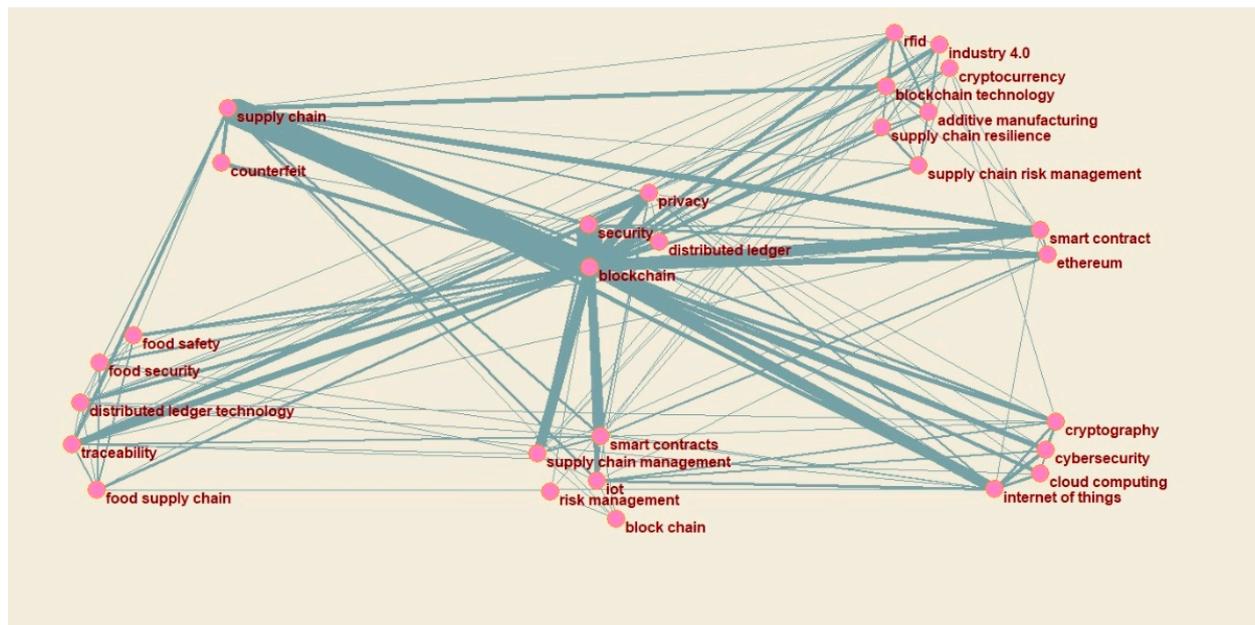


Figure 7. Authors keywords’ co-occurrence network.

Table 3. Authors keywords’ co-occurrence network.

Main Subjects	Keywords
Cluster 1: Digitalization for improved supply chain resilience	Additive manufacturing; blockchain technology; cryptocurrency; industry 4.0; RFID; supply chain resilience; supply chain risk management
Cluster 2: Employing blockchain technology with smart contracts in supply chain management	Blockchain; IoT; risk management; smart contracts; supply chain management
Cluster 3: Traceability database systems to ensure food safety and security	Distribute ledger technology; food safety; food security; food supply chain; traceability
Cluster 4: Blockchain’s roles in strengthening cybersecurity	cloud computing; cryptography; cybersecurity; Internet of things
Cluster 5: Privacy and security challenges and blockchain solutions	Blockchain; distributed ledger; privacy; security
Cluster 6: Security of smart contracts in Ethereum platforms	Ethereum; smart contract
Cluster 7: Monitoring counterfeited products in the supply chain	Counterfeit; supply chain

Note that the software considers neither difference between singular and plural terms nor between words with the same roots; therefore, the keywords with the same meanings (e.g., “blockchain” and “block chain” or “smart contract” and “smart contracts”) were merged.

A discussion of the whole set of works contained in the author’s keywords network is presented in the following.

5.3.1. Cluster 1: Digitalization for Improved Supply Chain Resilience

The papers in this community appear to be focused on issues of the protection of supply chains from threats and disruptions to enhance risk management practices and improved supply chain resilience, as highlighted by the keywords “supply chain risk management” and “supply chain resilience”. The importance of supply chain resilience in the body of literature was already mentioned in the main path analysis. This cluster adds other shades of attempts carried out to control disruptions in the supply chain. The most common disruption risks affecting the supply chain and significantly its performance stem from natural disasters (e.g., earthquakes, hurricanes, and floods), cyber threats (human errors,

failures, and terrorism), and disruptions of environmental regulations [8,24,74,75]. Recently, attempts to enhance supply chain resilience by emerging technologies in times of increased risks and uncertainty have become increasingly popular, including blockchain [36], digital innovations and Industry 4.0 [25] and 3D printing/additive manufacturing [76]. For example, the benefits of additive manufacturing, also known as 3D printing, are to increase flexibility and resilience in the manufacturing and supply chain with quick response to demand and reduction of storage of finished goods as well as to identify supplier risk exposure, since there is no intermediate inventory in between the stages [25]. One of the most highly exploited cases for 3D printing facilities can be during the COVID-19 pandemic in that it allows for efficient and timely deployment of medical equipment or replacement of urgent missing supplies [77]. However, the need for the rapid delivery of spare parts by 3D printing may lead to counterfeit products or fake parts during the delivery [76]. Based on these challenges, the application of digital rights management can be a successful solution for implementation in the area of additive manufacturing and protection against intellectual property theft with blockchain technology [76].

5.3.2. Cluster 2: Employing Blockchain Technology with Smart Contracts in Supply Chain Management

This cluster is focused on the development of smart contracts, enabling and fostering the traditional supply chain, as shown by the keywords “supply chain management” and “smart contracts”. A smart contract is a self-sufficient decentralized code deployed in the blockchain node to digitally execute a special transaction when certain conditions of a business process are met [78].

The literature discusses these applications and opportunities associated with smart contracts. For instance, Reference [79] proposed an efficient solution to automate the supply chain processes by applying a blockchain network based on Ethereum, with smart contracts also known as cryptocontract, keeping the whole data of a company. This proposed system based on blockchain, IoT and smart contracts improve traditional supply chain management systems by replacing the standard contract with smart contracts.

Studies also focus on specific sectors, such as the food supply chain and healthcare, where blockchain technology represents an opportunity to ensure the monitoring and traceability of food and pharmaceutical products. The authors of [33] analyzed a new blockchain ontology with the integration of IoT devices and translated it into a smart contract to achieve supply chain provenance tracing. According to Internet technologies, this blockchain technology was built using a natural interface web browser. Interaction between JavaScript interface with the deployed smart contract in the truffle framework by ConsenSys to execute source tracking and traceability. This object-oriented design of the traceability data model was implemented in the Ethereum platform.

The authors of [80] highlighted the opportunities that the advent of blockchain technology and the concept of smart contracts open up for pharmacies, hospitals, or other healthcare stakeholders, to effectively and efficiently respond to epidemic relief. Likewise, epidemics such as disease and its spreading can be monitored through smart contract capabilities with automated responses or warnings.

In addition, recent literature also proposed a theoretical design and practical implementation of unmanned aerial vehicles (UAVs) in the warehouse for inventory and traceability applications. This system is integrated with RFID and a blockchain to collect, and process validated data and send them to trusted parties. Moreover, smart contracts applied to this system lead to automating certain tasks as the result of less human intervention and provide cybersecurity, redundancy, and data integrity [81].

5.3.3. Cluster 3: Traceability Database Systems to Ensure Food Safety and Security

This cluster of keywords appears to be focused mainly on the use of blockchain for assuring traceability and transparency to reduce food safety risks and to evaluate the health risks of food processing at all stages of the food supply chain. Transparency of a supply chain refers to the accessibility of all the information of food products through shared

and transaction systems, providing a trusted source of information without loss, noise, delay, and distortion [82,83]. The authors of [84] define traceability in terms of “what, how, where, why, and when aspects of underlying product along a supply chain”. Blockchain technology facilitates safe information sharing across the whole supply chain [49]. The information stored on the blockchain platforms can be accessed, and it is not possible to manipulate by anyone, and from the customer perspective, they can monitor food information by anyone, and from the customer perspective, they can monitor food information from smartphones more accurately, which reinforce their confidence. According to [85], trust, security, and transparency in Wal-Mart’s food supply chain increased thanks to the adoption of blockchain technology, which requires parties who access blockchain to present documents and register data. Subsequently, food waste can be controlled, and the chance of corruption and risk of food fraud can be minimized significantly [86,87].

5.3.4. Cluster 4: Blockchain’s Benefits in Strengthening Cybersecurity and Cryptography

This cluster of keywords appears to address the use of blockchain, cloud computing, and the Internet of things in cybersecurity and cryptography. Examples include the study by [28], who proposed the implementation of blockchain or distributed ledger technologies (DLTs) to execute cryptographic transactions by providing superior data integrity to mitigate cyber risks in the end-to-end supply chain. The authors of [88] examined the opportunities of applying blockchain technology to secure critical energy and electricity infrastructures and their range of vulnerable energy delivery systems and IoT-based systems through a cryptographic signed distributed ledger that helps in enhancing data security, provenance, and audibility. The authors of [89] supported existing literature on current themes in information technology, including blockchain and cybersecurity solutions for repulsing attacks and threats. They listed types of direct attacks at blockchain implementation that can be summarized into the following: (1) Double-spending threats; (2) Mining/pool threats; (3) Wallet threats; (4) Network threats; (5) Smart contract threats, and in order to improve the security of blockchain technology, they also suggested new security solutions such as digital identity; authentication and access management; security platforms; privacy management; and DDoS protection. The content of the exploratory paper by [34] also focused on the “security and trust issues on digital supply chain management” with an application of some new information technologies, i.e., Internet of Things, cloud computing and blockchain, to boost different performance and properties of the system, such as the transparency, visibility, trust, traceability, and efficiency of information.

5.3.5. Cluster 5: Privacy and Security Challenges and Blockchain Solutions

Cluster 5 focuses mainly on privacy and security issues and reviews the security aspects of the blockchain. The main goal of the paper by [90] is to define an authentication security protocol with blockchain to ensure the privacy and security of departments and companies against potential attacks. The authors of [91] furthermore presented a “privacy sharing” on an innovative blockchain system for the protection of IoT data securely and privately. The privacy of data is maintained by the blockchain platform to limited connected participants in a distributed way; data within a channel is encrypted and managed by embedding access control systems.

There are papers that give special emphasis to possible applications in the healthcare industry [92], drug supply chain [93] and e-voting [94]. The authors of [95] applied the decentralized blockchain technology with an Ethereum platform in IoT systems to deal with security and privacy challenges in the healthcare insurance sector. The results are proved by showing trust management, security, and privacy data. Blockchain or distributed ledger technologies (DLT) also have great potential for collecting and integrating data from medical records and clinical technologies to provide real-time information for patients and providers [96]. In another study, Reference [97] presented a systematic literature review of blockchain-based 5G-enabled IoT for tracing various transactions and databases that can

prove authenticity, consistency, security, and privacy in future Industrial automation such as smart homes, smart cities, healthcare, agriculture and autonomous vehicles.

5.3.6. Cluster 6: Security of Smart Contracts in Ethereum Platforms

The security against vulnerabilities of smart contracts in a blockchain system is a new research area being dealt with. Another definition of the smart contract put forward by [98] is “a piece of code that executes a specific business logic when a certain condition is met”. Smart contracts have been applied to a wide range of industries, including supply chain, healthcare, intellectual property, electronic voting, and have many benefits ranging from traceability, transparency, data provenance to reducing costs and time expenditures. However, many security issues in smart contracts have been reported by practitioners and researchers, mostly causing major economic losses. According to [99], the common issues in Ethereum smart contracts include the following: risk to unprotected self-destruct, which relates to the permits access to an unauthorized actor; the risk to locked money, which relates to the immaturity of blockchain platforms; and risk to timestamp dependence, which relates to malicious miners. The security solutions for smart contracts offer different phases based on secure design [100,101], secure implementation [102], testing before deployment [103–105], and monitoring and analysis [106,107].

5.3.7. Cluster 7: Monitoring Counterfeited Products in the Supply Chain

Product Counterfeiting is a type of customer fraud: a product consisting of bad or unsafe quality ingredients or with false information on the package is produced and sold. Counterfeited products can be applied to every industry sector, including food, pharmaceuticals, cosmetics, electronics, and vehicle parts. Some authors have focused on counterfeiting on different products. Concerns about the above-mentioned problems have become front and center for companies worldwide. For example, a European medicine agency is warning about buying falsified/substandard medicines from unauthorized websites or other suppliers during the ongoing pandemic of coronavirus disease COVID-19 [108].

Some authors have recently focused on counterfeiting in specific sectors. The authors of [109] proposed a new solution based on blockchain implemented on the Hyperledger Fabric platform for exploring counterfeiting and improving visibility and traceability in the pharma supply chain. The authors of [110] introduced a blockchain-based technology known as counterchain for increasing the authenticity of drugs and consumer confidence in products. Another study by [111] proposed a model based on simulation in Hyperledger Fabric that can be applied to a vehicle supply chain to solve issues related to counterfeiting in vehicle parts.

6. Discussion of Findings and Future Research Directions

Below we summarize the research gaps and future research directions in the field of blockchain technology proposed by various researchers in managing cyber and disruption risks in the supply chain and based on a bibliometric review of the literature. Based on the various analyses (Louvain community detection, main path extraction, Global citation score analysis, as well as Co-occurrence all keywords analysis) of 192 works, we obtained a holistic view of the state of the art of research trajectories, thereby enabling us to explore the main trends and the recent research streams on blockchain adoption for the supply chain risk management.

A new trend emerging in the literature referred to the key role of emerging technologies, including digital technology, Industry 4.0 [25], and blockchain [27], in supply chain (Sc) disruption risk management. It examines how these advanced technologies can manage and predict disruptions and lead to resilience and robustness of the supply chain. The findings examine the application of advanced technologies such as RFID, IoT, blockchain, big data, and artificial intelligence in order to reduce information disruption risks as the result of real-time identification and material tracing, to reduce supply and time risks due to real-time coordination, to increase the ability to reconfigure resources

at the recovery stages and to improve collaboration through swift trust between the different actors participating in disaster relief efforts. However, despite receiving attention from scientific communities, the emerging technologies still have a huge opportunity for improvement with regard to the field of supply chain disruption risk management.

Therefore, future research can concentrate on investigating how to design and implement different mechanisms and methods, mainly in response to different types of disruptions. Major research efforts also should focus on identifying the current classifications of potential disruptions, reassessment of laws and regulations towards a more efficient approach, and the emergence of smart platforms and architectures in response to these disruptions. In particular, it is necessary to refine the efficiency of current studies that categorize disruptions as those by natural disasters like acts of nature or technological disasters like acts of humans. For example, how can blockchain technology and AI techniques contribute to developing control actions to recover Sc operability, or how can these technologies be integrated into a traceability system to avoid or decrease the pandemic's impacts from a shortage of supplies.

As we see from the works of [23–25], the ripple effect has drawn attention to the field of disruption risk management and the impact of opportunities and benefits of blockchain on it, regarding response to outbreak-related disruptions by increasing operation supply chain flexibility and improving response traceability, real-time coordination, and the ability to reconfigure resources at the recovery stages and provide a robust and resilient supply chain. We believe that further theoretical and empirical effort is required to understand what technological developments and how can contribute to enhancing ripple effect control.

Interestingly, several contributions also highlight the opportunities from collaboration and trust perspectives in both public and private sectors among various humanitarian actors in terms of real-time response to demands, facilitating transparency and traceability in the flow of material, information and financing in the supply chain, so that firms can obtain the essential knowledge and rapidly react to disruptions and cyber threats and real-time information sharing to all supply chain partners to enhance awareness and create knowledge to empower firms to deal with these threats [27,50,112]. Therefore, more publications are needed to deal with the lack of awareness and knowledge about blockchain technology adoption decisions throughout industry sectors, corporate cultures, government intervention, and the behavior of actual and potential users on the adoption or non-adoption of blockchain solutions in the supply chain field. This could give us clear answers to this challenge. Future research should also study the role of third-party regulators and authority organizations in order to consider standardization, compliance, and forensics as a priority to promote blockchain adoption by firms.

In the context of capabilities and strategies of the supply chain in applying blockchain as a key component of cyber supply chain risk management (CSR), various researchers (e.g., [6,49,68,91]) proposed different blockchain systems, models, and architectures alone or in combination with other technologies to manage privacy and security challenges, the security of smart contracts, monitoring counterfeiting, and traceability database systems to ensure food safety and security. However, future research is required to consider some challenges concerning an assessment of network latency, high-energy consumption, standardization of data, and low-performance of blockchain-based IoT networks during the implementation of blockchain in the supply chain.

Building on former research (e.g., [98,100]), further insights may also consider a review of different methods in which blockchain-based Ethereum platforms and smart contracts can be used for innovative cybersecurity solutions.

An important body of research explores security and safety in IoT networks as a most important priority, despite the majority of studies on blockchain cybersecurity referred that the security of IoT networks could be improved if it is integrated by blockchain technology, which for instance appears in the community D (i.e., [46]) and cluster 2 (i.e., [79]). Yet, a few studies discussed the critical success factors for blockchain adoption in a cyber-secure

supply chain to mitigate IoT security risks/threats. Thus, future research should apply guidelines and tools that can help fill this gap in the literature.

Additionally, in the last few years, blockchain technology is growing to gain attention to address traceability and transparency issues within the agri-food supply chain (e.g., [82,83,85]); even most of the articles have been paid to the advantages of blockchain adoption and a few studies have explored the obstacles of adoption in the food supply chain. A further investigation on the barriers may provide more insights regarding blockchain adoption for researchers and practitioners.

Finally, most of the proposed blockchain systems are still in the academic stage, and more efforts are required from developers to present more applicative cybersecurity models, tools, and architectures in industries and startups. On the other hand, when more blockchain solutions are adopted with a larger number of organizations, more research is needed to address technical and behavioral challenges and limitations in the adoption of this technology. For example, looking deeper into issues such as storage capacity, the security and privacy of blockchain, the high investment of adoption, less collaboration and trust among key stakeholders, and behavioral intentions would accelerate adoption by providing some proper solutions for future studies in the area of blockchain technology.

7. Conclusions

In this study, we conducted an SLNA to answer the research question of the study: what are the main trends and the recent research streams in managing cyber and disruption risks in the supply chain with blockchain, taking into account their evolution over time?

The result of this quantitative bibliometric analysis indicates that blockchain is a rather new technology with an increase in the number of publications over the past few years. First, based on SLNA analysis of 192 articles, two main streams were identified: one devoted to the capabilities and strategies of the supply chain to apply blockchain as a key component of cyber supply chain risk management (CSR); the other one referred to a perspective in managing supply chain (SC) disruption risks, examining how to combine blockchain technology with other digital technologies and how smart operations can manage and predict disruptions and lead to resilience and robustness of the supply chain. Second, this systematic review sheds light on different research areas, such as the blockchain's role as a solution for privacy and security challenges, security of smart contracts, monitoring counterfeiting, and traceability database systems to ensure food safety and security.

In terms of implications, this study contributes to the body of knowledge in determining and analyzing the development of trajectories and research areas within the topic. This has resulted in several quantitative bibliometric studies based on algorithms and software tools that have allowed us to detect the flow of information, and it is dynamic over time. This enabled us to provide a comprehensive picture of the knowledge on the subject, to identify some directions in research, and to build a future agenda that covers the dynamic development of the subject. An additional contribution is represented by depicting a landscape of the scientific literature enriched by an author keywords analysis in order to develop and understand blockchain's capabilities as a new technology for cyber-risk and disruption risk prevention in international supply chains. Finally, there are some criticisms in this work that need to be addressed in future research. The main limitation is related to data collection from a single source, Scopus, which is not able alone to cover all scientific contributions in the studied fields. Future studies may extend the data sources to include more publications and compare the results on the evolving research trends. Moreover, due to the "Matthew effect", authors are interested in citing papers with a high number of citations because of their reputation and popularity.

Notwithstanding the discussed limitations, this study contributes an overview of the most established study areas regarding disruptions, cyber risks, and blockchain paradigms, and how these are changing and evolving over time, thereby assisting newcomers in aiming to adopt any of the identified themes as their research focus.

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

Funding: This research was funded by LIUC Università Carlo Cattaneo Ateneo 2019's competitive research awards, grant number 3840.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Acknowledgments: We would like to thank the anonymous reviewers for their comments that allow us to further enhance the outcome of this research.

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

References

- Chen, T.M.; Abu-Nimeh, S. Lessons from Stuxnet. *Computer* **2011**. [CrossRef]
- Boyes, H. Cybersecurity and Cyber-Resilient Supply Chains. *Technol. Innov. Manag. Rev.* **2015**. [CrossRef]
- Deloitte. *The Future of Cyber Survey 2019 Cyber Everywhere. Succeed Anywhere*; Deloitte: London, UK, 2019; pp. 1–32.
- Raab, M.; Griffin-Cryan, B. *Digital Transformation of Supply Chains: Creating Value—When Digital Meets Physical*; Capgemini Consulting: Paris, France, 2011.
- Aceto, B. Blockchain e Dintorini. 2019. Retrieved 22 May 2019. Available online: <http://tendenzeonline.info/articoli/2019/05/08/blockchain-edintorini> (accessed on 5 February 2021).
- Kshetri, N. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommun. Policy* **2017**, *41*, 1027–1038. [CrossRef]
- Swan, M. Climate Change 2013—The Physical Science Basis. In *Blockchain: Blueprint for a New Economy*; O'Reilly Media, Inc.: Newton, MA, USA, 2015. [CrossRef]
- Ghadge, A.; Weiß, M.; Caldwell, N.D.; Wilding, R. Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Manag.* **2019**. [CrossRef]
- Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.K. A systematic literature review of blockchain cyber security. *Digit. Commun. Netw.* **2019**. [CrossRef]
- Strozzi, F.; Colicchia, C.; Creazza, A.; Noè, C. Literature review on the “Smart Factory” concept using bibliometric tools. *Int. J. Prod. Res.* **2017**, *55*, 6572–6591. [CrossRef]
- Zhao, G.; Liu, S.; Lopez, C.; Lu, H.; Elgueta, S.; Chen, H.; Boshkoska, B.M. Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions. *Comput. Ind.* **2019**, *109*, 83–99. [CrossRef]
- Etemadi, N.; Borbon, Y.G.; Strozzi, F. Blockchain technology for cybersecurity applications in the food supply chain: A systematic literature review. In Proceedings of the XXIV Summer School “Francesco Turco”—Industrial Systems Engineering, Bergamo, Italy, 9–11 September 2020.
- Denyer, D.; Tranfield, D. Producing a Systematic Review. In *The SAGE Handbook of Organizational Research Methods*; 2009; Available online: <https://psycnet.apa.org/record/2010-00924-039> (accessed on 5 February 2021).
- Van Eck, N.J.; Waltman, L. How to normalize cooccurrence data? An analysis of some well-known similarity measures. *J. Am. Soc. Inf. Sci. Technol.* **2009**. [CrossRef]
- De Nooy, W.; Mrvar, A.; Batagelj, V. Exploratory Social Network Analysis with Pajek. *Connections* **2011**. [CrossRef]
- Colicchia, C.; Strozzi, F. Supply chain risk management: A new methodology for a systematic literature review. *Supply Chain Manag.* **2012**. [CrossRef]
- Falagas, M.E.; Pitsouni, E.I.; Malietzis, G.A.; Pappas, G. Comparison of PubMed, Scopus, Web of Science, and Google Scholar: Strengths and weaknesses. *FASEB J.* **2008**. [CrossRef]
- Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: <https://bitcoin.org/bitcoin.pdf> (accessed on 5 February 2021).
- Kamada, T.; Kawai, S. An algorithm for drawing general undirected graphs. *Inf. Process. Lett.* **1989**. [CrossRef]
- Blondel, V.D.; Guillaume, J.L.; Lambiotte, R.; Lefebvre, E. Fast unfolding of communities in large networks. *J. Stat. Mech. Theory Exp.* **2008**. [CrossRef]
- Lucio-Arias, D.; Leydesdorff, L. Main-path analysis and path-dependent transitions in HistCite™-based historiograms. *J. Am. Soc. Inf. Sci. Technol.* **2008**. [CrossRef]
- Liu, J.S.; Lu, L.Y.Y. An Integrated Approach for Main Path Analysis: Development of the Hirsch Index as an Example. *J. Am. Soc. Inf. Sci. Technol.* **2012**, *63*, 528–542. [CrossRef]

23. Ivanov, D.; Dolgui, A.; Das, A.; Sokolov, B. Digital Supply Chain Twins: Managing the Ripple Effect, Resilience, and Disruption Risks by Data-Driven Optimization, Simulation, and Visibility. *Int. Ser. Oper. Res. Manag. Sci.* **2019**. [[CrossRef](#)]
24. Ivanov, D. Revealing interfaces of supply chain resilience and sustainability: A simulation study. *Int. J. Prod. Res.* **2018**, *56*, 3507–3523. [[CrossRef](#)]
25. Ivanov, D.; Dolgui, A.; Sokolov, B. The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. *Int. J. Prod. Res.* **2019**. [[CrossRef](#)]
26. Manupati, V.K.; Schoenherr, T.; Ramkumar, M.; Wagner, S.M.; Pabba, S.K.; Inder Raj Singh, R. A blockchain-based approach for a multi-echelon sustainable supply chain. *Int. J. Prod. Res.* **2020**. [[CrossRef](#)]
27. Dubey, R.; Gunasekaran, A.; Bryde, D.J.; Dwivedi, Y.K.; Papadopoulos, T. Blockchain technology for enhancing swift-trust, collaboration and resilience within a humanitarian supply chain setting. *Int. J. Prod. Res.* **2020**, *58*, 3381–3398. [[CrossRef](#)]
28. Kshetri, N. Can Blockchain Strengthen the Internet of Things? *IT Prof.* **2017**. [[CrossRef](#)]
29. Cui, Y.; Idota, H. Improving supply chain resilience with establishing a decentralized information sharing mechanism. *ACM Int. Conf. Proc. Ser.* **2018**. [[CrossRef](#)]
30. Agrell, P.J.; Lindroth, R.; Norrman, A. Risk, information and incentives in telecom supply chains. *Int. J. Prod. Econ.* **2004**. [[CrossRef](#)]
31. Gao, Z.; Xu, L.; Chen, L.; Zhao, X.; Lu, Y.; Shi, W. CoC: A Unified Distributed Ledger Based Supply Chain Management System. *J. Comput. Sci. Technol.* **2018**. [[CrossRef](#)]
32. Xiong, F.; Xiao, R.; Ren, W.; Zheng, R.; Jiang, J. A key protection scheme based on secret sharing for blockchain-based construction supply chain system. *IEEE Access* **2019**. [[CrossRef](#)]
33. Kim, H.Y.; Suh, T.; Xu, L.; Shi, W. FPGA based decentralized ledger for enterprise applications. In Proceedings of the ICBC 2019—IEEE International Conference on Blockchain and Cryptocurrency 2019, Seoul, Korea, 14–17 May 2019. [[CrossRef](#)]
34. Zhang, H.; Nakamura, T.; Sakurai, K. Security and trust issues on digital supply chain. In Proceedings of the IEEE 17th International Conference on Dependable, Autonomic and Secure Computing, IEEE 17th International Conference on Pervasive Intelligence and Computing, IEEE 5th International Conference on Cloud and Big Data Computing, 4th Cyber Scienc, Fukuoka, Japan, 5–8 August 2019. [[CrossRef](#)]
35. Choi, T.M. Blockchain-technology-supported platforms for diamond authentication and certification in luxury supply chains. *Transp. Res. Part E Logist. Transp. Rev.* **2019**. [[CrossRef](#)]
36. Min, H. Blockchain technology for enhancing supply chain resilience. *Bus. Horiz.* **2019**, *62*, 35–45. [[CrossRef](#)]
37. Choi, T.M.; Wen, X.; Sun, X.; Chung, S.H. The mean-variance approach for global supply chain risk analysis with air logistics in the blockchain technology era. *Transp. Res. Part E Logist. Transp. Rev.* **2019**. [[CrossRef](#)]
38. Cai, S.; Xu, M.; Zhang, L. Automatic information disclosure with value chains based on blockchain technology. In Proceedings of the 2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference, ITAIC, Chongqing, China, 24–26 May 2019. [[CrossRef](#)]
39. Zhai, S.; Yang, Y.; Li, J.; Qiu, C.; Zhao, J. Research on the Application of Cryptography on the Blockchain. *J. Phys. Conf. Ser.* **2019**, *1168*. [[CrossRef](#)]
40. Jiang, N.; Wang, W.; Wu, J.; Wang, J. Traceable Method for Personal Information Registration Based on Blockchain. *IEEE Access* **2020**, *8*, 52700–52712. [[CrossRef](#)]
41. Choi, T.M.; Feng, L.; Li, R. Information disclosure structure in supply chains with rental service platforms in the blockchain technology era. *Int. J. Prod. Econ.* **2020**. [[CrossRef](#)]
42. Montecchi, M.; Plangger, K.; Etter, M. It's real, trust me! Establishing supply chain provenance using blockchain. *Bus. Horiz.* **2019**. [[CrossRef](#)]
43. Feng, H.; Wang, X.; Duan, Y.; Zhang, J.; Zhang, X. Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges. *J. Clean. Prod.* **2020**. [[CrossRef](#)]
44. Azzi, R.; Chamoun, R.K.; Sokhn, M. The power of a blockchain-based supply chain. *Comput. Ind. Eng.* **2019**, *135*, 582–592. [[CrossRef](#)]
45. Mondal, S.; Wijewardena, K.P.; Karuppuswami, S.; Kriti, N.; Kumar, D.; Chahal, P. Blockchain inspired RFID-based information architecture for food supply chain. *IEEE Internet Things J.* **2019**. [[CrossRef](#)]
46. Sengupta, J.; Ruj, S.; Das, S. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [[CrossRef](#)]
47. Tse, D.; Zhang, B.; Yang, Y.; Cheng, C.; Mu, H. Blockchain application in food supply information security. In Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management, Bangkok, Thailand, 16–19 December 2018. [[CrossRef](#)]
48. Treiblmaier, H. The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. *Supply Chain Manag.* **2018**. [[CrossRef](#)]
49. Malik, S.; Kanhere, S.S.; Jurdak, R. ProductChain: Scalable blockchain framework to support provenance in supply chains. In Proceedings of the NCA 2018—2018 IEEE 17th International Symposium on Network Computing and Applications 2018, Cambridge, MA, USA, 1–3 November 2018. [[CrossRef](#)]
50. Peña, M.; Llivisaca, J.; Siguenza-Guzman, L. Blockchain and Its Potential Applications in Food Supply Chain Management in Ecuador. *Adv. Intell. Syst. Comput.* **2020**. [[CrossRef](#)]

51. Toyoda, K.; Mathiopoulous, P.T.; Sasase, I.; Ohtsuki, T. A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain. *IEEE Access* **2017**. [[CrossRef](#)]
52. Kumar, R.; Tripathi, R. Traceability of counterfeit medicine supply chain through Blockchain. In Proceedings of the 2019 11th International Conference on Communication Systems and Networks, COMSNETS 2019, Bangalore, India, 7–11 January 2019. [[CrossRef](#)]
53. Pham, H.L.; Tran, T.H.; Nakashima, Y. Practical Anti-Counterfeit Medicine Management System Based on Blockchain Technology. In Proceedings of the TIMES-iCON 2019—2019 4th Technology Innovation Management and Engineering Science International Conference, Bangkok, Thailand, 11–13 December 2019. [[CrossRef](#)]
54. Negka, L.; Gketsios, G.; Anagnostopoulos, N.A.; Spathoulas, G.; Kakarountas, A.; Katzenbeisser, S. Employing blockchain and physical unclonable functions for counterfeit IoT devices detection. *ACM Int. Conf. Proc. Ser.* **2019**. [[CrossRef](#)]
55. Sidorov, M.; Ong, M.T.; Sridharan, R.V.; Nakamura, J.; Ohmura, R.; Khor, J.H. Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains. *IEEE Access* **2019**. [[CrossRef](#)]
56. Wen, Q.; Gao, Y.; Chen, Z.; Wu, D. A blockchain-based data sharing scheme in the supply chain by IIoT. In Proceedings of the 2019 IEEE International Conference on Industrial Cyber Physical Systems, ICPS 2019, Taipei, Taiwan, 6–9 May 2019. [[CrossRef](#)]
57. Zheng, K.; Zhang, Z.; Chen, Y.; Wu, J. Blockchain adoption for information sharing: Risk decision-making in spacecraft supply chain. *Enterp. Inf. Syst.* **2019**. [[CrossRef](#)]
58. Liu, L.; Li, F.; Qi, E. Research on Risk Avoidance and Coordination of Supply Chain Subject Based on Blockchain Technology. *Sustainability* **2019**, *11*, 2182. [[CrossRef](#)]
59. Meng, W.; Tischhauser, E.W.; Wang, Q.; Wang, Y.; Han, J. When intrusion detection meets blockchain technology: A review. *IEEE Access* **2018**. [[CrossRef](#)]
60. Engelenburg, S.; van Janssen, M.; Klievink, B. Design of a software architecture supporting business-to-government information sharing to improve public safety and security: Combining business rules, Events and blockchain technology. *J. Intell. Inf. Syst.* **2019**. [[CrossRef](#)]
61. Cui, Y.; Idota, H.; Ota, M. Improving Supply Chain Resilience with a Hybrid System Architecture. *Commun. Comput. Inf. Sci.* **2019**. [[CrossRef](#)]
62. Kulkarni, A.; Hazari, N.A.; Niamat, M. A Blockchain Technology Approach for the Security and Trust of the IC Supply Chain. In Proceedings of the IEEE National Aerospace Electronics Conference, NAECON, 2019, Dayton, OH, USA, 15–19 July 2019. [[CrossRef](#)]
63. Liang, X.; Shetty, S.; Tosh, D.; Ji, Y.; Li, D. Towards a reliable and accountable cyber supply chain in energy delivery system using blockchain. In Proceedings of the Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, Osaka, Japan, 28–29 February 2018. [[CrossRef](#)]
64. Kshetri, N. 1 Blockchain's roles in meeting key supply chain management objectives. *Int. J. Inf. Manag.* **2018**, *39*, 80–89. [[CrossRef](#)]
65. Queiroz, M.M.; Wamba, S.F. Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA. *Int. J. Inf. Manag.* **2019**, *46*, 70–82. [[CrossRef](#)]
66. Liu, Z.; Li, Z. A blockchain-based framework of cross-border e-commerce supply chain. *Int. J. Inf. Manag.* **2020**, *52*, 102059. [[CrossRef](#)]
67. Tian, F. A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things. In Proceedings of the 14th International Conference on Services Systems and Services Management, ICSSSM 2017—Proceedings, Dalian, China, 16–18 June 2017. [[CrossRef](#)]
68. Habib, M.A.; Sardar, M.B.; Jabbar, S.; Faisal, C.N.; Mahmood, N.; Ahmad, M. Blockchain-based Supply Chain for the Automation of Transaction Process: Case Study based Validation. In Proceedings of the 2020 International Conference on Engineering and Emerging Technologies, ICEET 2020, Tokyo, Japan, 22–23 February 2020. [[CrossRef](#)]
69. Ahmed, S.; Islam, M.E.; Hosen, M.T.; Hasan, M.H. Blockchain based fertilizer distribution system: Bangladesh perspective. *ACM Int. Conf. Proc. Ser.* **2020**. [[CrossRef](#)]
70. The World Health Organization (WHO). Situation Report—18. 7 February 2020. Available online: https://www.who.int/docs/default-source/coronaviruse/transcripts/transcript-coronavirus-press-conference-full-07feb2020-final.pdf?sfvrsn=3beba1c0_2 (accessed on 5 February 2021).
71. Ministry of Commerce, People's Republic of China. Online Press Conference on 10 February 2020. In Chinese. Available online: <http://www.mofcom.gov.cn/article/i/jyj/1/202002/20200202936313.shtml> (accessed on 5 February 2021).
72. Knoke, D.; Yang, S. *Social Network Analysis*, 2nd ed.; Sage Publications: Szczenek, CA, USA, 2019.
73. Ding, Y.; Chowdhury, G.G.; Foo, S. Bibliometric cartography of information retrieval research by using co-word analysis. *Inf. Process. Manag.* **2001**. [[CrossRef](#)]
74. Ivanov, D.; Sokolov, B.; Solovyeva, I.; Dolgui, A.; Jie, F. Dynamic recovery policies for time-critical supply chains under conditions of ripple effect. *Int. J. Prod. Res.* **2016**, *54*, 7245–7258. [[CrossRef](#)]
75. Hosseini, S.; Ivanov, D.; Dolgui, A. Review of quantitative methods for supply chain resilience analysis. *Transp. Res. Part E Logist. Transp. Rev.* **2019**. [[CrossRef](#)]
76. Holland, M.; Nigischer, C.; Stjepandic, J. Copyright protection in additive manufacturing with blockchain approach. *Adv. Transdiscipl. Eng.* **2017**. [[CrossRef](#)]

77. Queiroz, M.M.; Ivanov, D.; Dolgui, A.; Wamba, S.F. Impacts of epidemic outbreaks on supply chains: Mapping a research agenda amid the COVID-19 pandemic through a structured literature review. *Ann. Oper. Res.* **2020**. [[CrossRef](#)] [[PubMed](#)]
78. Global Blockchain Business Council. Global Blockchain Business Council (GBBC) Announces Release of Annual Report. *Medium* **2018**. Available online: <https://www.google.com.hk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi5o4ji3tLuAhUTy4sBHTBaCYgQFjAAegQIAhAC&url=https%3A%2F%2Fgbbc.medium.com%2Fglobal-blockchain-business-council-gbbc-announces-release-of-annual-report-f7f1fd533db6&usg=AOvVaw3mnlHq8VHHum8e30QpTh79> (accessed on 5 February 2021).
79. Naidu, V.; Mudliar, K.; Naik, A.; Bhavathankar, P. A Fully Observable Supply Chain Management System Using Block Chain and IOT'. In Proceedings of the 2018 3rd International Conference for Convergence in Technology, I2CT 2018, Pune, India, 6–7 April 2018. [[CrossRef](#)]
80. Di Francesco Maesa, D.; Mori, P. Blockchain 3.0 applications survey. *J. Parallel Distrib. Comput.* **2020**. [[CrossRef](#)]
81. Fernández-Caramés, T.M.; Blanco-Novoa, O.; Froiz-Míguez, I.; Fraga-Lamas, P. Towards an Autonomous Industry 4.0 Warehouse: A UAV and Blockchain-Based System for Inventory and Traceability Applications in Big Data-Driven Supply Chain Management. *Sensors* **2019**, *19*, 2394. [[CrossRef](#)]
82. Galvez, J.F.; Mejuto, J.C.; Simal-Gandara, J. Future challenges on the use of blockchain for food traceability analysis. *Trends Anal. Chem.* **2018**. [[CrossRef](#)]
83. Mao, D.; Wang, F.; Hao, Z.; Li, H. Credit evaluation system based on blockchain for multiple stakeholders in the food supply chain. *Int. J. Env. Res. Public Health* **2018**, *15*, 1627. [[CrossRef](#)] [[PubMed](#)]
84. Aung, M.M.; Chang, Y.S. Traceability in a food supply chain: Safety and quality perspectives. *Food Control* **2014**. [[CrossRef](#)]
85. Yiannas, F. A New Era of Food Transparency Powered by Blockchain. *Innov. Technol. Gov. Glob.* **2018**. [[CrossRef](#)]
86. Shaikh, S.; Butala, M.; Butala, R.; Creado, M. AgroVita using Blockchain. In Proceedings of the 2019 IEEE 5th International Conference for Convergence in Technology, I2CT 2019, Bombay, India, 29–31 March 2019. [[CrossRef](#)]
87. Kayikci, Y.; Subramanian, N.; Dora, M.; Bhatia, M.S. Food supply chain in the era of Industry 4.0: Blockchain technology implementation opportunities and impediments from the perspective of people, process, performance, and technology. *Prod. Plan. Control* **2020**, 1–21. [[CrossRef](#)]
88. Mylrea, M.; Gouriseti, S.N.G. Blockchain for Supply Chain Cybersecurity, Optimization and Compliance. In Proceedings of the Resilience Week 2018, RWS 2018, Denver, CO, USA, 20–23 August 2018. [[CrossRef](#)]
89. Rot, A.; Blaicke, B. Blockchain's Future Role in Cybersecurity. Analysis of Defensive and Offensive Potential Leveraging Blockchain-Based Platforms. In Proceedings of the 2019 9th International Conference on Advanced Computer Information Technologies, ACIT 2019—Proceedings, Ceske Budejovice, Czech Republic, 5–7 June 2019. [[CrossRef](#)]
90. Wang, S.; Zhu, S.; Zhang, Y. Blockchain-based Mutual Authentication Security Protocol for Distributed RFID Systems. *IEEE Symp. Comput. Commun.* **2018**. [[CrossRef](#)]
91. Makhdoom, I.; Zhou, I.; Abolhasan, M.; Lipman, J.; Ni, W. PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Comput. Secur.* **2020**. [[CrossRef](#)]
92. Hemalatha, K.; Hema, K.; Deepika, V. Utilization of blockchain technology to overthrow the challenges in healthcare industry. *Adv. Intell. Syst. Comput.* **2020**. [[CrossRef](#)]
93. Sahoo, M.; Singhar, S.S.; Sahoo, S.S. A blockchain based model to eliminate drug counterfeiting. *Adv. Intell. Syst. Comput.* **2020**. [[CrossRef](#)]
94. Abuidris, Y.; Kumar, R.; Wenyong, W. A survey of blockchain based on e-voting systems. *ACM Int. Conf. Proc. Ser.* **2019**. [[CrossRef](#)]
95. Mohanta, B.K.; Panda, S.S.; Satapathy, U.; Jena, D.; Gountia, D. Trustworthy Management in Decentralized IoT Application using Blockchain. In Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2019, Kanpur, India, 6–8 July 2019. [[CrossRef](#)]
96. Badr, N.G. Blockchain or distributed ledger technology what is in it for the healthcare industry? In Proceedings of the IC3K 2019—Proceedings of the 11th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management, Vienna, Austria, 9–11 November 2019. [[CrossRef](#)]
97. Mistry, I.; Tanwar, S.; Tyagi, S.; Kumar, N. Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. *Mech. Syst. Signal Process.* **2020**, *135*, 106382. [[CrossRef](#)]
98. Mann, S.; Potdar, V.; Gajavilli, R.S.; Chandan, A. Blockchain technology for supply chain traceability, transparency and data provenance. *ACM Int. Conf. Proc. Ser.* **2018**. [[CrossRef](#)]
99. Huang, Y.; Bian, Y.; Li, R.; Zhao, J.L.; Shi, P. Smart contract security: A software lifecycle perspective. *IEEE Access* **2019**. [[CrossRef](#)]
100. Bartoletti, M.; Pompianu, L. An Empirical analysis of smart contracts: Platforms, applications, and design patterns. In Proceedings of the International Conference on Financial Cryptography and Data Security, Sliema, Malta, 3–7 April 2017. [[CrossRef](#)]
101. Wohrer, M.; Zdun, U. Smart contracts: Security patterns in the ethereum ecosystem and solidity. In Proceedings of the 2018 IEEE 1st International Workshop on Blockchain Oriented Software Engineering, IWBOSE 2018—Proceedings, Campobasso, Italy, 1 November 2018. [[CrossRef](#)]
102. Clack, C.D. Smart Contract Templates: Legal semantics and code validation. *J. Digit. Bank.* **2018**, *2*, 338–352.

103. Abdellatif, T.; Brousmiche, K.L. Formal Verification of Smart Contracts Based on Users and Blockchain Behaviors Models. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018—Proceedings, Paris, France, 26–28 February 2018. [CrossRef]
104. Grishchenko, I.; Maffei, M.; Schneidewind, C. A semantic framework for the security analysis of ethereum smart contracts. In *Principles of Security and Trust, Proceedings of the 7th International Conference, POST 2018, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2018, Thessaloniki, Greece, 16–19 April 2018*; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2018. [CrossRef]
105. Hildenbrandt, E.; Saxena, M.; Zhu, X.; Rodrigues, N.; Daian, P.; Guth, D.; Rosu, G. KEVM: A complete formal semantics of the ethereum virtual machine. In Proceedings of the IEEE Computer Security Foundations Symposium, Cernayla-Ville, France, 9–12 July 2018; pp. 204–217. [CrossRef]
106. Breidenbach, L.; Daian, P.; Tramèr, F.; Juels, A. Enter the Hydra: Towards principled bug bounties and exploit-resistant smart contracts. In Proceedings of the 27th USENIX Security Symposium, Berkeley, CA, USA, 12 August 2018.
107. Nikolić, I.; Kolluri, A.; Sergey, I.; Saxena, P.; Hobor, A. Finding the greedy, prodigal, and suicidal contracts at scale. *ACM Int. Conf. Proc. Ser.* **2018**. [CrossRef]
108. Ema.europa.eu. COVID-19: Beware of Falsified Medicines from Unregistered Websites. 2020. Available online: <https://www.ema.europa.eu/en/news/covid-19-beware-falsified-medicines-unregistered-website> (accessed on 21 May 2020).
109. Raj, R.; Rai, N.; Agarwal, S. Anticounterfeiting in Pharmaceutical Supply Chain by establishing Proof of Ownership. In Proceedings of the IEEE Region 10 Annual International Conference, Proceedings/TENCON, Osaka, Japan, 16–19 November 2019. [CrossRef]
110. Chitre, M.; Sapkal, S.; Adhikari, A.; Mulla, S. Monitoring Counterfeit Drugs using CounterChain. In Proceedings of the 2019 6th IEEE International Conference on Advances in Computing, Communication and Control, ICAC3 2019, Mumbai, India, 20–21 December 2019. [CrossRef]
111. Wang, K.; Liu, M.; Jiang, X.; Yang, C.; Zhang, H. A Novel Vehicle Blockchain Model Based on Hyperledger Fabric for Vehicle Supply Chain Management. *Commun. Comput. Inf. Sci.* **2020**. [CrossRef]
112. Scott, B.; Loonam, J.; Kumar, V. Exploring the rise of blockchain technology: Towards distributed collaborative organizations. *Strateg. Chang.* **2017**. [CrossRef]