

Review

# The Role of Blockchain Technology in Augmenting Supply Chain Resilience to Cybercrime

Aya Bayramova , David J. Edwards \*  and Chris Roberts

Faculty of Engineering and the Built Environment, City Centre Campus, Birmingham City University, Millennium Point, Birmingham B4 7XG, UK; ayabayramova@gmail.com (A.B.); chri51988@live.com (C.R.)  
\* Correspondence: drdavidedwards@aol.com

**Abstract:** Using a systematic review of literature, this study identifies the potential impact of blockchain solutions for augmenting supply chain resilience (SCR) to cybercrime. This rich literature synthesis forms the basis of a novel theoretical framework that provides guidance and insight for blockchain adopters and vendors as well as delineate palpable benefits of this novel technology. An interpretivist philosophical design and inductive reasoning are adopted to conduct the systematic review of literature. A total of 867 papers were retrieved from Scopus database between the years of 2016 and 2020 and subsequently analysed via abductive reasoning, grounded theory and a thematic meta-analysis; where the latter was achieved using a scientometric approach and software tools such as VOS viewer and NVivo. Scientometric analysis revealed the most prolific countries, sources, publications and authors who reside at the vanguard of blockchain developments and adoption. Subsequent grounded theory analysis identified six main clusters of research endeavour viz: “case study”, “challenges and opportunity”, “traceability”, “smart contract” “blockchain and IoT” and “data security”. From 28 SCR metrics identified within literature, five were found to have been positively impacted by blockchain technology solutions, namely: “visibility”, “collaboration”, “integration”, “risk management” and “information sharing.” Prominent applications of blockchain technology in practice were “traceability systems” and “smart contracts” which are often implemented separately or in combination and primarily in food supply chains. This research constitutes the first study to critically synthesise extant literature for evaluation of blockchain solutions’ implication on SCR metrics. New perspectives obtained provided a basis for the novel theoretical framework for implementation that will be valued by software developers and adopting organizations, whilst creating new direction for researchers interested in blockchain technology.



**Citation:** Bayramova, A.; Edwards, D.J.; Roberts, C. The Role of Blockchain Technology in Augmenting Supply Chain Resilience to Cybercrime. *Buildings* **2021**, *11*, 283. <https://doi.org/10.3390/buildings11070283>

Academic Editor: David Arditì

Received: 2 June 2021

Accepted: 27 June 2021

Published: 30 June 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/>).

**Keywords:** blockchain technology; supply chain resilience; cybersecurity; resilience metrics

## 1. Introduction

Since the discovery of blockchain technology’s viability in environments other than original cryptocurrency practices, applications have exponentially proliferated in diverse industrial sectors such as: insurance [1]; content distribution [2]; logistics [3,4]; travel [5]; healthcare [6,7]; e-commerce [8]; and banking systems [9]. Novel supply chain applications are no exception and various work has been undertaken to explore its applications primarily on food supply chains, particularly emphasizing product traceability and visibility enhancement features cf. [10,11]. Other researchers such as Queiroz et al. [2], Sawyerr and Harrison [12] and Maesa and Mori [13] studied blockchain’s innate immutability aspects of stored transactional data.

However, with multitudinous and largely unforeseen disturbances to global supply chains (e.g., the Global Financial Crises in 2008 [14]; the 9–11 terrorist attack [15,16] and Covid-19 pandemic [17,18]) engenders the necessity to evaluate the impact of technological advancements on supply chains in times of disruption rather than solely measuring their impact in a “business as usual” scenario [19,20]. Researchers studying the risks associated

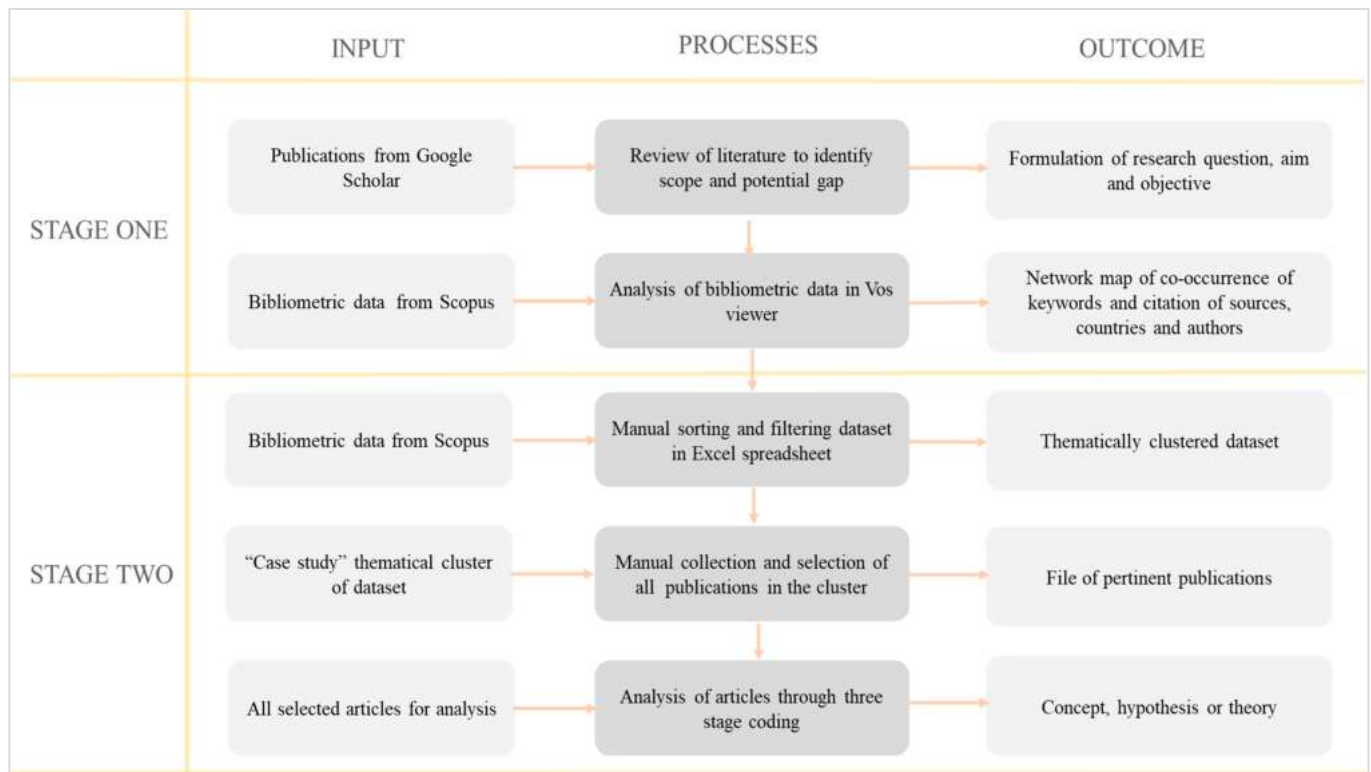
with these unforeseen disruptions, categorize them into two major dichotomous group of “external” and “internal” risk groups [21–23]. External risks are associated with unexpected events occurring extrinsically that stifle the supply chain system and induce a ripple effect (throughout the supply chain) that prolong the recovery from the disruption [21,22]. Examples of external risks include force majeure (e.g., earthquakes, hurricanes and floods) but also man-made catastrophes (e.g., computer viruses, terrorist attacks, economic turbulence or recession) [19,20]. These risks not only have the inherent capacity to create operational disruptions and shortages to supply chain participants, but also threatens an organisation’s financial and human resources such that distribution, transportation and communication suffers immeasurably [20]. External risks are largely unavoidable and hence, organisations can only prepare to mitigate their disruption vis-à-vis eliminate them [23]. Conversely, internal risks are associated with uncertainties of supply-demand coordination events or unprecedented change in product specifications [20,24]. Forrester [25] defined the “bull-whip effect” concept in supply chains as depicting fluctuations in purchasing an inventory to fulfil customer demand that accumulates towards the upstream of a supply chain. This concept occurs when a supplier’s order is larger than a buyer’s order and is often caused by poor quality of information sharing, erroneous perceived demand and delays in supply chains [26]. Other examples of internal risks are information technology problems or breakdowns, uncertainties in lead times, power outages, equipment malfunctions and systemic failures [27].

These numerous internal and external risks (and their frequency of occurrence) increase the vulnerability of supply chains and necessitate development of risk mitigation methods and strategies to engender organisational resilience and preparedness [20,28]. Yet, despite these risks elucidated upon, circa 69% of organisations globally have no complete visibility of their supply chains [29] and 30% of organisations fail to analyse the source of disruptions [30]. These compelling statistics engender the need for novel studies that answer the question: what are the blockchain technology applications that could potentially augment supply chain resilience (SCR) against disruption risks? Therefore, this research seeks to define and delineate the potential impact of these applications and their adoption(s) on SCR metrics using a scientometric review of existing literature. Concomitant research objectives are to: provide much needed guidance on blockchain applications for industry practitioners and for organisations planning to adopt them; and create a cyber threat map (as a novel theoretical framework) by identifying common cyber threats according to their target types and their current solutions to contrast those solutions with blockchain potentials. New insights (including a novel framework) generated will serve to incite wider polemic debate but will also provide much needed guidance and clarification for software developers and adopting organizations.

## 2. Methodology

The overarching epistemological design adopted a mixed philosophical stance of interpretivism and post-positivism cf. [31–34] to systematically analyse extant literature using a scientometric approach (a sub-branch of bibliometrics) cf. [35–38]. As a philosophical approach, interpretivism seeks to understand and interpret a phenomenon under investigation from different points of view in a subjective way [39,40]. Conversely, postpositivism is an approach of pursuing objectivity to reduce the potential effect of researchers’ bias by applying both quantitative and qualitative methods of data analysis [41]; in this present study using meta-data analysis. Objectivity in postpositivist paradigm results in establishing nascent theory that enables building categories and dimensions from an irregular data set [42]. Mixed philosophies are widely used within contemporary construction and project management literature. For example, Ghosh et al. [43] explored patterns and trends in the application of the internet of things (IoT) research to identify future applications in the construction industry; and Oshodi et al. [44] conducted a systematic review of construction output modelling techniques. Given the investigative nature of this research, inductive and abductive reasoning [39,45] are adopted to deduce comprehensive conclusions based upon

theoretical understanding [40] of blockchain technology applications' impact on SCR. From an approach and methods perspective, the research is conducted in two consecutive stages (refer to Figure 1); where stage one adopts inductive reasoning to conduct a meta-analysis of literature (as a secondary data source) and stage two builds upon this body of knowledge using abductive reasoning and grounded theory.



**Figure 1.** Research processes and their outcomes.

### 2.1. Meta-Analysis Technique

Meta-analysis is a form of inquiry in which studies about investigated phenomenon (each representing a research unit) are aggregated and integrated to summarise literature based on relationships between different research items [46]. Hunter and Schmidt [47] proffer that this method creates cumulative knowledge by eliminating potential distortive effects of primary research whilst maintaining track of ongoing research. To facilitate this first stage, the software tool VOS viewer with functionalities of visualizing, exploring and creating bibliometric networks was adopted [48]. Bibliometric data was sourced from Scopus database with the search rules of TITLE-ABS-KEY (blockchain AND technology AND in AND supply AND chains) AND (EXCLUDE (PUBYEAR, 2021)) AND (EXCLUDE (SRCTYPE, "k") OR EXCLUDE (SRCTYPE, "b") OR EXCLUDE (SRCTYPE, "d")) AND (EXCLUDE (LANGUAGE, "Chinese") OR EXCLUDE (LANGUAGE, "Spanish") OR EXCLUDE (LANGUAGE, "German") OR EXCLUDE (LANGUAGE, "French")). All these search criteria were selected to source a critical mass of existing publications within the scientific community to perform substantiated literature analysis from different perspectives. This refined search provided 867 publications with 44.2% of conference papers, followed by 44.6% of journal articles, excluding: book series; trading journals; books; and 15 papers that were translated from Chinese, Spanish, German and French. While there was no limit set for "date range" except for excluding 2021, year of publication for pertinent papers started from 2016. Conference papers were sampled because the rapid progress of blockchain developments and relatively expedient publication rates means that many researchers (particularly in information technology fields of science) choose to publish their work at these events.

## 2.2. Grounded Theory Technique

Grounded theory analysis was conducted using computer-assisted qualitative data analysis software (CAQDAS) called NVivo to provide a deeper and richer interrogation of the prevailing academic discourse. To narrow the scope of data analysis, this stage commenced with thematic analysis of bibliometric data retrieved from Scopus journal database (obtained from stage 1). All data retrieved were analysed manually in a Microsoft Excel spreadsheet by colour-coding each emerging theme through screening the titles and abstracts of each publication and clustering them together. From initially sourced 867 publications, papers with irrelevant application areas (such as rental service, auditing and public voting) were excluded. Similarly, papers based on generic supply chain management and risk management matters were excepted from the dataset. Based on these screening and filtering processes, thematical clusters of 'case study' (with 89 papers) and 'data security' (with 27 papers) were selected to further study using grounded theory analysis. All the publications in those clusters were retrieved by locating their digital object identifier (DOI) addresses except for those without access or link.

Grounded theory is an approach of analysing data by fragmenting them using key processes of 'coding', 'theoretical sampling' and 'theoretical saturation' [39]. The first stage of open coding reveals emerging concepts in the publications [39]. This approach of data collection (by open coding through selected publications) and analysis is referred as a "theoretical sampling" which is distinguished from other sampling approaches because it emphasises selection of data to generate a theoretical understanding rather than focusing on statistical adequacy of a sample [49]. Further these concepts are aggregated to achieve theoretical saturation, via which categories are generated. Based on these concepts and categories the guidance note of blockchain application for vendors and potential adopters was subsequently generated.

## 3. Supply Chain Resilience

Globalization has stimulated organisations to change their strategies to expedite response time and consequently, conventional competition amongst organizations has been transformed into a race between whole supply chains that foregrounded supply chain management and SCR [27,50]. A supply chain is a group of specialists such as supplier, manufacturer, distributor and retailer that create chains through service and production by maintaining a flow of goods and information [50]. It comprises a set of facilities that help in purchasing required materials, transforming them into intermediate or finished goods, eventually distributing these goods to customers [51]. Conversely, supply chain management characterizes planning and control of all business processes, activities regarding the sourcing, inventory and logistics along with coordination and collaboration with other participants in the supply chain [52]. The main objective of supply chain management is to deliver superior customer value by integrating supply and demand management within each organisation as well as whole supply chains [17]. However, the formation of supply chains is scattered globally with different parts of the chain located in different geographical locations; this increases supply chains' vulnerability to disruptions [12,23,53]. This is because, every actor in the supply chain is affected differently by external impacts such as environmental, social, economic and political factors [17,54]. Mitigation or eradication of such risks, can be achieved by integration of the entire supply network and by improving transparency and visibility amongst supply chain participants, which eventually augments SCR [22]. The term resilience has been used in different subjects such as psychology, ecology, economy, social and organisational concepts to denote the ability of a given system to return to a state of equilibrium after temporary disturbance [28]. While, some authors cf. [55,56] analogously accepted this definition in SCR area, others cf. [28,57] define resilience in supply chain as a capability of supply chains to develop preparedness against unforeseen disruptions to respond in a resourceful and timely manner and restore their former condition or preferably in an improved state.

Resilience in supply chains mitigates negative impacts of contingencies by identifying and adopting strategies and apposite plan of actions to recover to its original or better state [20]. A myriad of systematic literature review studies have been conducted to outline SCR strategies, metrics, capabilities and performance measures to identify barriers and enablers to resilience in supply chains [58]. A study by Bhamra et al. [59] discusses literature about resilience in small-to-medium-enterprises (SMEs) during the 1976–2010 timespan and accentuate on the importance of more case-study based empirical studies. Contrary to this view, scholars such as Pereira et al. [60], Tukamuhabwa et al. [21], Ali et al. [58] note the inadequacy of theoretical applications in SCR studies, while Datta [61] proposes using more context-specific interventions. Both Linnenluecke [62] and Sawyerr and Harrison [12] examine high reliability theories stressing the practicality of insights from high reliability studies for SCR improvement.

### 3.1. Supply Chain Resilience Metrics

Measuring resilience in supply chains has stimulated, scholars to define and delineate numerous metrics differently. Common terminologies used by authors to describe SCR metrics include: core dimension [63]; antecedents [20,57,64]; capabilities [65,66]; enablers [60,67]; competencies [68]; elements [55,58,69,70]; formative elements [12,65]; and dimensions [71]. Sawyerr and Harrison [12] conclude that from thirteen formative elements of SCR, ‘redundancy’, ‘human resource management’, ‘collaboration’, ‘agility’, ‘flexibility’, ‘culture’ and ‘risk avoidance’ resilience metrics can be applied to supply chains. The findings indicate that ‘collaboration’ with supply chain partners in the event of a disruption is the first prerequisite, because it improves other elements of resilience such as ‘visibility’, ‘awareness’ and ‘decision making’. More recent research by Shekarian and Parast [20] assess the impact of four common resilience elements, namely: ‘flexibility’, ‘agility’, ‘redundancy’ and ‘collaboration’ on alleviating demand, supply, process, control and environmental risks. Their findings [20] state that ‘collaboration’ is the most important strategy to cope with control disruptions, while ‘flexibility’ is found to be essential to mitigate demand, supply, process and environmental risks in supply chains. Conversely, Karl et al. [27] categorize thirteen elements of resilience into ‘pre-disruption’, ‘during-disruption’ and ‘post-disruption’ phases and analyse their relationship with ten common non-financial key performance indicators (KPI) of organizations. Using co-occurrence analysis, the authors [27] establish that ‘financial strength’ and ‘visibility’ resilience elements have no link to any organisational KPIs, whereas, ‘knowledge management’ present the highest co-occurrence with KPIs.

### 3.2. Blockchain Technology

According to Yoo [72] blockchain is a distributed ledger technology that allows participants in a network to exchange various transactional data between them. This distributed database maintains a constantly growing list of information records in a decentralized way, forming blocks that are protected against tampering and adjustments [72,73]. Blockchain technology is a platform on which various services and applications can be constructed [74]. Depending on the level of accessibility, this platform is differentiated with public, private and consortium types [75]. As the name suggests, public blockchain is a permissionless platform that is openly accessible to anyone to join the network, whereas a private type platform requires permission from network participants to join [76]. Bitcoin and Ethereum are the earliest and most widespread examples of a public type blockchain [77,78]. A consortium type blockchain is a hybrid approach of public and private platforms where network access is allocated to a group of pre-defined members [76,79]. Common aspects (or features) of blockchain technology adopted throughout industry are ‘trust’, ‘data security’, ‘traceability’, ‘smart contract’, ‘decentralization’ and ‘immutability’ [73]. Given this variety of features, extant literature claims that blockchain technology will transform businesses and improve the integration of economic and legal processes in the digital world [80,81]. Specifically, huge potential is anticipated in the automation of activities that

require disintermediation to reduce the number of intermediaries between producer and consumers during investments made, thus offering greater security and protection against cybercrime [1,82].

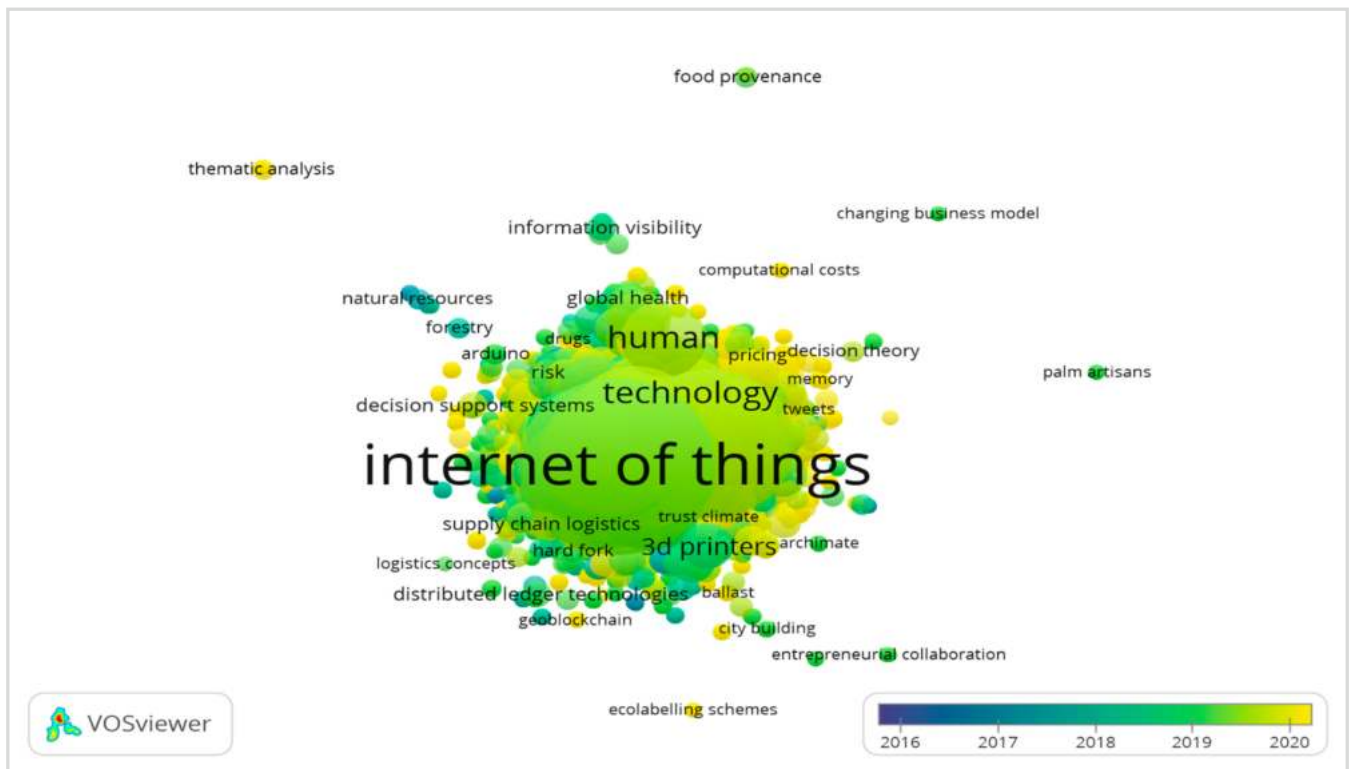
#### 4. Analysis and Findings

Network maps of scientometric data generated in VOS viewer comprise nodes signifying different items that present an object of interest such as publications, researchers, countries or keywords [35,83,84]. Generally, a map subsumes only one type of item hence, it is uncommon to incorporate, for instance, both publications and keywords in one network map [48]. The size of the network nodes conveys the numerical value of the item to be investigated: the greater the number of certain items occurring, the bigger the nodes [48]. Relationships between those nodes are depicted through links that connect pairs of investigated items. Links symbolize the strength or weight of a connection and therefore, in case the link between items has the strength of one, VOS viewer does not display the strength of link. Depending on the items being presented in those nodes, the links indicates different connections such as: bibliographic coupling links between publications, co-occurrence links between keywords or co-authorship links between researchers [48]. Similar to nodes, each map encompasses only one type of link between any pair of items. VOS viewer allows to create a citation, bibliographic coupling, keyword co-occurrence, co-authorship and co-citation analysis based on bibliometric data. For this present study citation analysis on 'sources', 'documents' and 'authors' units, along with, co-occurrence analysis on 'all keywords' unit had been selected.

##### 4.1. Co-Occurrence of Keywords

Visualization of keywords in a visualisation network provides a comprehensive image of existing knowledge and signposts the direction in which current studies are moving [85,86]. The network consists of nodes representing the volume of co-occurring keywords and links portraying the weight or number of publications in which two keywords occur together. With the purpose of achieving rich and comprehensive depiction of keywords in a co-occurrence map, 'all keywords' was selected instead of 'authors' keywords', as building a network on authors' keywords is constrained by authors' knowledge in terms of the number/range of word selections. Therefore, selecting all keywords is preferable approach, except for the situation when network map turns unmanageable and illegible because of the overflow of dataset. The resultant network map illustrated in Figure 2 consists of 4682 items, 61,338 links and 64 clusters.

From the list of keywords prior to network construction, terms 'blockchain', 'blockchain technology', 'supply chain', 'supply chain' and 'supply chain management' were purposefully eliminated from the list to improve visualisation. The network map reveals terms viz. 'internet of things' (IoT), '3D printing', 'digital storage' and 'tracking systems' to be predominate in the field highlighting the popularity of blockchain adoption in combination with those technological developments and its main usage in terms of tracking and tracing the goods in supply chains. All four keywords tend to occur particularly in 2018 and in the beginning of 2019 based on the colour-coded nodes. However, most recent keywords in bright yellow nodes exhibit the potential shift in the research focus. Specifically, 'environmental technology', 'sustainable development', 'sustainability', 'carbon emission' and 'sustainable supply chains' are the most recent keywords in bigger yellow nodes suggesting more recent momentum in the field towards sustainability concerns from earlier studies into cybercrime.



**Figure 2.** Overlay visualisation of co-occurrence of all keywords in the field of blockchain technology in supply chains.

#### 4.2. Key Authors, Papers, Countries and Journals

Data included in Table 1 describes the top ten most prolific sources, authors and countries and top ten mostly cited sources, authors and papers. Data was extracted from VOS viewer in the process of citation analysis and was manually sorted in a Microsoft Excel spreadsheet. Countries such as United States, India, United Kingdom and China are the most prominent in terms of publications and perhaps reflects the proportionate number of supply chains across those countries. As Singh et al. [50] suggest, most global supply chains are in USA, India, UK, China and Germany, which makes these countries most attracted to the field of supply chains and associated advanced technological developments in supply chains that could improve organisational performance. Additionally, an overlay visualisation of these indicators during citation analysis revealed that papers of those countries are predominantly from the period of 2018–2019 years, whereas developing countries such as Bangladesh, Peru, Chile, Kazakhstan, Iran, Turkey and Tunis have conducted and published studies predominantly in 2020. This geographical expansion proves that the proliferation of blockchain adoption and interest across all continents has gathered momentum but that developing countries lag behind this development pace.

**Table 1.** Key countries, sources, authors, documents [87–96].

<b>Top Ten Most Prolific Sources, Authors and Countries in Descending Order</b>					
<b>Sources</b>	<b>Papers</b>	<b>Author</b>	<b>Papers</b>	<b>Countries</b>	<b>Papers</b>
IEEE Access	35	Li Z.	10	United States	153
ACM International Conference Proceeding Series	22	Choi T.M.	9	China	126
Sustainability (Switzerland)	18	Wang Y.	9	India	117
International Journal of Production Research	17	Kumar A.	8	United Kingdom	73
IOP Conference Series: Earth and Environmental Science	17	Li J.	8	Germany	48
International Journal of Information Management	13	Queiroz M.M.	7	Australia	44
CEUR Workshop Proceedings	10	Sarkis J.	7	Italy	35
IFAC- Papers Online	9	Wang X.	7	Canada	31
Supply Chain Management	8	Gunasekaran A.	6	Korea	29
International Journal of Production Economics	8	Jayaraman R.	6	France	25
<b>Top Ten Most Cited Sources, Authors and Documents in Descending Order</b>					
<b>Sources</b>	<b>Citations</b>	<b>Authors</b>	<b>Citations</b>	<b>Documents</b>	<b>Citations</b>
IEEE Access	1118	Tian F.	643	Mengelkamp et al. [87]	472
International Journal of Production Research	1028	Sarkis J.	511	Tian [88]	422
International Journal of Information Management	597	Kouhizadeh M.	488	Saberi et al. [89]	340
Applied Energy	472	Gärtner J.	472	Casino et al. [90]	275
Supply Chain Management	452	Kessler S.	472	Ivanov et al. [91]	239
13th International Conference on Service Systems and Service Management-2016	422	Mengelkamp E.	472	Tian [92]	221
Sustainability (Switzerland)	308	Orsini L.	472	Kim and Laskowski [93]	187
Telematics and Informatics	275	Rock K.	472	Meng et al. [94]	177
Intelligent Systems in Accounting, Finance and Management	270	Weinhardt C.	472	Kshetri [95]	176
International Journal of Production Economics	259	Wang Y.	430	Bocek et al. [96]	169

Not surprisingly, ‘IEEE Access’ (an open-source and peer-reviewed journal) dominates the field with 35 publications (indicated in the first section of Table 1) and 1118 citations (in the second section of Table 1), as blockchain technology’s applications in terms of ‘data security’, ‘smart contracts’ and ‘distributed ledger platform’ attract more researchers from the technology field. IEEE Access is an electronic-archival journal published by the Institute of Electrical and Electronics Engineers that presents the results of research and developments across electronics engineering field of interest [97]. Based on the network visualisation map, the sources such as ‘International Journal of Information Management’



with 13 publications and 'International Journal of Production Research' with 17 publications have the most recent publications in this field, alongside being in the most productive top ten journals list.

The most prolific author in the field is Li, Z. with 10 papers, followed by Choi, T. and Wang, Y. with 9 papers in the field. Li, Z. is an academic from Guangdong University of Technology in China, renowned in Engineering, Computer Science and Social Sciences subject areas. Three of Li's papers are on the traceability aspect of blockchain technology in food supply chains, while six other publications are a combination of different blockchain technology applications in industry and service. From the top ten list of authors with the most publications, Li, Z. has collaborated with Queiroz, M. A. and a more recent article by Li, Z. in the field of blockchain technology presents a content-analysis based literature review of blockchain adoption in food supply chains and offers four benefits and five associated challenges of blockchain adoption in this sector [73]. The four main benefits of blockchain technology adoption were: 'food traceability'; 'recall efficiency'; 'information transparency'; 'efficiency combined with IoT' while barriers to adoption were listed as: 'lack of deeper understanding of blockchain'; 'raw data manipulation'; 'getting all stakeholders'; 'buy-in unanimously'; 'deficiency of regulation' and 'technology difficulties' [73]. In terms of highly cited documents in the field, an article by Mengelkamp et al. [87] prevails placing all six authors (namely: Mengelkamp, E., Kessler, S., Gärtner, J., Orsini, L., Rock, K. and Weinhardt, C.) fourth after Tian, F. with 643 citations, Sarkis, J. with 511 citations and Kouhizadeh, M. with 488 citations. Tian, F. has only two articles in the field in 2016 and 2017, both of which are frequently cited by other academics. Both studies are on applications of blockchain traceability feature in combination with IoT and RFID in food supply chains. In contrast, the study by Mengelkamp et al. [87] is conducted in blockchain based local energy trading. This case-study based research [87] concludes that blockchain technology is appropriate to operate in a decentralized microgrid energy market, as it meets their seven identified market components delineated upon in their study's framework.

#### 4.3. Findings from Grounded Theory Analysis

Based on extensive manual screening of topics and abstracts mined from Scopus in thematic analysis, the field of blockchain technology in supply chains generated six thematic clusters as illustrated in the Figure 3. Emergent themes of 'case study', 'challenges and opportunity', 'traceability', 'smart contract', 'blockchain and IoT' and 'data security' have been observed. The graph demonstrates a trend of publications in each cluster respectively which covers a timespan from 2016 and 2020.

In order to maintain consistency between the aim of this study and processes taken to achieve them, the 'case study' (with 89 papers) and 'data security' (with 27 papers) thematic groups were selected to study in grounded theory analysis; albeit, only the case study cluster was analysed further for this present research. During the analysis of the 'case study' cluster publications in NVivo, 19 nodes emerged to be nascent concepts in the initial open-coding stage. As a result of iterative subsequent coding stages, concepts were aggregated into categories. Consequently, three main categories of 'case studies', 'application of blockchain with other technologies' and 'blockchain technology in different industries' were generated. In the 'case study' category different examples of blockchain project (e.g., credit evaluation system [10]; tracking system for medicine traceability [79]; carbon trading, tracking [98]) in different industries (e.g., food supply chains, pharmaceutical, shipping, construction and oil gas) were identified. Some of the examples were case studies and pilot projects and others were various use cases that could be adopted as proof of concepts that required further development and testing. Concepts such as 'trust', 'traceability', 'cybersecurity', 'smart contract' and 'distributed ledger technology' were developing from the analysis to be the main features of blockchain technology. Further, all identified concepts and categories were analysed in cluster analysis (refer to Figure 4).

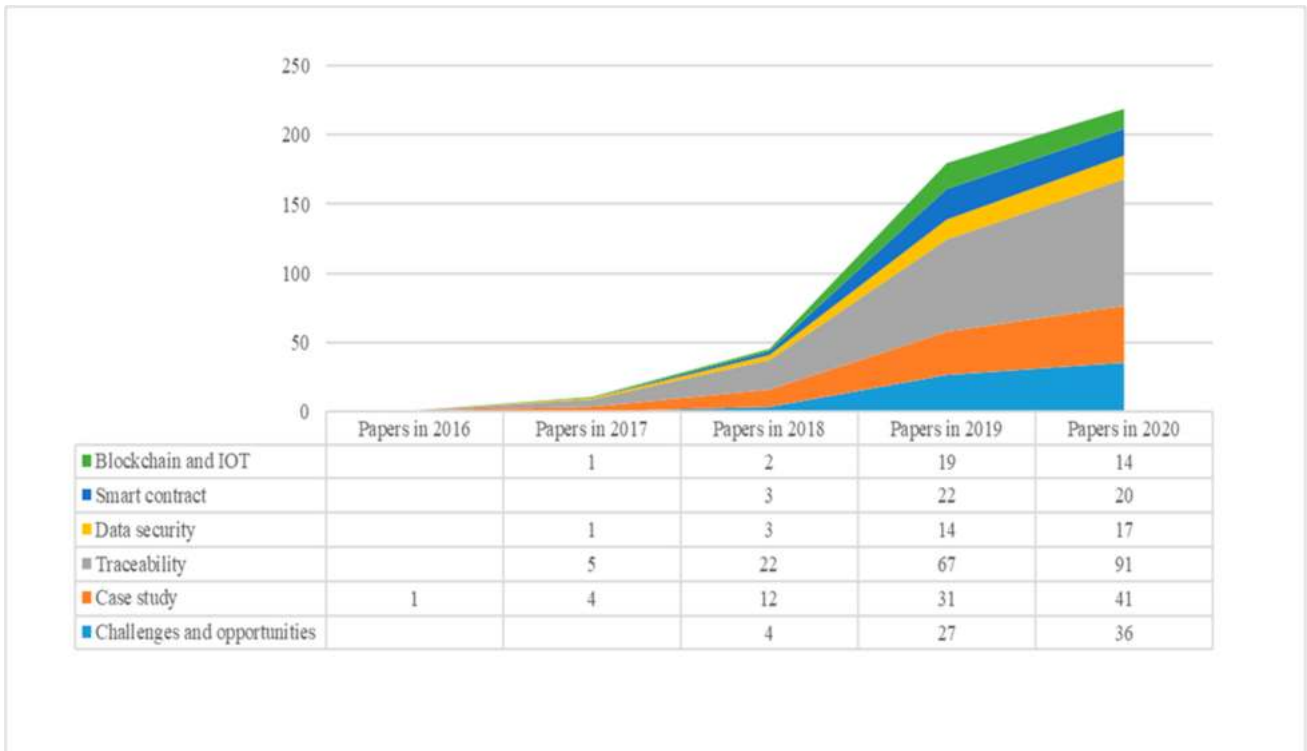


Figure 3. Trend of publication number in identified clusters.

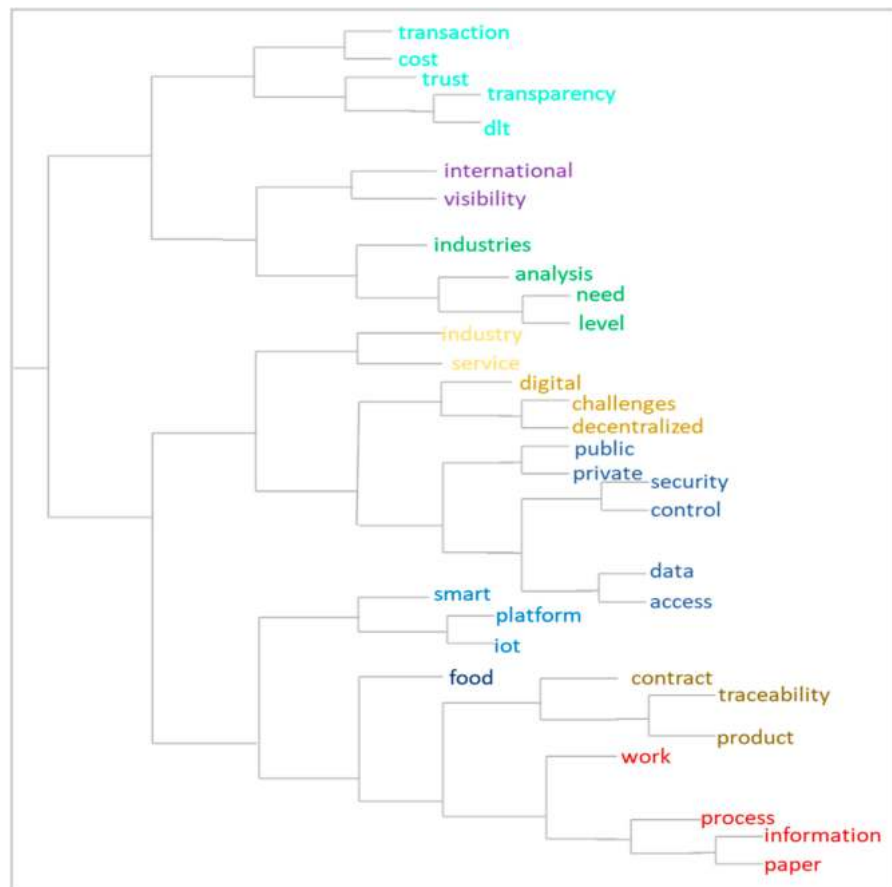


Figure 4. Clusters in grounded theory analysis.

The dendrogram was created selecting 33 most frequently occurring keywords with minimum length of three words in NVivo word frequency query. Stemmed words with similar meaning were filtered by adding them to 'stop words list'. For a similarity metric to form clusters 'Pearson correlation coefficient' was selected, which means that words that have higher degree of similarity based on their occurrence and frequency are shown clustered together and words with lower degree of similarity are displayed further apart. The formation of these clusters demonstrates three main branches (in Figure 4) that describe blockchain technology's main functions and their uses: 'trust and transparency in transactional use', 'data access and security use in public and private sectors' and 'smart contract and traceability system use for process improvement and information sharing'. From which the latter two branches together form the biggest cluster in the dendrogram stating about the most frequently used application of blockchain technology. For finer scrutiny of the impact of blockchain technology on SCR, keywords of SCR metrics were analysed in word frequency as depicted in word cloud in the Figure 5 to contrast them with the most cited 28 resilience metrics identified through preliminary literature review. Based on this analysis, it can be concluded that resilience metrics such as 'information sharing', 'integration', 'risk management', 'visibility' and 'collaboration' to be pivotal in the times of disruption. Moreover, adoption of blockchain technology augments these metrics by removing all the existing silos amongst supply chain participants and increasing connectivity and visibility between them.

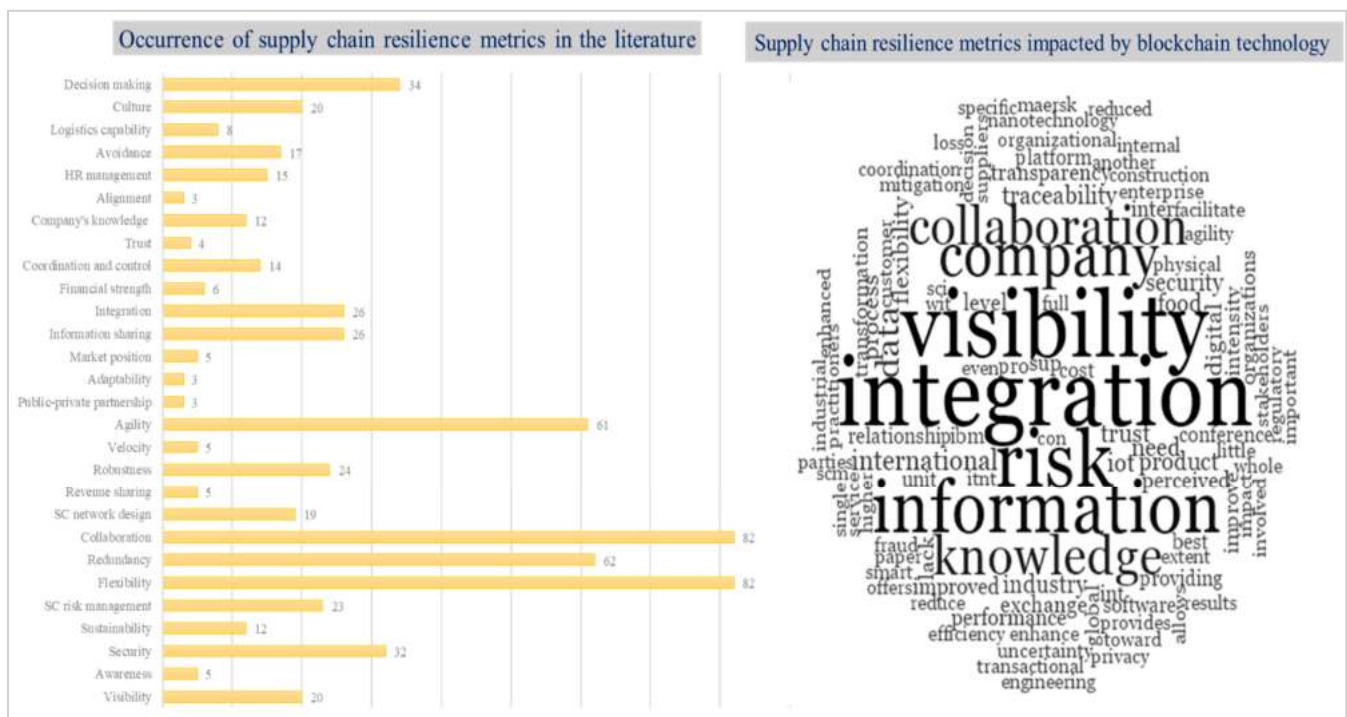
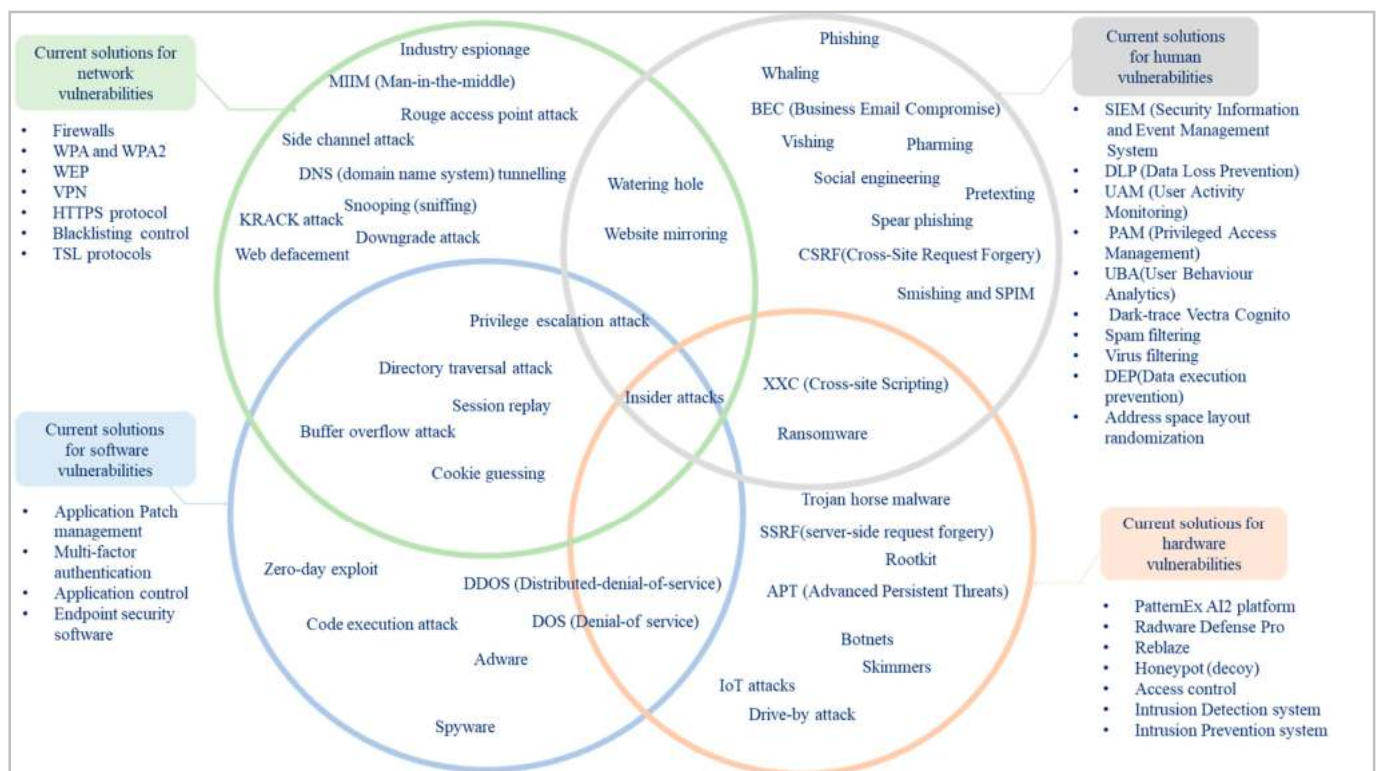


Figure 5. Word cloud depiction of supply chain resilience metrics in terms of their frequency of occurrence.

## 5. Discussion

Using both sets of analyses, it can be concluded that blockchain technology has implications on SCR in terms of 'visibility', 'risk management', 'integration', 'collaboration' and 'information sharing'. Other SCR metrics such as 'agility', 'flexibility', 'company's knowledge' and 'redundancy' were not at the centre of discussion by researchers who were studying blockchain applications. The 'visibility' metric tends to be improved in the cases of blockchain technology adoption in the form of traceability systems [80,99] whilst 'information sharing' and 'collaboration' metrics are enhanced in instances of blockchain technology adoption for distributed ledger technology features [82,100]. However, there

are some opponents of this idea of improving interconnectivity who claim the ever-growing connectivity itself to be a precursor for the cyberspace disruption caused by cyber-criminal attacks or cyber warfare [101]. Examples of cyber-attacks on financial entities' and organisations' information systems by targeting their: operational systems, data server, Supervisory Control and Data Acquisition (SCADA) control systems [101,102]; critical national infrastructure (CNI) [101]; industrial control systems (ICS) and internet of things (IoT) [103,104]. Such attacks in the public sector have given rise to the question as to whether blockchain technology is immune to criminal or nefarious activities in the digital world. Figure 6 depicts commonly known cyber-attacks (such as ransomware, Distributed Denial of Service (DDoS), phishing, IoT attacks, insider threat, AI/machine learning-based attacks, spear-phishing and web-based attacks)—each of which has different targets and different motives for interception or infiltration [105].

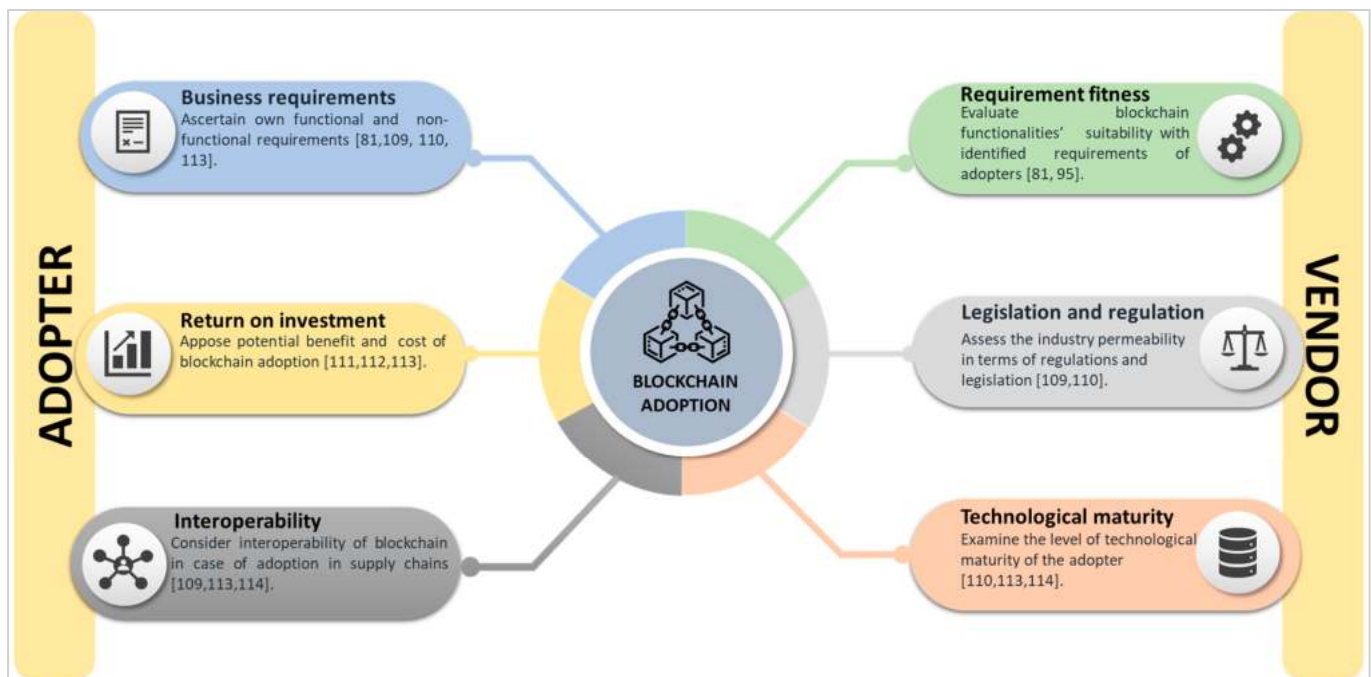


**Figure 6.** Common cyber-attack types categorized by their target types (people, hardware, software, network) and their current solutions.

The figure was developed based on the 'data security' cluster publications that describe four main attack vectors namely: software, people, network and hardware that adversaries exploit for data breach, data mining, cyber espionage, to obtain ransom or merely to cause chaos and disruption [101–104]. From four potential attack vectors, targeting people or staff of the organizations (e.g., by using phishing or spear-phishing technique) is the most vulnerable and easy threat vector for cyber-attackers [106]. In addition to these potential vulnerabilities to cyber-attacks, there is another inherent downside in traditional data storage method, namely: storing all critical digital assets in a centralized way inadvertently creates a single point of failure and easy target for adversaries. As described in the Figure 6, multiple prevention, detection or remediation control tools are currently available to prevent already known cyber-attack types, yet there is no largely offered solutions against unknown attacks. A myriad of research has been conducted in this field; contrasting blockchain technology solutions with cloud computing [102,105] or with traditional databases [107,108] and claiming that single-point-of-failure type data storage

practices lead to the breach of mission critical data. This in turn poses a tangible threat to individuals, organization and consequently to the whole supply chains [102].

Because blockchain technology provides permanent record-keeping of all data with their authorized entrance source in a tamper-proof and decentralized way, it retains the intrinsic potential to address the issues associated with both easy attack vector and single-point-of-failure weakness alluded earlier [107]. With blockchain technology all data shared in a network are performed in an encrypted version which creates another layer of protection against the intrusion or data breach that usually occurs on network level attack vector. Single point of failure risk is eliminated with decentralization; while threat of insider attack (from people attack vector) is eradicated with the traceability capability of permanent record (supported by a digital signature feature) of all the transactions performed by legitimate users in the permissioned network. However, despite all these potential benefits of improving resilience against multiple occurring disruptions in the ‘physical’ and ‘digital world’, prevailing literature also reveals numerous challenges associated with blockchain implementation for both vendors and adopters. This problem enhances the importance of developing guidance (as a theoretical framework) for potential adopters and vendors (refer to Figure 7).



**Figure 7.** Theoretical framework for blockchain technology adopters and vendors [81,95,109–114].

As the main success factor for new technology adoption is to prevent misalignment between organizational requirements and technological propositions, potential adopters should clearly define their own needs based on which select corresponding application and functionalities of blockchain technology [81,108,110]. Similarly, vendors are required to assess the suitability of organisations’ needs and available blockchain solutions [81,95]. For measuring a return on investment (ROI), the potential value and cost of new technological solution must be considered [111–113]. For instance, adopting a traceability system is worthwhile for high value goods (such as diamonds) in order to prevent counterfeit [95] or products with greater risk of contamination (such as medicine or dairy and meat products) [81,110]. Whereas, software developers or vendors should assess the feasibility and adaptability level of the industry the adopter is operating in, to ensure the successful adoption of proposed solution [109,110]. Lastly, it is compulsory for adopters to consider interoperability of their selected blockchain solution within supply chains, as the merits of this disruptive technology are leveraged through broad acceptance rather

than being limited to one organization only [109,113,114]. Moreover, vendors should evaluate the technological maturity level of potential adopters for successful adoption of the technology [110,113,114].

## 6. Conclusions

The findings of this present study suggest that the field of blockchain technology remains embryonic and yet, the field is also rapidly evolving to meet societal, economic and political needs. However, despite several introduced proposals and use cases by researchers cf. [1,10,100,112,115,116] there is still a notable deficiency of applications of blockchain technology in supply chains in real world contexts. Moreover, most use cases lack standard methods to design and consequently validate the blockchain solutions [112]. According to Deloitte Insights [117] only 8% of blockchain projects are continued, whereas the remaining initiatives tend to fail. This failure can perhaps be attributed to users (rather than organizations) who are developing stand-alone blockchain applications instead of foundational libraries that allow to create multiple applications [117]. Additionally, projects initiated by commercial organizations tend to have higher adoption rates compared to users' developments, as organizational blockchain projects are reportedly five times more likely to be copied [117]. This present study also reveals the latest trends and potential gaps within this systematic literature review that employed meta-analysis, thematic analysis and grounded theory analysis methods. The much-needed clarity provided by this present study will enable both researchers and practitioners to review the blockchain technology landscape and better understand developments in this field. Moreover, contributions of the present study can be recognised by achievement of aims and objectives delineated at the outset of this work, but also by practical implications in the form of cyber threat map and guidance note that elucidates upon requirements for both software developers and vendors. Different perspectives are provided about the value of this technology, not only to improve trust, time and cost effectiveness, but also to augment the overall SCR in the times of internal or external disruptions.

However, all indicated contributions carry some constraints and limitations that must be considered further. The guidance framework provided for adopters and vendors represent an indicative list of guidance and is by no means exhaustive. This list of guidance must be expanded in scope and enriched with more insights from applications of blockchain technology in real-world contexts; such work would expand upon the academic research literature studied in this paper—some of which may be based on pure theory not practice. With a substantial number of case studies in the field, studying the impact of each specific applications of blockchain technology (such as smart contract, traceability systems or DLT) on each resilience metrics could provide greater insights for practitioners and create new directions for enthusiastic researchers. Furthermore, solutions indicated in the cyber threat map are exclusively based on current tools and technologies used to prevent, detect or remediate the aftermath of disruption: the map does not cover available frameworks or standards to manage the risk and threat of cyber-attack occurrences.

Despite the initial precarious hype about blockchain technology with its introduction in cryptocurrency (specifically within the financial sector), its various applications with promising features became the reason for its proliferation. On the contrary, banks, insurers and brokerages have started to actively test ways of harnessing its merits. Because regulators have not yet determined certain standards around utilization of blockchain-based systems, (which is one of the challenges of blockchain adoption) this initial interest by financial sector could serve as a starting point for policymakers to develop and apply formal regulations. Currently the International Organization for Standardization (ISO) is developing the ISO/TC307 standard that will contribute towards establishing market confidence and augment proper adoption of the technology [118]. However, there remains a caveat to blind widespread adoption of blockchain technology, as the most common reason of technology adoption projects' failure tends to occur because of the misfit between organisational requirements and technological proposition. Therefore, for successful

blockchain technology adoption, adopters should rigorously ascertain their own needs first, then identify their functional and non-functional requirements from this technology. In conclusion, as with every technological adoption, the main point to consider is that any technology is merely an enabler and not the panacea to a problem that organizations hope to tackle. Therefore, other organisational aspects such as processes and particularly people must be considered, as staff resistance to changes implemented is another reason of most project failures. This aspect is particularly pivotal in blockchain adoption, as its merits can be leveraged only when multiple stakeholders implement collectively. Otherwise, interoperability of different blockchain applications could be another difficulty they face.

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

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

**Institutional Review Board Statement:** The study was conducted according to an ethical protocol that was approved by the Computing, Engineering and the Built Environment Faculty Academic Ethics Committee) of Birmingham city University (Edwards/#7741/sub1/Mod/2020/Sep/CEBE FAEC—BNV6200 ACM Version D.J. Edwards—13 October 2020).

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

**Data Availability Statement:** Data is available from the corresponding author upon written request and subject to review.

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

## References

1. Crosby, M.N.; Pattanayak, P.; Verma, S.; Kalyanaraman, V. BlockChain Technology: Beyond Bitcoin. Applied Innovation Review 2016. Available online: <https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf> (accessed on 1 May 2021).
2. Qureshi, A.; Megias, D. Blockchain-based P2P multimedia content distribution using collusion-resistant fingerprinting. In Proceedings of the 2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC) IEEE, Lanzhou, China, 18–21 November 2019; pp. 1606–1615.
3. Hackius, N.; Petersen, M. Blockchain in logistics and supply chain: Trick or treat? Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. In Proceedings of the Hamburg International Conference of Logistics (HICL), Berlin, Germany, 12–13 October 2017; Volume 23, pp. 3–18.
4. Dobrovnik, M.; Herold, D.M.; Fürst, E.; Kummer, S. Blockchain for and in Logistics: What to Adopt and Where to Start. *Logistics* **2018**, *2*, 18. [CrossRef]
5. Ozdemir, A.I.; Ar, I.M.; Erol, I. Assessment of blockchain applications in travel and tourism industry. *Qual. Quant.* **2019**, *54*, 1549–1563. [CrossRef]
6. Gordon, W.; Wright, A.; Landman, A. Blockchain in Health Care: Decoding the Hype. NEJM Catalyst 2017. Available online: <https://catalyst.nejm.org/doi/full/10.1056/CAT.17.0523> (accessed on 1 May 2021).
7. Cichosz, S.L.; Stausholm, M.N.; Kronborg, T.; Vestergaard, P.; Hejlesen, O. How to use blockchain for diabetes health care data and access management: An operational concept. *J. Diabetes Sci. Technol.* **2019**, *13*, 248–253. [CrossRef] [PubMed]
8. Liu, Z.; Li, Z. A blockchain-based framework of cross-border e-commerce supply chain. *Int. J. Inf. Manag.* **2020**, *52*, 102059. [CrossRef]
9. Scott, B. *How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?* UNRISD Working Paper No. 2016-1; United Nations Research Institute for Social Development (UNRISD): Geneva, Switzerland, 2016.
10. Mao, D.; Wang, F.; Hao, Z.; Li, H. Credit evaluation system based on blockchain for multiple stakeholders in the food supply chain. *Int. J. Environ. Res. Public Health* **2018**, *15*, 1627. [CrossRef]
11. Potma, M. Blockchain to Restore Trust in Food Supply Chains? 2020. Available online: <https://waag.org/sites/waag/files/2019-01/Blockchain-trust-food-supply-sector-margo-potma-article.pdf> (accessed on 1 May 2021).
12. Sawyerr, E.; Harrison, C. Developing resilient supply chains: Lessons from high-reliability organisations. *Supply Chain Manag.* **2019**, *25*, 77–100. [CrossRef]
13. Maesa, D.F.; Mori, P. Blockchain 3.0 applications survey. *J. Parallel Distrib. Comput.* **2020**, *138*, 99–114. [CrossRef]

14. Escaith, H. Trade Collapse, Trade Relapse and Global Production Networks: Supply Chains in the Great Recession, Trade Relapse and Global Production Networks: Supply Chains in the Great Recession. 2019. Available online: [https://mpra.ub.uni-muenchen.de/18433/1/MPra\\_paper\\_18433.pdf](https://mpra.ub.uni-muenchen.de/18433/1/MPra_paper_18433.pdf) (accessed on 1 May 2021).
15. Hale, T.; Moberg, C.R. Improving supply chain disaster preparedness. *Int. J. Phys. Distrib. Logist. Manag.* **2005**, *35*, 195–207. [CrossRef]
16. Solano, B.A.; Campos, M.G. Dynamic impact on global supply chains performance of disruptions propagation produced by terrorist acts. *Transp. Res. Part E Logist. Transp. Rev.* **2014**, *61*, 1–12. [CrossRef]
17. 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**, *7*, 1–38. [CrossRef]
18. Reardon, T.; Bellemare, M.F.; Zilberman, D. How COVID-19 May Disrupt Food Supply Chains in Developing Countries. IFPRI Book Chapters: 78–80. Available online: <https://www.ifpri.org/blog/how-covid-19-may-disrupt-food-supply-chains-developing-countries> (accessed on 1 May 2021).
19. Barroso, A.P.; Machado, V.H.; Carvalho, H.; Cruz, M.V. Quantifying the Supply Chain Resilience. In *Applications of Contemporary Management Approaches in Supply Chains*; Tozan, H., Ertürk, A., Eds.; InTech: Saint Paul, MN, USA, 2015. [CrossRef]
20. Shekarian, M.; Mellat-Parast, M. An Integrative approach to supply chain disruption risk and resilience management: A literature review. *Int. J. Logist. Res. Appl.* **2020**, 1–29. [CrossRef]
21. Tukamuhabwa, B.R.; Stevenson, M.; Busby, J.; Zorzini, M. Supply chain resilience: Definition, review and theoretical foundations for further study. *Int. J. Prod. Res.* **2015**, *3*, 5592–5623. [CrossRef]
22. Namdar, J.; Li, X.; Sawhney, R.; Pradhan, N. Supply chain resilience for single and multiple sourcing in the presence of disruption risks. *Int. J. Prod. Res.* **2018**, *56*, 2339–2360. [CrossRef]
23. Rangel, D.A.; de Oliveira, T.K.; Leite, M.S.A. Supply chain risk classification: Discussion and proposal. *Int. J. Prod. Res.* **2015**, *53*, 6868–6887. [CrossRef]
24. Garvey, M.D.; Carnovale, S. The rippled newsvendor: A new inventory framework for modelling supply chain risk severity in the presence of risk propagation. *Int. J. Prod. Econ.* **2020**, *228*, 107752. [CrossRef]
25. Forrester, J.W. *Industrial Dynamics*; Massachusetts Institute of Technology: Cambridge, MA, USA; Jon Wiley and Sons: Hoboken, NJ, USA, 1962; ISBN 978-0-2620-6003-5.
26. Morán, F.; Carranza, O.; Antún, J.P. Supply Chain Dynamics, a Case Study on the Structural Causes of the Bullwhip Effect. *Ing. Investig. Tecnol.* **2006**, *7*, 29–44. Available online: [http://www.scielo.org.mx/scielo.php?script=sci\\_arttext&pid=S1405-774320060001000003](http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-774320060001000003) (accessed on 1 May 2021).
27. Karl, A.A.; Micheluzzi, J.; Leite, L.R.; Pereira, C.R. Supply chain resilience and key performance indicators: A systematic literature review. *Products* **2018**, *28*, 20. [CrossRef]
28. Silva, A.; Lea, W.; Pereira, C. The contribution of Purchasing/Supply Management to Supply Chain Resilience: Insights about an Emerging Market 2016. Available online: <https://www.pomsmeetings.org/ConfProceedings/065/Full%20Papers/Final%20Full%20Papers/065-1697.pdf> (accessed on 1 May 2021).
29. GEODIS. Geodis White-Paper. 2018. Available online: <https://geodis.com/sites/default/files/2019-03/170509> (accessed on 1 May 2021).
30. BCI. Business Continuity Institute: Supply Chain Resilience Report 2018. Available online: <https://www.thebci.org/uploads/assets/uploaded/c50072bf-df5c-a5e1876aafb15bd0.pdf> (accessed on 1 June 2021).
31. Roberts, C.J.; Pärn, E.A.; Edwards, D.J.; Aigbavboa, C. Digitalising asset management: Concomitant benefits and persistent challenges. *Int. J. Build. Pathol. Adapt.* **2018**, *36*, 152–173. [CrossRef]
32. Al-Saeed, Y.; Edwards, D.; Scaysbrook, S. Automating construction manufacturing procedures using BIM digital objects (BDOs): Case study of knowledge transfer partnership project in UK. *Constr. Innov.* **2020**, ahead-of-print. [CrossRef]
33. Spellacy, J.; Edwards, D.J.; Roberts, C.J.; Hayhow, S.; Shelbourn, M. An investigation into the role of the quantity surveyor in the value management workshop process. *J. Eng. Des. Technol.* **2020**, *19*, 423–445. [CrossRef]
34. Smith, J.; Edwards, D.J.; Martek, I.; Chileshe, N.; Roberts, C.; Hayhow, S. The antecedents of construction project change: An analysis of design and build procurement application. *J. Eng. Des. Technol.* **2021**, *12*, 507. [CrossRef]
35. Chamberlain, D.; Edwards, D.J.; Lai, J.; Thwala, W.D. Mega event management of formula one grand prix: An analysis of literature. *Facilities* **2019**, *37*, 1166–1184. [CrossRef]
36. Nazir, F.; Edwards, D.J.; Shelbourn, M.; Martek, I.; Thwala, W.D.; El-Gohary, H. Comparison of modular and traditional UK housing construction: A bibliometric analysis. *J. Eng. Des. Technol.* **2020**, *19*, 164–186. [CrossRef]
37. Edwards, D.J.; Akhtar, J.; Rillie, I.; Chileshe, N.; Lai, J.; Roberts, C.; Ejohwomu, O. Systematic analysis of driverless technologies. *J. Eng. Des. Technol.* **2021**. [CrossRef]
38. Aghimien, D.; Aigbavboa, C.; Oke, A.; Edwards, D.J.; Thwala, W.D.; Roberts, C. Dynamic Capabilities for Digitalisation in the AECO sector—A Scientometric Review. *Eng. Constr. Archit. Manag.* **2021**. [CrossRef]
39. Bryman, A. *Social Research Methods*, 4th ed.; Oxford University Press: Oxford, NY, USA, 2012; ISBN 978-0-1996-8945-3.
40. Saunders, M.N.K.; Lewis, P.; Thornhill, A. *Research Methods for Business Students*, 8th ed.; Pearson: New York, NY, USA, 2019; ISBN 978-1-2922-0878-7.
41. Edwards, D.J.; Pärn, E.A.; Sing, C.P.; Thwala, W.D. Risk of excavators overturning: Determining horizontal centrifugal force when slewing freely suspended loads. *Eng. Constr. Archit. Management.* **2019**, *26*, 479–498. [CrossRef]



42. Levers, M.J.D. Philosophical paradigms, grounded theory, and perspectives on emergence. *SAGE Open* **2013**, *3*, 2158244013517243. [CrossRef]
43. Ghosh, A.; Edwards, D.J.; Hosseini, M.R. Patterns and trends in internet of things (IoT) Research: Future applications in the construction industry. *Eng. Constr. Archit. Manag.* **2020**, *28*, 457–481. [CrossRef]
44. Oshodi, O.; Edwards, D.J.; Lam, K.C.; Olanipekun, A.; Aigbavboa, C. Construction output modelling: A systematic review. *Eng. Constr. Archit. Manag.* **2020**, *27*, 2959–2991. [CrossRef]
45. Emmanuel, N.J. Analysis of Saunders Research Onion, Thesis Mind. Available online: <https://thesismind.com/analysis-of-saunders-research-onion/> (accessed on 1 July 2020).
46. Levitt, H.M.; Bamberg, M.; Creswell, J.W.; Frost, D.M.; Josselson, R.; Suárez-Orozco, C. Journal article reporting standards for qualitative primary, qualitative meta analytic, and mixed methods research in psychology: The APA Publications and Communications Board task force report. *Am. Psychol.* **2018**, *73*, 26–46. [CrossRef]
47. Hunter, J.E.; Schmidt, F.L. *Methods of Meta-Analysis: Correcting Error and Bias in Research Findings*, 2nd ed.; Sage: Thousand Oaks, CA, USA, 2004; ISBN 978-1-4129-0479-7.
48. Van Eck, N.J.; Waltman, L. VOS Viewer Manual: Manual for VOSviewer Version 1.6.11. 2019. Available online: [https://www.vosviewer.com/documentation/Manual\\_VOSviewer\\_1.6.11.pdf](https://www.vosviewer.com/documentation/Manual_VOSviewer_1.6.11.pdf) (accessed on 1 September 2020).
49. Creswell, J.W. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 4th ed.; Sage: Thousand Oaks, CA, USA, 2014; ISBN 978-1-5063-8676-8.
50. Singh, C.S.; Soni, G.; Bahotiya, G.K. Performance indicators for supply chain resilience: Review and conceptual framework. *J. Ind. Eng. Int.* **2019**, *15*, 105–117. [CrossRef]
51. Han, Y.; Chong, W.K.; Li, D. A systematic literature review of the capabilities and performance metrics of supply chain resilience. *Int. J. Prod. Res.* **2020**, *34*, 1–26. [CrossRef]
52. Queiroz, M.M.; Telles, R.; Bonilla, S.H. Blockchain and supply chain management integration: A systematic review of the literature. *Supply Chain Manag. Int. J.* **2019**, *25*, 241–254. [CrossRef]
53. Pires, R.J.; Barbosa, P.A. Supply chain resilience: Definitions and quantitative modelling approaches—A literature review. *Comput. Ind. Eng.* **2018**, *115*, 109–122. [CrossRef]
54. Mena, C.; Hoek, R.V.; Christopher, M. *Leading Procurement Strategy: Driving Value Through the Supply Chain*; Kogan Page, Limited: London, UK, 2018.
55. Christopher, M.; Peck, H. Building the Resilient Supply Chain. *Int. J. Logist. Manag.* **2004**, *15*, 1–14. [CrossRef]
56. Ali, I.; Gölgeci, I. Where is supply chain resilience research heading? A systematic and co-occurrence analysis. *Int. J. Phys. Distrib. Logist. Manag.* **2019**, *49*, 793–815. [CrossRef]
57. Ponomarov, S.Y.; Holcomb, M.C. Understanding the concept of supply chain resilience. *Int. J. Logist. Manag.* **2009**, *20*, 124–143. [CrossRef]
58. Ali, A.; Mahfouz, A.; Arisha, A. Analysing supply chain resilience: Integrating the constructs in a concept mapping framework via a systematic literature review. *Supply Chain Manag. Int. J.* **2017**, *22*, 16–39. [CrossRef]
59. Bhamra, R.S.; Dani, S.; Burnard, K.J. Resilience: The concept, a literature review and future directions. *Int. J. Prod. Res.* **2011**, *49*, 5375–5393. [CrossRef]
60. Pereira, C.R.; da Silva, A.L.; Tate, W.L.; Christopher, M. Purchasing and supply management (PSM) contribution to supply-side resilience. *Int. J. Prod. Econ.* **2020**, *228*, 107740. [CrossRef]
61. Datta, P. Supply network resilience: A systematic literature review and future research. *Int. J. Logist. Manag.* **2017**, *28*, 1387–1424. [CrossRef]
62. Linnenluecke, M.K. Resilience in Business and Management Research: A Review of Influential Publications and a Research Agenda. *Int. J. Manag. Rev.* **2015**, *19*, 4–30. [CrossRef]
63. Ponis, S.; Koronis, E. Supply Chain Resilience: Definition of Concept and Its Formative Elements. *J. Appl. Bus. Res. (JABR)* **2012**, *28*, 921–930. [CrossRef]
64. Scholten, K.; Schilder, S. The role of collaboration in supply chain resilience. *Supply Chain Manag. Int. J.* **2015**, *20*, 471–484. [CrossRef]
65. Jüttner, U.; Maklan, S. Supply chain resilience in the global financial crisis: An empirical study. *Supply Chain Manag. Int. J.* **2011**, *16*, 246–259. [CrossRef]
66. Pettit, T.J.; Croxton, K.L.; Fiksel, J. The Evolution of Resilience in Supply Chain Management: A Retrospective on Ensuring Supply Chain Resilience. *J. Bus. Logist.* **2019**, *40*, 56–65. [CrossRef]
67. Soni, U.; Jain, V.; Kumar, S. Measuring supply chain resilience using a deterministic modeling approach. *Comput. Ind. Eng.* **2014**, *74*, 11–25. [CrossRef]
68. Wieland, A.; Wallenburg, C.M. The influence of relational competencies on supply chain resilience: A relational view. *Int. J. Phys. Distrib. Logist. Manag.* **2013**, *43*, 300–320. [CrossRef]
69. Peck, H. Drivers of supply chain vulnerability: An integrated framework. *Int. J. Phys. Distrib. Logist. Manag.* **2005**, *35*, 210–232. [CrossRef]
70. Hohenstein, N.-O.; Feisel, E.; Hartmann, E.; Giunipero, L. Research on the phenomenon of supply chain resilience. *Int. J. Phys. Distrib. Logist. Manag.* **2015**, *45*, 90–117. [CrossRef]

71. Stevenson, M.; Spring, M. Flexibility from a supply chain perspective: Definition and review. *Int. J. Oper. Prod. Manag.* **2007**, *27*, 685–713. [CrossRef]
72. Yoo, S. Blockchain based financial case analysis and its implications. *Asia Pac. J. Innov. Entrep.* **2017**, *11*, 312–321. [CrossRef]
73. Duan, J.; Zhang, C.; Gong, Y.; Brown, S.; Li, Z. A Content-Analysis Based Literature Review in Blockchain Adoption within Food Supply Chain. *Int. J. Environ. Res. Public Health* **2020**, *17*, 1784. [CrossRef] [PubMed]
74. Scully, P.; Höbig, M. Exploring the impact of blockchain on digitized Supply Chain flows: A literature review. In Proceedings of the Sixth International Conference on Software Defined Systems (SDS), Rome, Italy, 10–12 June 2019; pp. 278–283.
75. Oh, J.; Shong, I. A case study on business model innovations using Blockchain: Focusing on financial institutions. *Asia Pac. J. Innov. Entrep.* **2017**, *11*, 335–344. [CrossRef]
76. Barghuthi, N.B.; Ncube, C.; Said, H. State of Art of the Effectiveness in Adopting Blockchain Technology—UAE Survey Study. In *2019 Sixth HCT Information Technology Trends (ITT)*; Institute of Electrical and Electronics Engineers (IEEE): Ras Al Khaimah, United Arab Emirates, 2019; pp. 54–59.
77. Corbet, S.; Lucey, B.; Yarovaya, L. Date-stamping the Bitcoin and Ethereum bubbles. *Financ. Res. Lett.* **2018**, *26*, 81–88. [CrossRef]
78. Mensi, W.; Al-Yahyaee, K.H.; Kang, S.H. Structural breaks and double long memory of cryptocurrency prices: A comparative analysis from Bitcoin and Ethereum. *Finance Res. Lett.* **2019**, *29*, 222–230. [CrossRef]
79. Bryatov, S.R.; A Borodinov, A. Blockchain technology in the pharmaceutical supply chain: Researching a business model based on Hyperledger Fabric. *CEUR Work. Proc.* **2019**, *2416*, 134–140. [CrossRef]
80. Czachorowski, K.; Solesvik, M.; Kondratenko, Y. The Application of Blockchain Technology in the Maritime Industry. In *Green IT Engineering: Social, Business and Industrial Applications*; Kharchenko, V., Kondratenko, Y., Kacprzyk, J., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 561–577, ISBN 978-3-0300-0252-7.
81. Chowdhury, M.J.M.; Ferdous, S.; Biswas, K.; Chowdhury, N.; Muthukkumarasamy, V. A survey on blockchain-based platforms for IoT use-cases. *Knowl. Eng. Rev.* **2020**, *35*, 19. [CrossRef]
82. Habib, M.A.; Sardar, M.B.; Jabbar, S.; Faisal, C.M.N.; Mahmood, N.; Ahmad, M. Blockchain-based Supply Chain for the Automation of Transaction Process: Case Study based Validation. In Proceedings of the International Conference on Engineering and Emerging Technologies (ICEET), Melbourne, Australia, 20–22 March 2020; pp. 1–7.
83. Akinlolu, M.; Haupt, T.C.; Edwards, D.J.; Simpeh, F. A bibliometric review of the status and emerging research trends in construction safety management technologies. *Int. J. Constr. Manag.* **2020**, 1–13. [CrossRef]
84. Newman, C.; Edwards, D.; Martek, I.; Lai, J.; Thwala, W.D.; Rillie, I. Industry 4.0 deployment in the construction industry: A bibliometric literature review and UK-based case study. *Smart Sustain. Built Environ.* **2020**, ahead-of-print. [CrossRef]
85. Darko, A.; Chan, A.P.; Adabre, M.A.; Edwards, D.J.; Hosseini, M.R.; Ameyaw, E.E. Artificial intelligence in the AEC industry: Scientometric analysis and visualization of research activities. *Autom. Constr.* **2020**, *112*, 103081. [CrossRef]
86. Shirowzhan, S.; Sepasgozar, S.M.; Edwards, D.J.; Li, H.; Wang, C. BIM compatibility and its differentiation with interoperability challenges as an innovation factor. *Autom. Constr.* **2020**, *112*, 103086. [CrossRef]
87. Mengelkamp, E.; Gärttner, J.; Rock, K.; Kessler, S.; Orsini, L.; Weinhardt, C. Designing microgrid energy markets. *Appl. Energy* **2018**, *210*, 870–880. [CrossRef]
88. Tian, F. An agri-food supply chain traceability system for China based on RFID blockchain technology. In Proceedings of the 13th International Conference on Service Systems and Service Management (ICSSSM), Kunming, China, 24–26 June 2016; pp. 1–6. [CrossRef]
89. Saberi, S.; Kouhizadeh, M.; Sarkis, J.; Shen, L. Blockchain technology and its relationships to sustainable supply chain management. *Int. J. Prod. Res.* **2019**, *57*, 2117–2135. [CrossRef]
90. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2019**, *36*, 55–81. [CrossRef]
91. 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**, *57*, 829–846. [CrossRef]
92. Tian, F. A supply chain traceability system for food safety based on HACCP, blockchain Internet of things. In Proceedings of the 2017 International Conference on Service Systems and Service Management, Dalian, China, 16–18 June 2017; pp. 1–6. [CrossRef]
93. Kim, H.M.; Laskowski, M. Toward an ontology-driven blockchain design for supply-chain provenance. *Intell. Syst. Account. Financ. Manag.* **2018**, *25*, 18–27. [CrossRef]
94. Meng, W.; Tischhauser, E.W.; Wang, Q.; Wang, Y.; Han, J. When Intrusion Detection Meets Blockchain Technology: A Review. *IEEE Access* **2018**, *6*, 10179–10188. [CrossRef]
95. Kshetri, N.; Loukoianova, E. Blockchain Adoption in Supply Chain Networks in Asia. *IT Prof.* **2019**, *21*, 11–15. [CrossRef]
96. Bocek, T.; Rodrigues, B.B.; Strasser, T.; Stiller, B. Blockchains everywhere—A use-case of blockchains in the pharma supply-chain. In Proceedings of the 15th IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017; pp. 772–777. [CrossRef]
97. IEEE Access: The Multidisciplinary Open Access Journal. 2020. Available online: <https://ieeaccess.ieee.org/> (accessed on 17 August 2020).
98. Kadry, H. Blockchain Applications in Midstream Oil and Gas Industry. In Proceedings of the International Petroleum Technology Conference, Dhahran, Saudi Arabia, 13–15 January 2020.

99. Musah, S.; Medeni, T.D.; Soylu, D. (2019). Assessment of Role of Innovative Technology through Blockchain Technology in Ghana's Cocoa Beans Food Supply Chains. In Proceedings of the 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkey, 11–13 October 2019; pp. 1–12. Available online: <https://ieeexplore.ieee.org/document/8932936/> (accessed on 15 August 2020).
100. Gonczol, P.; Katsikouli, P.; Herskind, L.; Dragoni, N. Blockchain Implementations and Use Cases for Supply Chains—A Survey. *IEEE Access* **2020**, *8*, 11856–11871. [[CrossRef](#)]
101. Chelvachandran, N.; Kendzierskyj, S.; Shah, Y.; Jahankhani, H. Cyberwarfare—Associated Technologies and Countermeasures. In *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity. Advanced Science and Technologies for Security Applications*; Jahankhani, H., Kendzierskyj, S., Chelvachandran, N., Ibarra, J., Eds.; Springer: Cham, Switzerland, 2020. [[CrossRef](#)]
102. Kendzierskyj, S.; Jahankhani, H. Critical national infrastructure, C4ISR and cyber weapons in the digital age. In *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity. Advanced Sciences and Technologies for Security Applications*; Jahankhani, H., Kendzierskyj, S., Chelvachandran, N., Ibarra, J., Eds.; Springer: Cham, Switzerland, 2020. [[CrossRef](#)]
103. Pantserov, K.A. The malicious use of ai-based deepfake technology as the new threat to psychological security and political stability. In *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity. Advanced Science and Technologies for Security Applications*; Jahankhani, H., Kendzierskyj, S., Chelvachandran, N., Ibarra, J., Eds.; Springer: Cham, Switzerland, 2020. [[CrossRef](#)]
104. Sagay, A.; Jahankhani, H. Consumer awareness on security and privacy threat of medical devices. In *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity. Advanced Science and Technologies for Security Applications*; Jahankhani, H., Kendzierskyj, S., Chelvachandran, N., Ibarra, J., Eds.; Springer: Cham, Switzerland, 2020. [[CrossRef](#)]
105. Vähäkainu, P.; Lehto, M.; Kariluoto, A.; Ojalainen, A. Artificial Intelligence in Protecting Smart Building's Cloud Service Infrastructure from Cyberattacks. In *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity. Advanced Science and Technologies for Security Applications*; Jahankhani, H., Kendzierskyj, S., Chelvachandran, N., Ibarra, J., Eds.; Springer: Cham, Switzerland, 2020. [[CrossRef](#)]
106. Ibarra, J.; Jahankhani, H.; Beavers, J. Biohacking capabilities and threat/attack vectors. In *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity. Advanced Science and Technologies for Security Applications*; Jahankhani, H., Kendzierskyj, S., Chelvachandran, N., Ibarra, J., Eds.; Springer: Cham, Switzerland, 2020. [[CrossRef](#)]
107. Adeodato, R.; Pournouri, S. Secure implementation of e-governance: A case study about estonia. In *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity. Advanced Science and Technologies for Security Applications*; Jahankhani, H., Kendzierskyj, S., Chelvachandran, N., Ibarra, J., Eds.; Springer: Cham, Switzerland, 2020. [[CrossRef](#)]
108. Epiphaniou, G.; Bottarelli, M.; Al-Khateeb, H.; Ersotelos, N.T.; Kanyaru, J.; Nahar, V. Smart distributed ledger technologies in Industry 4.0: Challenges and opportunities in supply chain management. In *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity. Advanced Science and Technologies for Security Applications*; Jahankhani, H., Kendzierskyj, S., Chelvachandran, N., Ibarra, J., Eds.; Springer: Cham, Switzerland, 2020. [[CrossRef](#)]
109. Lakhanpal, V.; Samuel, R. Implementing Blockchain Technology in Oil and Gas Industry: A Review. In Proceedings of the SPE Annual Technical Conference and Exhibition, Dallas, TX, USA, 24–26 September 2018; Society of Petroleum Engineers. Available online: <http://www.onepetro.org/doi/10.2118/191750-MS> (accessed on 15 August 2020).
110. Erol, I.; Ar, I.M.; Ozdemir, A.I.; Peker, I.; Asgary, A.; Medeni, I.T.; Medeni, T. Assessing the feasibility of blockchain technology in industries: Evidence from Turkey. *J. Enterp. Inf. Manag.* **2021**, *34*, 746–769. [[CrossRef](#)]
111. Lu, Q.; Xu, X. Adaptable Blockchain-Based Systems: A Case Study for Product Traceability. *IEEE Softw.* **2017**, *34*, 21–27. [[CrossRef](#)]
112. Perboli, G.; Musso, S.; Rosano, M. Blockchain in Logistics and Supply Chain: A Lean Approach for Designing Real-World Use Cases. *IEEE Access* **2018**, *6*, 62018–62028. [[CrossRef](#)]
113. Sternberg, H.S.; Hofmann, E.; Roeck, D. The Struggle is Real: Insights from a Supply Chain Blockchain Case. *J. Bus. Logist.* **2021**, *42*, 71–87. [[CrossRef](#)]
114. Rogerson, M.; Parry, G.C. Blockchain: Case studies in food supply chain visibility. *Supply Chain Manag. Int. J.* **2020**, *25*, 601–614. [[CrossRef](#)]
115. Aste, T.; Tasca, P.; Di Matteo, T. Blockchain Technologies: The Foreseeable Impact on Society and Industry. *Computer* **2017**, *50*, 18–28. [[CrossRef](#)]
116. Akaba, T.I.; Norta, A.; Udokwu, C.; Draheim, D. A framework for the adoption of blockchain-based e-procurement systems in the public sector: A case study of Nigeria. In *Responsible Design, Implementation and Use of Information and Communication Technology*; Hattingh, M., Matthee, M., Smuts, H., Pappas, I., Dwivedi, Y.K., Mäntymäki, M., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2020; pp. 3–14. Available online: [http://link.springer.com/10.1007/978-3-030-44999-5\\_1](http://link.springer.com/10.1007/978-3-030-44999-5_1) (accessed on 1 June 2020).
117. Deloitte Insights. The Evolution of Blockchain Technology 2017. Available online: <https://www2.deloitte.com/us/en/insights/industry/financial-services/evolution-of-blockchain-github-platform.html> (accessed on 1 September 2020).
118. ISO. Standards by ISO/TC 307 Blockchain and Distributed Ledger Technologies. Available online: [www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0](http://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0) (accessed on 1 August 2020).