sustainability

Article

An ISM Modeling of Barriers for Blockchain/Distributed Ledger Technology Adoption in Supply Chains towards Cybersecurity

Niloofar Etemadi [1,2,*], Pieter Van Gelder [2] and Fernanda Strozzi [1]

[1] Centro Sulla Logistica e il Supply Chain Management, LIUC Università Carlo Cattaneo, Via Corso Matteotti 22, 21053 Castellanza, Italy; fstrozzi@liuc.it

[2] Faculty of Technology, Policy and Management, Delft University of Technology, Jaffalaan 5, 2628 BX Delft, The Netherlands; P.H.A.J.M.vanGelder@tudelft.nl

* Correspondence: netemadi@liuc.it

Abstract: Over the last few years, the increasing level of cyber risks derived from the growing connectedness of Industry 4.0 has led to the emergence of blockchain technology as a major innovation in supply chain cybersecurity. The main purpose of this study is to identify and rank the significant barriers affecting the implementation of blockchain technology as a key component of cyber supply chain risk management (CSCRM). This research relied on the "interpretive structural modeling (ISM)" technique in the structure of a hierarchical model to investigate the contextual relationships of identified challenges for blockchain adoption in CSCRM; it also classifies the influential challenges based on their driving and dependence powers. The results highlight that "cryptocurrency volatility" is the challenge at the top level of the hierarchy, implying weak driving power but it is strongly dependent on the other challenges. "Poor regulatory provisions", "technology immaturity", "dependent on input information from external oracles", "scalability and bandwidth issues", and "smart contract issues" are significant challenges for the adoption of blockchain in cyber supply chain risk management and are located at the bottom level of the hierarchy with higher driving power. The implications for theory and practice of the research are also highlighted.

Keywords: blockchain technology; cyber supply chain risk management; ISM; MICMAC

Citation: Etemadi, N.; Van Gelder, P.; Strozzi, F. An ISM Modeling of Barriers for Blockchain/Distributed Ledger Technology Adoption in Supply Chains towards Cybersecurity. *Sustainability* **2021**, *13*, 4672. https://doi.org/10.3390/su13094672

Academic Editor: Piera Centobelli

Received: 26 March 2021
Accepted: 19 April 2021
Published: 22 April 2021

1. Introduction

The vulnerability of international supply chains to cyber-attacks, such as the ones on Natanz uranium enrichment plant's controller in Iran in November 2010 [1] and Norsk Hydro's operations in the U.S. and Europe in 2019 [2], is becoming clear. "A cyberattack is any disturbance to this interdependent network that leads to loss of functionality, connectivity, or capacity" [3]. The cost of cyberattacks on Italian companies' data in 2018 has been estimated at an average of EUR 3 million for each cyber-attack [4].

The sources of cyber threats cover a lot of territories. The National Institute of Standards and Technology [5] reported several cyber concerns leading to disruption in the supply chain, such as the uncertainty of information security practices by lower-tier suppliers, vendors' software or hardware with some security vulnerabilities, risks of third-party data storage, and so on. Reference [6] also reported the first cyber victims of denial-of-service attacks on the websites of corporations, such as eBay, Amazon, and CNN, designed to disrupt the data traffic of a targeted server. As an additional example, in summer of 2017, a major shipping line calculated the estimated cyber-attack cost up of to Dollar 300 million, leading to some challenges to their clients' operations [7].

In recent years, the components of the 4th industrial revolution, such as Internet of things (IoT), Cloud Computing (CC), Big Data Analytics (BDA), Cyber-Physical Systems (CPS), and other automation technologies have transformed the way of operations in the supply chain. However, more than 900 million IoT devices were expected to be potentially under threat of cyber-attacks in 2020 [8]. Reference [9] also presented a comprehensive review on cybersecurity attacks, including data breach, tampering, Sybil attacks, malicious code injection, and so on, for IoT and industrial IoT devices.

With this in mind, relying on ICT and technical security solutions such as passwords, access controls, such as firewalls, and intrusion detection methods are not sufficient. This reflects a thought-provoking fact that invites the cybersecurity community to go beyond the traditional approaches and be aware of innovative solutions to confront cyber threats and adopt different potential technologies for securely executing supply chain operations.

With the advent of new technologies, such as the implementation of blockchain and distributed ledger technologies (DLTs), the mitigation of cyber risks in the end-to-end supply chain is possible with the integrity of data and systems [10,11].

The origin of DLTs is traced back to 1978 with a fault-tolerant consensus mechanism for the validation of information without relying on the intermediary's central authority in the systems [12,13]. As stated by Saur: "A distributed ledger is a type of digital data structure residing across multiple computer devices, generally at geographically distinguished locations" [14]. Distributed ledger technologies (DLTs) are a type of technology that enables the keeping and sharing of records in a decentralized manner.

Blockchain technologies are currently the most popular variant form of distributed ledger technologies. Blockchain is a cutting-edge technology that offers many solutions to overcome the challenges associated with CSCRM. Blockchain is a decentralized, distributed, and shared digital ledger that is used to store a copy of blocks of valid transactions across many computers, so that no record involved can be manipulated retroactively without a breakdown of the chain of blocks [15]. Blockchain can be described as a decentralized database for achieving information transparency and data security. Out of the numerous fields of blockchain and distributed ledger technologies (BDLT), applications, including finance, healthcare [16,17], food [18,19], smart cities [20] and government [15], and those related to cybersecurity have gained the attention of the research community over recent years [11,21–23]. The applications of blockchain in the cyber-resilient supply chain in the case of the automotive industry to guarantee data transparency, operational efficiency, traceability, diminishing costs, and fewer human interventions were also highlighted in the work of [24]. Blockchain-based CSCRM can be enabled by integrating with some smart technologies, such as Internet of Things to solve privacy and security vulnerabilities [25], big data analytics and cloud computing to increase real-time information exchange and material tracing by trusted users participating in the transactions [26,27]. Therefore, BDLTs ensure resiliency, the provenance of products, transparency, and reduce privacy leakage and fraudulent activities, providing trusted information inputs and outputs for CSCRM initiatives. Potential benefits of BDLT adoption include a tamper-proof database, improved cyber risk management, data privacy, auditability, and the storage of immutable data of a transaction through its intrinsic characteristics to improve cyber risk supply chain management.

Surprisingly, despite a promising future and vast advantages, BDLTs have not taken over the supply chain sufficiently to mitigate cyber risks. So far, the BDLT applications and financial benefits, transparency, and traceability requirements are mainly aligned in the literature and have received much more attention in the number of articles published by scholars. The challenges for the diffusion of blockchain are also addressed in a few studies, and most of these available studies are focused on the impediments to blockchain adoption in a general way, not in a specific domain. For instance, the statements in reference [28] try to discuss the scalability problems and perceived lack of value in the nascent blockchain market. Reference [29] declares that, despite the benefits of distributed ledgers that are usually mentioned in the literature, such as trust, integration, or transparency in the supply chain, the implementation of this technology is unlikely. To the best of our knowledge, there is not much research work focused on the intersection between cybersecurity, BDLTs, and the supply chain; none of these studies empirically address the linkage to challenges that impede the adoption of blockchain technology in cyber supply chain risk management.

To bridge the knowledge gap, the existing number of research articles indicate that there has been no study that has entirely focused on the various challenges that affect the adoption of blockchain connected to the concept of cyber supply chain risk management, which is something that is missing in the existing studies and that attempts to depict a conceptual model of the hierarchical structural relationship that is characterized by a two-phase methodology, namely (i) a graph-based "Interpretive Structural Modeling" (ISM), to impose the linkage among the CSCRM challenges, and (ii) a complimentary analysis, namely "Cross-Impact Matrix Multiplication to Classification" (MICMAC), to classify the strength of the relationship between the CSCRM challenges based on their driving and dependence power. The findings of this study are discussed alongside unique insights into the theoretical and practical implications of the investigated topic.

In this sense, this study sets out some questions as follows:

- What are the challenges of BDLT adoption for cyber supply chain risk management?
- What hierarchical relationships exist among identified challenges?
- Which challenges have more driving power and which challenges have more dependency power on the adoption of BDLT technologies in CSCRM?

To address these questions, the paper is structured as follows. Following the introduction and the literature review, the adopted research methodology and research design are presented. The findings obtained from the analysis, and the theoretical and managerial implications of the study are then discussed. Final remarks, limitations, and directions for future research conclude the paper.

2. Literature Review

2.1. Supply Chain Risk Management

Over the past decade, our knowledge and awareness of supply chain risk management (SCRM) have risen due to technological and market turbulence, volatile customer demand, along with competitive intensity [30]. A definition of supply chain risk is "the variation in the distribution of possible supply chain outcomes, their likelihoods, and their subjective values" [31]. According to [32–34], the most common disruption risks affecting the supply chain and, significantly, its performance are related to natural and manmade disasters (e.g., earthquakes, hurricanes and floods), cyber threats (human errors, failures and terrorism), while operational risks are related to a company's reduced ability to produce and supply products and services [35]. Operational risks also include capacity constraints, supply and demand uncertainty, information management risk, and business interruption [36].

Different innovative methods have been adopted to identify cyber threats in the supply chain, which is the first phase in the supply chain risk management approach [34,37]. Reference [38] states that a shift from the traditional information technology infrastructure to Industry 4.0 systems makes it possible to automate the identification of cyber risks and explore the effects of such systems. The fragility of the supply chain is evidenced by some cyber incidents, varying from counterfeiting, fraud, and data manipulation to the visibility of data across the supply chain.

The basis of these increased risks has led to the cyber supply chain risk management concepts that constitute the main objective of this paper.

2.2. Cyber Supply Chain Risk Management

Cyber supply chain risk management (CSCRM) is emerging as a new "management construct resulting from the fusion of approaches, methods, and practices from the fields of cybersecurity, information risk management, and supply chain management". Such approaches and practices lead to reshaping relationships between organizations and governments, improving the integration of cyber–physical systems, and establishing standards and protocols [39]. Building on the definition by [40], the term CSCRM was coined to refer to the policies, procedures, and controls to protect the operations of a supply chain from cyber and information risks. This concept requires a comprehensive assessment of dynamic capabilities, high-level technical skills, and human elements across the supply chain to prevent and deal with the outcome of disruptions deriving from the massive amount of connectivity of today's operational systems [41]. The aim of CSCRM is to gain security, reliability, and safety, along with the broader objectives of trustworthiness, integrity, and quality [42].

The challenges faced by global companies in successfully implementing CSCRM are linked to a large number of suppliers in an organization's supply base [43] (Bode and Wagner, 2015), to the growing technological change and evolving threats, and training programs for security and technical personnel to identify and mitigate risks [44]. To add to these growing complexities of CSCRM, standards and guidelines, regulatory frameworks, and non-transparent supply chain partners in the cyber space are constantly changing [39,45]. In this new area, a holistic approach through CSCRM, combining processes, people, and technology, is considered a necessity to deal with the challenges for enhancing cybersecurity.

In light of the abovementioned concept of CSCRM, cybersecurity models need to take into account the technological, organizational, or environmental requirements during long-term planning to confront cyber and information risks to achieve cybersecurity.

2.3. Blockchain and Distributed Ledger Technologies

Distributed technologies are a database applied to share or record data based on various distributed ledgers across multiple nodes in different geographic areas, accessible by multiple participants, of which the blockchain is the most popular one. Each device or system in the network is called a node. Unlike centralized systems, distributed ledgers do not have any central location to store information [46]. The first attempt to implement the DLT was in aircraft operations, where the first primitive DLT with a consensus mechanism was applied to deal with the cyber risks derived from some automatic errors in the system's components clocks that would have led to an exchange of incorrect information and the likely inability to schedule internal aircraft tasks, and finally the loss of functionality of the aircraft systems [12].

The concept of blockchain was invented in 2008 as a platform entitled Bitcoin by Satoshi Nakamoto [47]. Blockchain technology is widely evolved from blockchain 1.0, which led to its first application for cryptocurrency purposes with Bitcoin; blockchain 2.0, which relied on the execution of smart contracts to the Ethereum for the transaction of digital assets; blockchain 3.0, which is based on DApps, a decentralized application that avoids centralized infrastructure and runs on a distributed network; to blockchain 4.0, making blockchain applicable in business cases [48–52]. Fundamentally, blockchain is a chain containing a growing list of data about transactions, called blocks, which are added in chronological order and cryptographically linked together. According to [53], 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". Blockchain works by relying on a peer-to-peer (P2P) topology, and new data records are added to the network through a consensus mechanism based on authentication and validation from multiple participants [54]. In the context of a block structure in the chain, each block is identified by three fundamental elements, which are as follows: the cryptographic hash algorithm on the header of the block, the timestamp which reports time for each transaction, and a Merkle tree to store all the transaction with authenticity, integrity, and consistency [55].

Transactions constitute the main core of the block records. When a user wants to add a new transaction to the ledger as a new block, the new block is received by all other nodes, which accept it according to a consensus mechanism. The accepted block is then generated to the whole network. Each new block contains a hash of its header and connects to the previous block in the chain through cryptography [56].

The concept of a Merkle tree based on the hashes was coined in 1987 with the publication of a paper entitled "A digital signature based on conventional encryption function" by [57]. Merkle trees are also one of the crucial components of blockchain technology and allow a huge amount of data to be stored in a single hash value, known as a Merkle root [58]. The root hash of the hash tree is used to detect tampered data and enables a secure and timely validation of the transactions [25]. Furthermore, the block header hash allows the transactions to connect to the chain by embedding the prior block hash in the current block header. In this way, every transaction remains tamper-proof and cannot be manipulated or removed, and with any change in a specific block, all subsequent blocks will be invalid in the chain [59].

2.4. BDLTs Key Capabilities for Cybersecurity

Blockchain and DLTs are a promising technology, predicted to span many more sectors over the next few years [60]. The prosperity of BDLTs pertains to their inherent features; the range of advantages in the realization of the cybersecurity properties they provide to their members is presented below.

- **Decentralization:** Unlike a traditional centralized transaction system where transactions are verified by a trusted centralized agency, such as a central bank or a government, in a decentralized infrastructure, two parties can access the database without the need for a third party to keep records or perform authorization. Within traditional systems, risks related to human error or criminal activity remain unidentified. Furthermore, such centralization can have several downsides, including more charges, lower overall performance, and various failures in the systems on the part of service providers [61,62]. Distributed ledgers record transactions without the association of a third party, which is helpful in the reduction of service costs, the improvement of the efficiency of the chain, and mitigation of the risk of system failures [63].
- **Availability:** The National Institute of Standards and Technology (NIST) defines availability as “ensuring timely and reliable access to and use of information” [64]. Cyberattacks start to impact availability of technology services with vulnerabilities, such as counterfeiting, theft, fraud, data manipulation, or falsification [65]. The DLT solution based on its decentralization and peer-to-peer characteristics makes it more difficult for criminals to disrupt. However, one of the most common attacks, known as distributed denial-of-service (DDoS) attacks, can target internet services and networks with more traffic than the server or network can handle and, hence, some disruptions to blockchain solutions. As a result, with the availability of information in decentralized platforms of DLTs, a rise in DDoS attacks could be observed [66].
- **Data Access and Disclosure:** According to reference [67], blockchain is a “secure public ledger platform shared by all parties through the Internet or an alternative distributed network of computers”. Blocks with sets of information are shared between participants. The participants have the ability to share records and have limited access to their relevant transactions whenever they need them [68]. The decentralized nature of blockchain technology contributes to information sharing among relevant parties, helping transactions with high security from potentially targeted attacks or complex incidents [69].
- **Traceability:** BDLTs provide a wide range of capabilities, including traceable and tamper-resistant records, a high level of traceability with trusted information, accessibility, and the visibility of data provenance [70,71]. All blockchain transactions are given an exact timestamp when the transactions are added to the chain [46]. Such an inherited characteristic of blockchain enhances traceability and authenticity for the transaction of products, data, and interactions [72].
- **Transparency:** Current centralized systems in the supply chain deal with issues such as fraudulent activities, privacy and security errors, lack of transparency and trust [73]. Blockchain technologies are potential enablers of a trusted and efficient supply chain and can improve transparency and bring high visibility, authenticity, and availability to all the stakeholders in the network [74,75]. The secure and tamper-resistant mechanism of blockchain paves the way for greater transparency, increasing

the trustworthiness of transactions through interaction and access to the network among users [76].

- **Privacy and Security:** Blockchains or cryptographic-based distributed ledgers allow more integrity and information security than traditional databases because blockchain connects devices to the networks and members to devices, and encrypted transactions are added to the chain with the authorization of all participants without the need for data disclosure [23]. So, given the abovementioned advantage of the BDLTs, it is very difficult to hack this impenetrable technology.
- **Immutability:** Immutability in the blockchain refers to the high ability of technology to remain censorship-resistant and indelible [77]. Immutability enables the transformation of each new transaction into the chain and approval by a consensus mechanism. In addition, all the historical registered operations are immutable; therefore, any manipulation and forgery of data records would need a cyber-attacker to break most of a network's nodes [74].
- **Reduced Overall Cost:** Blockchain technologies help reduce the overall cost because of the direct transfer of transactions without the need for a bank or other third party. Costs related to documentation, tax services, auditing, and governance can potentially be reduced. Subsequently, the reduction of transaction costs that can be supported by blockchain technology would lead to eliminating cybersecurity incidents [78,79].
- **Data Quality:** BDLT does not ensure the quality of data but any blocks that contain low accuracy and quality of data will not be allowed to add to the chain. Blockchain guarantees transformation of accurate and impenetrable data faster than any other system, and facilitates entities in exchanging information in a protected way [66].
- **Distributed:** The validated transactions and updated records are synchronized into blocks for processing and protocols and supporting infrastructures allow every node or participant in different locations to receive a real-time transaction [80].

2.5. Applications of BDLTs Adoption in CSCRM

This section provides a comprehensive identification of the specific supply chain functions that can be connected by the use of blockchain and cybersecurity. The prior contributions of blockchain technologies adoption in the supply chain management have been highlighted with notable examples, including improved data security and smart contracts; digital trust and supply chain relationship management; the tracking of the possession of goods and the identity of suppliers [81,82]; governance and legal frameworks for the execution of blockchain [83]; physical access control management based on Hyperledger Fabric platform and the security of IoT networks [84,85]; and integration with cutting edge technologies for storing and transferring encrypted data to the edge nodes [86]. Based on the most cybersecurity focused blockchain applications, "Internet of things" and "Transaction data" have received the most attention from scholars interested in the intersection of BDLT and cybersecurity and supply chain. In order to understand how the blockchain can be adapted to support the security of IoT devices, reference [87] presented a cloud-based IoT platform in the combination of blockchain for executing cryptographic transactions through smart contracts to securely track data management and prevent malware infections in IoT devices. Other applications of blockchain in the form of authorities management, secure communication sessions, access control, and prevention of bandwidth saturation are provided in some contributions [85,88,89]. However, apart from the integration advantages in the IoT with BDLTs, there are some challenges arising from different elements, such as the low computational power and scalability issues of IoT devices for a huge amount of data transmission, and the inherent latency of blockchain technology [90].

In another class of blockchain adoption in CSCRM, data management is one of the most promising features of the blockchain. The management and protection of transaction data have become increasingly uncontrollable in a distributed environment. Implementations and applications based on this technology improve secure data sharing among stakeholders in the supply chain and are aimed at secure and verifiable data management [91]. Although successful and interoperable communications have not yet reached a secure level between parties in the supply chain, there are some examples in the literature from the cross-organizational data management perspective. In the study, [92] designed a DLT with a certification or endorsement mechanism which allows the exchange of consumer data without revealing the information in the pharmaceutical supply chain. The result shows that blockchain has the potential to mitigate the counterfeiting issues with the cross-supply chain workflow management while maintaining transactional privacy.

Blockchain is also disrupting the human resource sector [93,94] by revolutionizing working procedures and employment document storage [94]. In the case of data storage in the form of decentralized and non-reversible platforms, [56] addressed the importance of information sharing by a governance model, considering blockchain architecture among parties in the supply chain. Additionally, access control mechanisms, metadata supporting key functions, and the encryption and decryption of data are the key concepts for their blockchain architectural design. Blockchain applications appear to offer significant trust to the participants or connected devices in a supply chain network. Reference [95] proposed and developed a decentralized microgrid model for distributing transactions between producer and consumer without the regulation of a central authorization. Their BDLT mechanism enables data distribution for certified and trusted parties by using attribute-based signatures of multiple producers.

BDLTs are also considered an opportunity for protecting the security of data that encounter malicious cyberattacks [96–100].

Collaborative IDS (CIDS) [101] is an intrusion detection system using smart contracts to address data privacy issues. Self Organizing Maps (SOMs) [102] are artificial networks consisting of thousands of nodes that can be applied in BDLT systems to cluster categorical data to the entire nodes for enhancing data privacy and confidentiality, as well as monitoring the blockchain. In [103], the authors proposed a cryptographic system known as Zerocoin to verify transactions with anonymity and user privacy. Zerocash [104] is a decentralized currency to guarantee privacy preservation by applying zero-knowledge proof variant (zkSNARKs) and provide user privacy by protecting details of the transaction. Reference [105] highlighted the fact that the capabilities of machine learning can be combined with blockchains to explore malware activities.

Despite multiple contributions highlighting the importance given to capabilities of blockchain technologies from the perspective of privacy and security concerns in different types of BDLTs, e.g., public, private, and smart contract, there is still a need to be cautious about the security challenges facing BDL adoption. In spite of the immutable nature of distributed ledger technologies, they are still vulnerable to cyberattacks. Transaction anonymity and transparency can be obtained by blockchain, but this technology cannot guarantee the privacy of data, and identity fraud and data breaches can occur anytime [106,107]. For example, anonymity and privacy concerns are rising in the blockchain due to the disclosure risk of users' identity. The users' transaction information, such as the sender and receiver address, even if pseudonymous, and the value can be publicly accessed and be visible to all network participants. In this case, all personal user information, such as transaction contents (e.g., amounts, account balance, and spending patterns), can be tracked under unexpected failures or malicious cyberattacks [108].

Several works also focused on the risk of privacy leakage in smart contracts, which poses some challenges for data confidentiality and privacy for sharing data [109,110]. Reference [111] focused on the privacy of transactions in the smart contract platforms and proposed Hawk, a decentralized smart contract system, which gives an efficient cryptographic protocol maintaining transactional privacy. ShadowEth [109] is a private smart contract on Ethereum to execute and store all metadata in an off-chain trusted execution environment called TEE-DS.

In the case of data privacy management, the European Union (EU) presented the general data protection regulation (GDPR) in May 2018, which addresses regulatory hurdles and contributes to the development of international guidelines and regulations to facilitate the use of BDLTs for all organizations.

Currently, BDLTs are applied to a wide range of digital and virtual financial markets, market predictions, and capital investments [112]. The numerous types of cybersecurity threats can occur during information, physical, and financial flows between supply chain stakeholders due to technical vulnerabilities in the systems [113]. Blockchain is expected to bring some advantages to customers, industrial and commercial institutions, and society as a whole [114]. For instance, to facilitate future market prediction, Augur [115] is a decentralized protocol for the global prediction market, enabling users to trade shares without the need for a single entity. Plasma [116] is a "proposed framework for incentivized and enforced execution of smart contracts, which is scalable to a significant amount of state updates per second (potentially billions) enabling the blockchain to be able to represent a significant amount of decentralized financial applications worldwide". Gnosis [117] is a platform that enables the trade of digital assets and cryptocurrencies on Ethereum's new market mechanisms, and it is claimed to be a reliable forecasting tool for increasing knowledge of upcoming events in finance, government, and among other sectors.

Despite the hype around different BDLT platforms, the studies confirm that the complexity of financial flows can lead to some difficulties in managing cyber supply chain risks. As a result, security violation and cryptocurrency volatility, such as volatile digital coins and hacking wallets of cryptocurrency exchange, have diverse effects on the reputation of BDLT platforms [118].

3. Challenges for Blockchain/BDLT Adoption in CSCRM

In previous studies, researchers and practitioners have made an effort to point out the potential of BDLTs based on risk reduction, transparency, traceability, peer-to-peer transactions, data safety, and decentralization, which are the significant objectives of supply chain management [71,119–121]. The main purpose of this paper lies at the intersection of cybersecurity and blockchoichain/BDLTs. Although the literature on cybersecurity is not entirely new, there is plenty of room to explore it in the context of supply chain literature. In the literature, cybersecurity and blockchain/BDLTs align to address barriers related to Internet of things, data sharing, the prediction marketplace, cryptocurrency, privacy, and security [122–124], whilst the implementation of BDLTs for cyber supply chain risk management is still at the pilot stage. Stakeholders have to deal with numerous challenges during the adoption process of blockchain disrupting the existing CSCRM. This should be a driving force for researchers and practitioners to be always ready to promote and regulate new technologies, as per the risk maturity models, interoperability capabilities, support of leadership, and different governance policies. Sixteen challenges identified from the literature review in the adoption process of BDLTs into a cyber secure supply chain are discussed as follows, and are shown in Table 1.

3.1. Immature, Early Stage of Development

The concept of technological maturity is defined as the readiness level for blockchain technology adoption since its first appearance. There is a potential for SMEs to understand the value of mature technology and adopt it to enrich their activities [125]. Despite the hype around the use of BDLTs, these technologies are still in the early stage of development. The immaturity of blockchain technology in the form of security vulnerabilities, a single point of failure, and the lack of experiential knowledge may lead to some ambiguities in adopting and implementing the technology [53].

3.2. Scalability and Bandwidth Issues

Scalability and bandwidth issues describe network throughput limitations. According to [126], "Scalability is the capability of blockchain calculating processes to apply in a vast range of potentialities and to fulfill these aims". Scalability has been described as becoming a major issue with the increasing number of entities, transactions, block sizes, and long latency, preventing large-scale blockchain implementation [127]. One example to consider is that if Bitcoin proceeded with the same amount of transaction volume as VISA, it would need to replicate data in the entire network, posing a massive challenge to the data capacity and bandwidth [128]. Next, from a technical perspective, scalability is considered to be one of the most critical constraints in BDLTs adoption. The scalability of BDLTs has not yet reached a mark with market demand. Indeed, scalability problems are ascribed to the large amounts of transactional data generated from multiple resources in the supply chain operations, including different geographical locations, types of goods, and various business members. The solution to managing scalability through increasing the size of the block is based on an assumption that the throughput will be higher, but at the same time, it conflicts with the security of the main chain due to generate and propagate slate blocks. Therefore, potential schemes need to be presented to enhance the scalability of blockchain systems, while preventing security concerns.

3.3. Wasted Resources or High Energy Consumption

One of the critical drawbacks impeding the adoption of blockchain technology is computational power and energy consumption [108,129,130] and refers to the energy consumed in handling transactions by all the miners [100]. In some consensus mechanisms, such as proof of work (PoW), all blockchain nodes perform a high computational power to mine the next blocks [108]. However, PoW is considered to consume an enormous level of electricity, because mining each block depends on intensive computations and lots of hashing and encryption by all blockchain miners. In this respect, researchers have proposed alternative mechanisms, such as proof of stake (PoS), to avoid high resource consumption, where the probability of successful mining with PoS depends on the invested stakes by nodes in the system. This consensus process relies on the hashing operation and a higher coin age, which refers to the amount of time to hold onto coins without spending or moving them, which will lead to a decrease in energy waste [131]. Another example is delegated proof of stake (DPoS) that contributes to obtain a higher speed of transactions and low electricity consumption [132]. However, the main criticism of PoS and DPoS is the lack of rigorous security analysis [108]. Practical byzantine fault tolerance (PBFT) algorithms depend on the honesty from different validator nodes of a network that may affect both speed and scalability and is not acceptable for systems with thousands of entities [133]. As a result of this, it is interesting to make more energy-efficient consensus mechanisms to make BDLTs more adoptable.

3.4. Throughput and Low Performance

Low transaction throughput and the limited rate for processing the transactions at the block are other important issues of blockchain adoption.

One example to consider is that in contrast to modern credit card platforms that handle 7000 transactions per second, the throughput of the Bitcoin blockchain is around 7 transactions per second and a decentralized open-source blockchain platform like Ethereum can only handle 20 transactions on average [130]. Moreover, by increasing the volume of the data, the propagation delay in blocks will be a considerable issue and the throughput will become more and more difficult. The time needed to synchronize transactions or obtain a consensus among all clients when involving and running the system is an issue [134]. This is critical for IoT devices and industries in the supply chain and their need for high-performance transaction processing with low computational resources [135]. Recently, new solutions have been proposed to avoid the aforementioned problems, such as consensus mechanisms applied in Hyperledger, Stellar, R3, and Ripple, to improve throughput and performance, reducing the block interval time. However, such limitations need to be considered by proper schemes so as to increase the throughput of blockchain systems.

3.5. Lack of Standardization and Interoperability

Another major challenge is the lack of interoperability with other organizations' databases, which often leads to multiple risks of errors and failures of various blockchain platforms.

The Institute of Electrical and Electronics Engineers (IEEE) defines interoperability as "the ability of two or more systems or components to exchange information and to use the information that has been exchanged" [136]. It is considered a determinant factor affecting the adoption of blockchain-based CSCRM technologies. Therefore, more efforts are needed to enable the interoperability of innovative BDLTs with legacy systems and to make the system compatible with the existing IT systems. Furthermore, it is recommended to follow the standards to make the interoperability of different infrastructures easier; this allows a better assessment of the interface between blockchain and the real world.

3.6. Privacy and Information Disclosure Issues

Privacy concerns refer to the anonymity of counterparts to the extent to which information can be shared with a particular entity [137]. For example, anonymity and privacy concerns are rising in the blockchain due to the disclosure risk of users' identities. The user's transaction information, such as the sender and receiver address, even if pseudonymous, and the value, can be publicly accessed and be visible to all network participants. In this case, all personal user information, such as transaction contents (e.g., amounts, account balance, and spending patterns), can be tracked under unexpected failures or malicious cyberattacks [108]. As a result, privacy data can be conducted and achieved with the legal and regulatory frameworks, along with laws for data privacy.

3.7. Criminal Activity, Malicious Attacks

Criminal activities and malicious attacks were found to be challenges in the technological context. Different types of attacks, such as denial-of-service (DoS), spoofing attacks, security threats, Sybil attacks, and double-spending attacks, can affect the performance of BDLT networks [138–140]. In this case, the best security and privacy policies must be included as an integral part of the design and implementation of industrial BDLT applications by designers and developers [141]. In addition, within the scope of these applications, provisions, including different levels of protection, must be provided [142].

3.8. Dependent on Input Information from External Oracles

The blockchain oracle problem is one of the most significant challenges triggering difficulties for the trustworthiness of information written in smart contracts [45,143]. "Oracles are centralized and trusted third parties that constitute the interface between blockchains and the real world" [144]. A smart contract often relies on information from external oracles that collect data from different sources, such as big data applications, Internet of things, and RFID sensors [24]. Indeed, it is likely that these external oracles will be most attractive to criminals.

Table 1. Challenges in BDLT adoptability in CSCRM.

Challenge No.	Challenge Names	References
3.1	Immature, an early stage of development	[78,122,145–147]
3.2	Scalability and bandwidth issues	[108,127,148–150]
3.3	Wasted resources or high energy consumption	[100,130,151,152]
3.4	Throughput and Low performance	[72,145,146,153]
3.5	Lack of standardization and interoperability	[139,154–158]
3.6	Privacy and information disclosure issues	[108,123,125,159,160]
3.7	Criminal activity, malicious attacks	[129,137,152,154,160,161]
3.8	Dependent on input information from external oracles	[24,45,96,144]
3.9	Poor user experience	[19,130,162,163]
3.10	Suitability of blockchain	[123,125,164,165]

Table 1. *Cont.*

Challenge No.	Challenge Names	References
3.11	Cryptocurrency volatility	[24,118,166,167]
3.12	Smart contract issues	[51,72,168,169]
3.13	Quantum Resilience	[123,160,170]
3.14	Lack of trust	[83,164,171–173]
3.15	Users' credential loss	[118,174]
3.16	Poor clarity regulatory provisions	[108,147,163,175–177]

3.9. Poor User Experience

Another concern in the adoption of BDLTs in the supply chain is in terms of the lack of support to end-users and sufficient platforms and tools. Blockchain platforms run under standards that are different from the defined way for existing systems, which poses some challenges for users [128]. An application programming interface (API) is a set of rules and protocols that allows applications to integrate with each other; this needs to be developed to make BDLTs easier to adopt for users [178]. Therefore, to make blockchain more successful, the users' acceptance should be considered during blockchain implementation. Furthermore, customer awareness and understanding of blockchain technology by providing professional training programs may be the key to moving forward with the productivity in organizations' supply chains, as well as securely control them against cyber risks [179,180].

3.10. Suitability of Blockchain

BDLTs do not cover all facets of the supply chain operations in terms of cybersecurity solutions. On the other hand, blockchain technology may not add any value to all core business use cases or processes. Blockchain or cryptographic-based distributed ledgers are a viable solution for trusted transactions among trustless entities or a permanent historical record [181]. Therefore, before adopting BDLT-enabled solutions, practitioners should assess the suitability of applying blockchain using the use-case requirements [182]. Different blockchain types (i.e., permissioned or permissionless) have been leveraged over the last couple of years, allowing industries to use them for their specific domains.

3.11. Cryptocurrency Volatility

An additional weakness is the volatility in crypto markets, which can be a challenge in terms of blockchain adoption in a short time [24]. For example, security violation and cryptocurrency volatility, such as volatile digital coins and hacking wallets of cryptocurrency exchange, have diverse effects on the reputation of BDLTs platforms [118]. Thus, it will take years for payment merchants based on blockchain platforms to be accepted by a large number of users [166,167].

3.12. Smart Contract Issues

A smart contract is "a piece of code that executes a specific business logic when a certain condition is met" [183]. This means that smart contracts are automatically executed when certain conditions in a contract or an agreement are met. Relying on the programming languages, a smart contract could describe all conditions in the contract and the characteristics of blockchain [168]. The complexity of programming languages and challenges of writing correct smart contracts are among the difficulties that face researchers and developers during blockchain adoption. For example, it has been reported that there was an average financial loss of USD 60 million due to the distributed autonomous organization (DAO) attack, which led to the transfer of money to an adversary account in 2016 [184]. Thus, more research is necessary to tackle the aforementioned issues.

3.13. Quantum Resilience

Cryptographic primitives in blockchain are classified into two basic functions, including hashes and public-key encryption for signing transactions [123]. With the advent of quantum computers, it may already be time to start worrying about the breaking of hashing algorithms. The performance and security in the blockchain are affected by this due to the ease of cracking the cryptographic keys using a brute force algorithm [107]. Significant efforts are currently being made to make the cryptographic keys stronger. For example, on the topic of post-quantum cryptography, research institutions such as NIST are calling for proposals, and expect to launch the early report between 2022 and 2024 [185].

3.14. Lack of Trust

Trust is another critical obstacle to success for future growth in BDLT adoption. Trust refers to the "reliability of information provided by trade partners, or the safety and security of the data managed by a central authority" [82]. Therefore, the challenge of trust is broader than just a lack of trust in the blockchain technology suppliers; there is also the problem of loss or breach of data during the distribution of the technology. Although several studies have been carried out to solve the barrier of trust in supply chain management, the problems that are arising are still difficult problems for the BDLTs used nowadays [152,172,186].

3.15. Users' Credential Loss

BDLTs have the potential to create trust within the network with the confirmation of the validity of the user's credentials and the identity issuer to attest the data inside the credential, without revealing the actual data. However, another major issue that can occur when applying BDLTs is in the case of users' credentials loss, e.g., wallet, keys, and some private/public information due to loss, theft, and expiration [174]. Therefore, a high volume of data, e.g., conditions of products and the expected date of delivery, could be exposed when a cryptographic key is compromised. Alternatively, a criminal party could appear to modify data to gain the benefit, e.g., manipulation of the main liable party to refuse the penalties. Ultimately, this scenario indicates how important it is to securitize these keys across BDLTs [118].

3.16. Poor Clarity Regulatory Provisions

Poor clarity regulatory provisions have been considered determinants among the main barriers affecting the adoption of blockchain [187,188]. This challenge is defined as "the policies and regulations provided by government to regulate and monitor the industries for the usage of new technology" [177]. It was identified as a means to overcome the organizational readiness barrier. Given the necessity for guidance and support from the government during the adoption of blockchain in CSCRM in different ways and capacities, in the form of providing proper infrastructures, capabilities, and the definition of laws and regulations to authenticate digital records, executive departments and agencies could be able to monitor and validate transactions, determine the validity of contracts and agreements between parties, and, lastly, define and develop the standards to track the processes under the blockchain platforms [142].

4. Methodology and Research Design

The aim of this research is to identify key challenges of BDLT adoption and provide a hierarchical framework of challenges identified in the field of cyber supply chain risk management. Firstly, through an extensive literature survey and consensus from a group of experts' opinions, the challenges affecting BDLT adoption are identified; secondly, an integrated "ISM-MICMAC" approach is used to identify the most significant of the sixteen challenges extracted from the literature and discussed with practitioners and academics. The proposed methodology consists of two steps: interpretive structural modeling (ISM) and cross impact matrix multiplication applied to classification (MICMAC), and is described in detail in the Sections 4.2 and 5.5. The methodology proposed in this research is depicted and described in Figure 1.

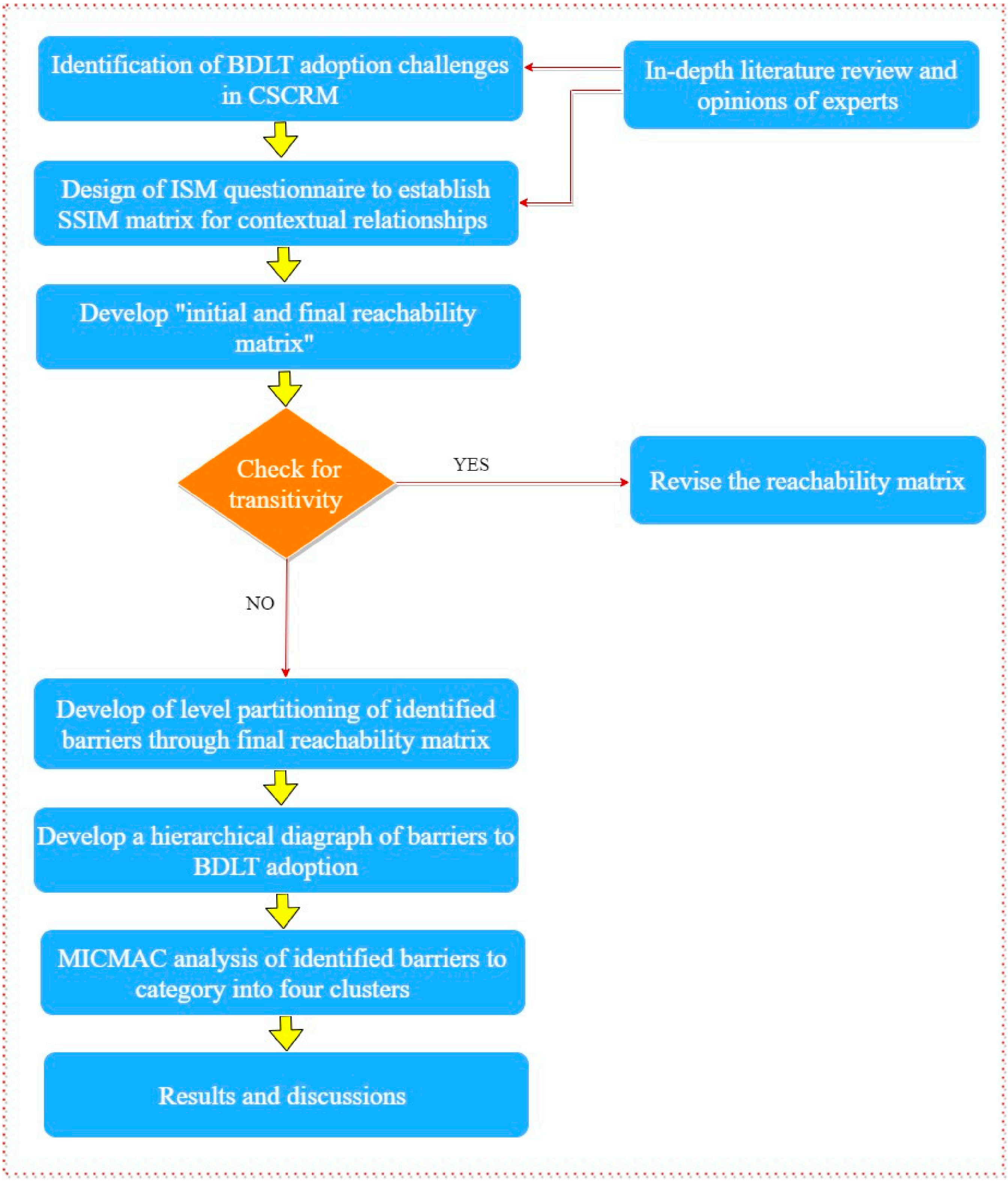
Identification of BDLT adoption challenges in CSCRM
In-depth literature review and opinions of experts
Design of ISM questionnaire to establish SSIM matrix for contextual relationships
Develop "initial and final reachability matrix"
Check for transitivity
YES
Revise the reachability matrix
NO
Develop of level partitioning of identified barriers through final reachability matrix
Develop a hierarchical diagraph of barriers to BDLT adoption
MICMAC analysis of identified barriers to category into four clusters
Results and discussions

Figure 1. Steps for conducting interpretive structural modeling (ISM).

4.1. Data Collection

The ISM methodology is built on the consensus from a group of experts' opinions through different techniques, such as nominal technique, questioner, face-to-face discussion, etc., to establish pairwise contextual relationships among variables [189,190]. With this in mind, a questionnaire was designed to collect each experts' opinions on the contextual and mutual relationships among the BDLT challenges listed in Table 1. The first section of the questionnaire contained general information about the experts' profiles and the professional roles and backgrounds they belong to, and the second section examined the contextual interactions between the identified challenges. The experts were requested to give their written opinions individually to avoid the influence of one opinion on another and were then aggregated and analyzed to develop the final contextual and mutual relationships matrix. The selected group of suitable experts who are conversant in the field of BDLT technologies and CSCRM was found to be small. However, the number of respondents participating in the ISM methodology should not be too many [191,192]. Thus, a total number of five experts (two academics and three industrial operators) from the field of cybersecurity and blockchain technology were involved in answering the questions by identifying what challenges lead to other challenges during the adoption of BDLTs in CSCRM. In the present study, two of the participating experts have a minimum of ten years of academic experience in the university: one has about 15 years of research experience in supply chain management, supply chain risk management, logistics 4.0, Industry 4.0, and management of cyber risks in supply chains, and the other has researched uncertainty analysis, safety and security, sustainability, and innovation for the last 20 years. Both professors are authors of over 90 publications at the international and national levels. They have combined academic qualifications with professional experience in research and consulting projects, and have participated in the implementation of several research projects funded by the government and industry. The other three experts are supply chain executives in different industrial sectors, working in positions, such as supply chain manager, operation manager, and plant quality manager, in manufacturing industries for 10–15 years. They are currently collaborating on several projects concerning the use of blockchain technology for the automation of transactions and processes, leading to a transparent and responsible global supply chain.

4.2. ISM Methodology

ISM is a mathematically derived methodology that was first proposed in 1973 by Professor Walter Felter. It can analyze a complex system into smaller sub-units with the use of experts' practical experience and knowledge and construct a structural multilevel model [193]. As stated by [194], "ISM is an interactive learning process where a set of directly and indirectly associated variables are structured into a comprehensive and systematic model". Based on another definition by [195], "ISM is a popular method of solving complex decision-making problems and for identifying relationships among elements or variables".

In the literature, ISM has been adopted by some researchers as a methodology to support blockchain adoption in various fields. Reference [196] proposed a TISM-based methodology to develop a hierarchical model for the factors facilitating the success of blockchain adoption in the cloud service industry, and to study the mutual interrelationship among critical success factors. Reference [197] used an integrated ISM-DEMATEL approach in an Indian agriculture supply chain (ASC) to model the significant challenges for blockchain implementation. Reference [173] deployed ISM methodology to analyze the technological, organizational, and environmental factors/elements influencing blockchain adoption in the supply chain. Reference [63] applied a combined Fuzzy-ANP and Fuzzy-ISM approach to identify blockchain enablers in a sustainable supply chain.

In this paper, the ISM was applied to envision the contextual relationship among identified challenges for BDLT adoption in a cyber-secure supply chain and cluster them according to their driver and dependence power. The following steps of the ISM process have been adopted in detail, contributing to developing the diagraph and final ISM model.

5. Results

5.1. *Structural Self-Interaction Matrix (SSIM)*

For developing a contextual relationship, the connection between a pair of challenges and the associated path of the relation is questioned to analyze the variables, and the contextual relationship among the identified challenges are hypothesized based on the concept of one challenge leads to another challenge. In this way, the experts were asked to complete pairwise contextual relationships between challenges using four alphabetical codes in a 16 * 16 SSIM. Keeping this in mind, the following symbols (V, A, X, O) have been used to denote the direction of relationships between challenges (*i* and *j*):

V: Challenges *i* enable/impact on challenges *j*.

A: Challenges *j* enable/impact on challenges *i*.

X: Challenges *i* and *j* are mutually interdependent (i.e., either will enable or influence the other).

O: No relationship between challenges *i* and *j*.

A final "Structural Self-Interaction Matrix (SSIM)" (Table 2) is developed by aggregating five SSIM gathered from the experts.

Table 2. Structural Self-Interaction Matrix (SSIM) of relationships among BDLT adoption challenges in CSCRM.

Sr. No.	Barriers	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
1	Immature, early stage of development	A	V	V	V	V	0	V	0	0	V	V	V	V	V	V	
2	Scalability and bandwidth issues	A	0	V	0	0	0	0	0	A	V	V	0	V	V		
3	Wasted resources or high energy consumption	0	0	V	0	0	0	0	0	A	0	0	0	V			
4	Throughput and Low performance	A	A	V	0	A	0	A	0	A	A	A	A				
5	Lack of standardization and interoperability	A	0	A	0	A	0	0	0	0	V	V					
6	Privacy and information disclosure issues	A	A	V	A	A	V	V	A	A	V						
7	Criminal activity, malicious attacks	A	A	V	A	A	V	V	A	A							
8	Dependent on input information from external oracles	A	0	V	0	V	V	0	0								
9	Poor user experience	A	A	A	0	A	0	0									
10	Suitability of blockchain	A	0	V	A	A	0										
11	Cryptocurrency volatility	A	A	A	A	A											
12	Smart contract issues	A	A	V	0												
13	Quantum Resilience	A	0	V													
14	Lack of trust in new technology	A	A														
15	Users' credential loss	A															
16	Poor clarity regulatory provisions																

5.2. *Reachability Matrix*

An "Initial reachability matrix (IRM)" is developed by converting the symbols "V, A, X, O" into binary elements (i.e., 1, 0) to get IRM. To construct an initial reachability matrix, shown in Table 3, some rules are adopted as follows:

i. If the symbol of V is shown in the cell of (i, j) in the SSIM matrix, then in the IRM, the value of cell (i, j) will become 1, and the corresponding cell (j, i) is replaced with the value '0'.

ii. If the symbol of A is shown in the cell of (i, j) in the SSIM matrix, then in the IRM, the value of cell (i, j) will become 0, and the corresponding cell (j, i) is replaced with the value '1'.

iii. If the symbol of X is shown in the cell of (i, j) in the SSIM matrix, then in the IRM, the value of cell (i, j) will become 1, and the corresponding cell (j, i) is replaced with the value '1'.

iv. If the symbol of O is shown in the cell of (i, j) in the SSIM matrix, then in the IRM, the value of cell (i, j) will become 0, and the corresponding cell (j, i) is replaced with the value '0'.

Subsequently, the "Final reachability matrix (FRM)" is achieved by incorporating transitivity rules in the IRM. The transitivity rules suggest that if factor X affects factor Y and factor Y affects factor Z, then factor X automatically affects factor Z. The FRM is shown in Table 4. The transitive links are highlighted using a yellow shade.

Table 3. Initial reachability matrix of relationships among BDLT adoption challenges in CSCRM.

Sr. No.	Barriers	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	Immature, early stage of development	1	1	1	1	1	1	1	0	0	1	0	1	1	1	1	0
2	Scalability and bandwidth issues	0	1	1	1	0	1	1	0	0	0	0	0	0	1	0	0
3	Wasted resources or high energy consumption	0	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0
4	Throughput and low performance	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0
5	Lack of standardization and interoperability	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0
6	Privacy and information disclosure issues	0	0	0	1	0	1	1	0	0	1	1	0	0	1	0	0
7	Criminal activity, malicious attacks	0	0	0	1	0	0	1	0	0	1	1	0	0	1	0	0
8	Dependent on input information from external oracles	0	1	1	1	0	1	1	1	0	0	1	1	0	1	0	0
9	Poor user experience	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0
10	Suitability of blockchain	0	0	0	1	0	0	0	0	0	1	0	0	0	1	0	0
11	Cryptocurrency volatility	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
12	Smart contract issues	0	0	0	1	1	1	1	0	1	1	1	1	0	1	1	0
13	Quantum resilience	0	0	0	0	1	1	1	0	0	1	1	0	1	1	0	0
14	Lack of trust in new technology	0	0	0	0	0	0	0	0	1	0	1	0	0	1	0	0
15	Users' credential loss	0	0	0	1	1	1	1	0	1	1	0	0	0	1	1	0
16	Poor clarity regulatory provisions	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1

Table 4. Final reachability matrix of relationships among BDLT adoption challenges in CSCRM with transitive links.

Sr. No.	Barriers	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Driving Power
1	Immature, an early stage of development	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	0	14
2	Scalability and bandwidth issues	0	1	1	1	1	1	1	0	1	1	1	0	0	1	0	0	10
3	Wasted resources or high energy consumption	0	0	1	1	1	1	1	0	1	1	1	0	0	1	0	0	9
4	Throughput and low performance	0	0	0	1	1	1	1	0	1	1	1	0	0	1	0	0	8
5	Lack of standardization and interoperability	0	0	0	1	1	1	1	0	1	1	1	0	0	1	0	0	8
6	Privacy and information disclosure issues	0	0	0	1	1	1	1	0	1	1	1	0	0	1	0	0	8
7	Criminal activity, malicious attacks	0	0	0	1	1	1	1	0	1	1	1	0	0	1	0	0	8
8	Dependent on input information from external oracles	0	1	1	1	1	1	1	1	1	1	1	1	0	1	1	0	13
9	Poor user experience	0	0	0	1	1	1	1	0	1	1	1	0	0	1	0	0	8
10	Suitability of blockchain	0	0	0	1	1	1	1	0	1	1	1	0	0	1	0	0	8
11	Cryptocurrency volatility	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1
12	Smart contract issues	0	0	0	1	1	1	1	0	1	1	1	1	0	1	1	0	10
13	Quantum resilience	0	0	0	1	1	1	1	0	1	1	1	0	1	1	0	0	9
14	Lack of trust in new technology suppliers	0	0	0	1	1	1	1	0	1	1	1	0	0	1	0	0	8
15	Users' credential loss	0	0	0	1	1	1	1	0	1	1	1	0	0	1	1	0	9
16	Poor clarity regulatory provisions	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	16
	Dependence Power	2	4	5	15	15	15	15	2	15	15	16	4	3	15	5	1	

5.3. Level Partitions

The final reachability matrix obtained is then divided into different levels of partition to construct the hierarchy graph. Three sets for each challenge are processed, namely "reachability set, antecedent set, and intersection set". The reachability set of each challenge comprises itself as well as the other challenges that it may drive and can be found as the set of elements that contain 1 in that particular row. Similarly, the antecedent set includes the challenge itself and the other challenge that may support in achieving it, and is the set of elements that contain 1 in that particular column. The challenges that are considered at level 1 or the top level in the ISM model are removed from the table for the next iteration set when both the reachability set and the intersection set are similar. This process of assigning the level of each challenge continues up to the defining of the last challenge. Table 5 shows the details of level partitions for sixteen challenges with six levels.

Table 5. Intersection of reachability and antecedent sets and presentation of the levels.

Iteration No.	Reachability Set	Antecedent Set	Intersection Set	Level
Iteration 1	1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15	1, 16	1	
	2, 3, 4, 5, 6, 7, 9, 10, 11, 14	1, 2, 8, 16	2	
	3, 4, 5, 6, 7, 9, 10, 11, 14	1, 2, 3, 8, 16	3	
	4, 5, 6, 7, 9, 10, 11, 14	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16	4, 5, 6, 7, 9, 10, 14	
	4, 5, 6, 7, 9, 10, 11, 14	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16	4, 5, 6, 7, 9, 10, 14	
	4, 5, 6, 7, 9, 10, 11, 14	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16	4, 5, 6, 7, 9, 10, 14	
	4, 5, 6, 7, 9, 10, 11, 14	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16	4, 5, 6, 7, 9, 10, 14	
	2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15	8, 16	8	
	4, 5, 6, 7, 9, 10, 11, 14	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16	4, 5, 6, 7, 9, 10, 14	
	4, 5, 6, 7, 9, 10, 11, 14	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16	4, 5, 6, 7, 9, 10, 14	
	11	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	11	I
	4, 5, 6, 7, 9, 10, 11, 12, 14, 15	1, 8, 12, 16	12	
	4, 5, 6, 7, 9, 10, 11, 13, 14	1, 13, 16	13	
	4, 5, 6, 7, 9, 10, 11, 14	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16	4, 5, 6, 7, 9, 10, 14	
	4, 5, 6, 7, 9, 10, 11, 14, 15	1, 8, 12, 15, 16	15	
	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	16	16	
Iteration 2	1, 2, 3, 4, 5, 6, 7, 9, 10, 12, 13, 14, 15	1, 16	1	
	2, 3, 4, 5, 6, 7, 9, 10, 14	1, 2, 8, 16	2	
	3, 4, 5, 6, 7, 9, 10, 14	1, 2, 3, 8, 16	3	
	4, 5, 6, 7, 9, 10, 14	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16	4, 5, 6, 7, 9, 10, 14	II
	4, 5, 6, 7, 9, 10, 14	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16	4, 5, 6, 7, 9, 10, 14	II
	4, 5, 6, 7, 9, 10, 14	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16	4, 5, 6, 7, 9, 10, 14	II
	4, 5, 6, 7, 9, 10, 14	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16	4, 5, 6, 7, 9, 10, 14	II
	2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15	8, 16	8	
	4, 5, 6, 7, 9, 10, 14	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16	4, 5, 6, 7, 9, 10, 14	II
	4, 5, 6, 7, 9, 10, 14	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16	4, 5, 6, 7, 9, 10, 14	II
	4, 5, 6, 7, 9, 10, 12, 14, 15	1, 8, 12, 16	12	
	4, 5, 6, 7, 9, 10, 13, 14	1, 13, 16	13	
	4, 5, 6, 7, 9, 10, 14	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16	4, 5, 6, 7, 9, 10, 14	II
	4, 5, 6, 7, 9, 10, 14, 15	1, 8, 12, 15, 16	15	
	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16	16	16	
Iteration 3	1, 2, 3, 12, 13, 15	1, 16	1	
	2, 3	1, 2, 8, 16	2	
	3	1, 2, 3, 8, 16	3	III
	2, 3, 8, 12, 15	8, 16	8	
	12, 15	1, 8, 12, 16	12	
	13	1, 13, 16	13	III
	15	1, 8, 12, 15, 16	15	III
	1, 2, 3, 8, 12, 13, 15, 16	16	16	
Iteration 4	1, 2, 12	1, 16	1	
Iteration 5	2	1, 2, 8, 16	2	IV
	2, 8, 12	8, 16	8	
	12	1, 8, 12, 16	12	IV
	1, 2, 8, 12, 16	16	16	
	1	1, 16	1	V
	8	8, 16	8	V
	1, 8, 16	16	16	
Iteration 6	16	16	16	VI

5.4. Building an ISM Model

The hierarchical framework is obtained as an ISM model using the inputs from the final reachability matrix as per the partition level. The relationship between the variables i and j is indicated by an arrow from i to j or vice versa. A final ISM model is also developed after removing the indirect links. This ISM model was checked with the experts for any conceptual inconsistency. Figure 2 shows the final diagraph without any conceptual inconsistency for blockchain adoption in a cyber secure supply chain. The level I challenges are at the top of the model, level II challenges appear in the second position and so on, and finally, level VI challenges come at the base of the ISM hierarchy.

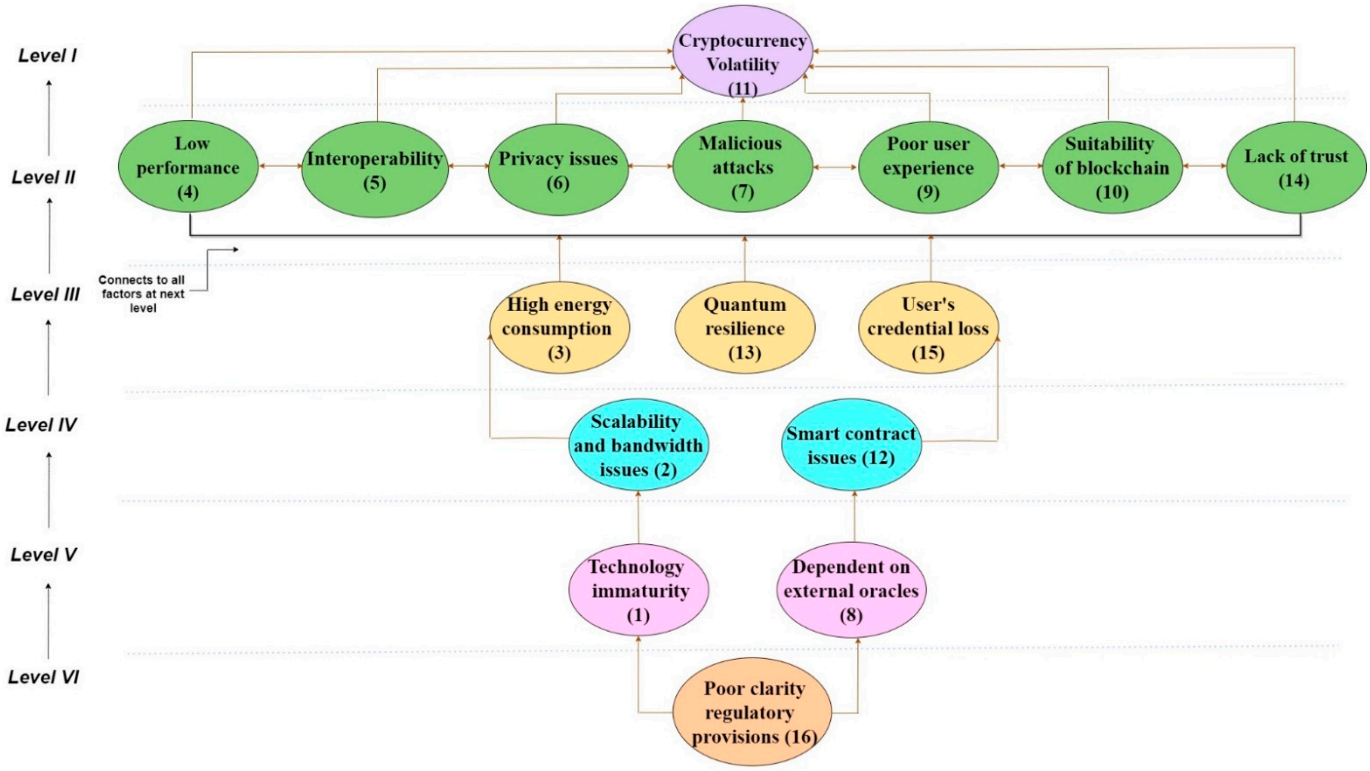
Level I
Level II
Level III
Level IV
Level V
Level VI
Connects to all factors at next level
Cryptocurrency Volatility (11)
Low performance (4)
Interoperability (5)
Privacy issues (6)
Malicious attacks (7)
Poor user experience (9)
Suitability of blockchain (10)
Lack of trust (14)
High energy consumption (3)
Quantum resilience (13)
User's credential loss (15)
Scalability and bandwidth issues (2)
Smart contract issues (12)
Technology immaturity (1)
Dependent on external oracles (8)
Poor clarity regulatory provisions (16)

Figure 2. Hierarchical diagram of BDLT adoption challenges relationships in CSCRM.

5.5. MICMAC Analysis

A MICMAC ("Matrice d'Impacts Croisé Multiplication Appliquée à un Classement") analysis was developed by [198]. It provides better comprehension of the relationships among the challenges of blockchain adoption in a cyber-secure supply chain. The MICMAC analysis is conducted to analyze the driving and dependence power of the variables and classification into four different categories (Figure 3).

From Figure 3, it could be observed that the dependance variables are graphed on the x-axis, while driving variables are generally plotted on the y-axis. The first category presents the variables with weak dependence and driving powers and has been clustered as "autonomous or excluded variables", which signifies that all types of these variables are incoherent with the system because they do not have any effect on the adoption of blockchain technology in CSCRM. No variable is identified in this category, which means that all the variables have high influence levels with each other. The second category consists of measures with strong dependence powers and weak driving powers, known as the "dependent variables". The dependent variables appear on the top levels of the ISM hierarchy model. In the present study, "cryptocurrency volatility" is a dependent variable. Then, the third category is known as "linkage or rely variables" and have high dependence as well as driving powers; any action on them will affect on other variables in the higher level.

In our case, challenges of "throughput and low performance", "lack of standardization and interoperability", "privacy and information disclosure issues", "criminal activity and malicious attacks", "poor user experience", "suitability of blockchain", "lack of trust in new technology suppliers", "quantum resilience", "wasted resources or high energy consumption" and "users' credential loss" fall into the third cluster of linkage and any action on these challenges will affect others. The remaining challenges of "technology immaturity", "poor clarity regulatory provisions", "dependent on input information from external oracles", "scalability and bandwidth issues", and "smart contract issues" are those that fall under the fourth cluster and are named "Driving factors". Related to weak dependence and strong driving powers, these challenges are the most significant factors that the CSCRM sees as an impediment at the point of adoption of BDLT technologies.

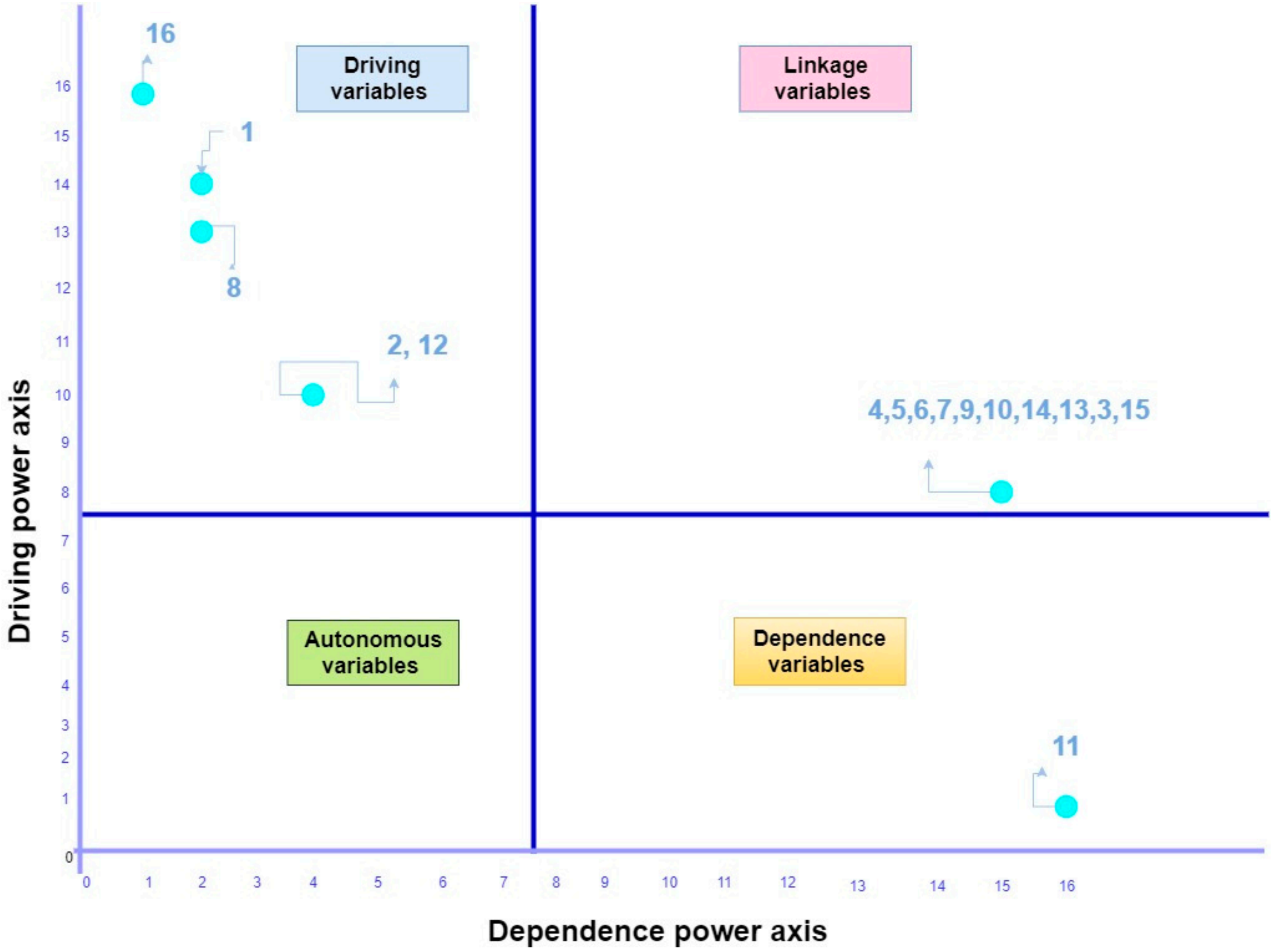

Figure 3. MICMAC matrix for influential challenges of BDLT adoption in a CSCRM context.

6. Discussion on Theoretical and Managerial Implications

6.1. Implications for Theory

The primary objective of this paper is to identify and rank the challenges affecting BDLT adoption in CSCRM and to unravel the causal relationships between them. From a theoretical point of view, the contribution of this paper is four-fold. First, this research adopted a comprehensive literature review and the opinion of experts with knowledge of blockchain to extract challenges of blockchain adoption in the CSCRM context. Second, this is one of the first studies of its type focusing on the challenges of BDLT adoption in CSCRM, modeling them using an ISM methodology in the structure of a hierarchical framework to envision the contextual relationships among the identified challenges. Third, using the MICMAC diagram, the influential challenges were clustered according to their driving and dependence powers. This research is expected to contribute to enabling researchers to propose and test theoretical models and different hypotheses based on the critical determinants of blockchain adoption in different supply chain contexts. Finally, the developed framework with the priority of the sixteen influencing challenges helps researchers and practitioners to get insights into a long-term capacity towards BDLTs adoption to achieve cybersecurity at a supply chain level.

6.2. Implications for Practice

The emergence of the imbalance towards the practical side of CSCRM in the real-world leads to a significant incentive for organizations to look at BDLTs from a cyber secure supply chain perspective, given the negative effects of cyber events that affect supply chain operations. For example, concerns include a lack of confidentiality during information sharing while maintaining data visibility and transparency between supply chain partners. Therefore, managers and employees are those who need to reach outside their "silo" activities and adopt a holistic view of cyber risks, as well as innovative solutions to deal with these risks. The most vital link problem from a cyber perspective in the supply chain could be identified via technologies, such as blockchain for leveraging the CSCRM process. However, the adoption of BDLTs comes with several challenges, including a lack of technology maturity, users' credential loss (e.g., wallet), and in some scenarios, being subject to cryptocurrency volatility; so, attention to them constitutes the main objective of this paper.

In this vein, the current study offers meaningful contributions for practitioners, consulting companies, and leading enterprises to be aware of the criticality and interplay of different influencing challenges and inter-relationships among them while implementing BDLTs in the CSCRM.

In this study, MICMAC analysis has been adopted to help the analysis of the driving and dependence powers of the challenges and their classification into four different clusters. The identified challenges in the "Drivers" cluster should be considered to guarantee the long-term success of BDLT-based cybersecurity in the industries since this is the early stage of development for BDLT technologies. These challenges are a pre-requisite to obtaining other challenges, which are the topmost reasons for an organization to make a decision for BDLT adoption and are reflected under the "dependent cluster" (cryptocurrency volatility). In this context, it is worth noting that the challenges in the "dependent cluster" are important because they need all the other challenges to reduce the impact of these challenges during the adoption of blockchain. However, a lot of focus on these challenges with high dependence and less driving power without considering a strong set of "driver" challenges will not be useful to manage the adoption of blockchain in CSCRM.

Therefore, for the sustained success of BDLT in CSCRM activities, decision-makers should also be aware of "driver" challenges (such as technology immaturity, poor clarity regulatory provisions, dependent on input information from external oracles, scalability and bandwidth issues, and smart contract issues). This enables them to have more incentives for transiting into the digital operation phase.

7. Conclusions, Discussion of Findings, and Scope for Future Research

The adoption of BDLTs in the cyber secure supply chain is in its nascent stage, and there are numerous challenges that must be overcome before these innovative technologies proceed to the next phase. BDLTs have enormous potential to enhance the cybersecurity of a supply chain if the issues to its adoption are reinforced with favorable regulations and methods. To achieve this objective, this research conducted an analytical hierarchy "ISM-based model" approach to analyze the interactions among the identified BDLT challenges and to partition the challenges into levels based on their driving and dependency powers. In line with the previous literature, sixteen key BDLT challenges of CSCRM were identified and validated with a group of experts in academics and in the industries. Furthermore, our findings classified each challenge into one of four different kinds of power.

The findings from the study suggest that the challenges "technology immaturity", "poor clarity regulatory provisions", "dependent on input information from external oracles", "scalability and bandwidth issues", and "smart contract issues" with high driving and low dependence powers are the major challenges for adoption of blockchain in CSCRM and are placed at the bottom of the ISM model. The challenges "throughput and low performance", "lack of standardization and interoperability", "privacy and information disclosure issues", "criminal activity and malicious attacks", "poor user experience", "suitability of blockchain", "lack of trust in new technology suppliers", "quantum resilience", "wasted resources or high energy consumption" and "users' credential loss" imply both strong powers; they play a key function in the tendency to adopt blockchain in CSCRM, and they need more attention. The challenge "cryptocurrency volatility" with high dependence and low driving power is located at the top of the ISM framework. No factor is identified as an autonomous factor, indicating that all the selected challenges should be paid attention to by policymakers. Given that BDLT adoption for cyber supply chain risk management is in its infancy, there are still a number of challenges behind the 16 barriers identified in this paper, which must be explored for their structural relationships that can be used to develop plans to overcome obstacles in the implementation of a BDLT-based cyber secure supply chain. Therefore, similar type of research can also be recommended in the future to eradicate any important obstacle that might have been affected in BDLTs' adoption in CSCRM. Despite the significance of the study, the current study was not without its limitations, one of which are the interdependencies among the selected challenges, which were developed based on judgments from academics and practitioners, which can be included the chosen experts' personal biases. To refuse the aforementioned problems in the outcomes of the study, further empirical studies could be conducted to quantity the effects of the explored challenges on blockchain adoption in the CSCRM and also examine the intensity of the causal relationship between them. Additionally, the use of empirical researches is recommended, such as confirmatory factor analysis (CFA) and structural equation modeling (SEM), to test and validate this proposed ISM-based model.

Author Contributions: N.E., P.V.G. and F.S. convinced, developed, analyzed the research model; contributed to the discussion and design of the framework, and wrote the manuscript. 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.

Data Availability Statement: Not applicable.

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

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

References

1. Chen, T.M.; Abu-Nimeh, S. Lessons from Stuxnet. *Computer* **2011**, *44*, 91–93. [CrossRef]
2. Burton, M.; Cho Walsgard, J. Cyber Attack Puts a Spotlight on Fragile Global Supply Chain—Bloomberg. Available online: https://www.bloomberg.com/news/articles/2019-03-19/cyber-attackputs-a-spotlight-on-fragile-global-supply-chains (accessed on 2 February 2021).
3. Boyes, H. Cybersecurity and Cyber-Resilient Supply Chains. *Technol. Innov. Manag. Rev.* **2015**, *5*, 28–34. [CrossRef]
4. ResilienceFrom Ports to Distribution: Insights into Supply Chain Cyber Threats. Available online: https://www.resilience360.dhl.com/resilienceinsights/fro-mports-to-production-insights-into-supply-chain-cyberthreats/?utm_source=GoogleAdwords&utm_medium=PaidSearch&utm_Capaign=cyber-crime-2018&utm_term=CyberSecurity&utm_content=Thought-Leadership&g (accessed on 26 February 2020).
5. NIST. Best Practices in Cyber Supply Chain Risk Management. Available online: https://www.nist.gov/system/files/documents/itl/csd/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf (accessed on 15 February 2021).
6. Hinde, S. Life Was Simple Then. *Comput. Secur.* **2000**, *19*, 222–229. [CrossRef]
7. Williams, P. Why Latin Port, Shipping and Supply Chain Security is Getting more Complex—And What it Means for Training. Available online: https://www.linkedin.com/pulse/why-latin-port-shipping-supply-chain-security-getting-rachael-white/?trackingId=Rzjy0I5pF8Dy7YG3Vsm5Rg%3D%3D (accessed on 25 January 2021).

8. Radanliev, P.; De Roure, D.C.; Nicolescu, R.; Huth, M.; Montalvo, R.M.; Cannady, S.; Burnap, P. Future developments in cyber risk assessment for the internet of things. *Comput. Ind.* **2018**, *102*, 14–22. [CrossRef]
9. Sengupta, J.; Ruj, S.; Das Bit, S. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [CrossRef]
10. Aceto, B. Blockchain e Dintorini. 2019. Retrieved 7 March 2021. Available online: http://tendenzeonline.info/articoli/2019/05/08/blockchain-edintorini (accessed on 18 August 2020).
11. Kshetri, N. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommun. Policy* **2017**, *41*, 1027–1038. [CrossRef]
12. Wensley, J.H.; Lamport, L.; Goldberg, J.; Green, M.W.; Levitt, K.N.; Milliar-Smith, P.M.; Shostak, R.E.; Weinstock, C.B. SIFT: Design and analysis of a fault-tolerant computer for aircraft control. *Proc. IEEE* **1978**, *66*, 1240–1255. [CrossRef]
13. Rauchs, M.; Glidden, A.; Gordon, B.; Pieters, G.C.; Recanatini, M.; Rostand, F.; Vagneur, K.; Zhang, B.Z. Distributed Ledger Technology Systems: A Conceptual Framework. *SSRN Electron. J.* **2018**. [CrossRef]
14. Saur, K.; Bowman, M.; Miele, A.; Held, J.P. Technology for Secure Partitioning and Updating of a Distributed Digital Ledger. U.S. Patent US20180145836A1, 18 November 2016.
15. Ølnes, S.; Ubacht, J.; Janssen, M. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Gov. Inf. Q.* **2017**, *34*, 355–364. [CrossRef]
16. Siyal, A.A.; Junejo, A.Z.; Zawish, M.; Ahmed, K.; Khalil, A.; Soursou, G. Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives. *Cryptography* **2019**, *3*, 3. [CrossRef]
17. Chod, J.; Trichakis, N.; Tsoukalas, G.; Aspegren, H.; Weber, M. On the Financing Benefits of Supply Chain Transparency and Blockchain Adoption. *Manag. Sci.* **2020**, *66*. [CrossRef]
18. 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]
19. Chen, S.; Liu, X.; Yan, J.; Hu, G.; Shi, Y. Processes, benefits, and challenges for adoption of blockchain technologies in food supply chains: A thematic analysis. *Inf. Syst. e-Bus. Manag.* **2020**, 1–27. [CrossRef]
20. Treiblmaier, H.; Rejeb, A.; Strebinger, A. Blockchain as a Driver for Smart City Development: Application Fields and a Comprehensive Research Agenda. *Smart Cities* **2020**, *3*, 853–872. [CrossRef]
21. Mathew, A.R. Cyber Security through Blockchain Technology. *Int. J. Eng. Adv. Technol.* **2019**, *9*, 3821–3824. [CrossRef]
22. Srivastava, S.S.; Dwivedi, R.; Gunda, A.; Meena, D.K.; Negi, R.; Vasita, N.; Singh, A. Blockchain and Its Application in Cybersecurity. In *Cyber Security in India*; IITK Directions; Shukla, S., Agrawal, M., Eds.; Springer: Singapore, 2020; Volume 4. [CrossRef]
23. Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.-K.R. A systematic literature review of blockchain cyber security. *Digit. Commun. Netw.* **2020**, *6*, 147–156. [CrossRef]
24. Fraga-Lamas, P.; Fernandez-Carames, T.M. A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry. *IEEE Access* **2019**, *7*, 17578–17598. [CrossRef]
25. Azzi, R.; Chamoun, R.K.; Sokhn, M. The power of a blockchain-based supply chain. *Comput. Ind. Eng.* **2019**, *135*, 582–592. [CrossRef]
26. 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. In *Handbook of Ripple Effects in the Supply Chain*; International Series in Operations Research & Management Science; Ivanov, D., Dolgui, A., Sokolov, B., Eds.; Springer: Cham, Switzerland, 2019; Volume 276. [CrossRef]
27. Zhang, H.; Nakamura, T.; Sakurai, K. Security and Trust Issues on Digital Supply Chain. In Proceedings of the 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Fukuoka, Japan, 5–8 August 2019; Institute of Electrical and Electronics Engineers (IEEE), 2019.
28. Hajric, V. Blockchain is Dead? Crypto Geeks Debate Merits of Once Dear Tech-Bloomberg. 2019. Available online: https://www.bloomberg.com/news/articles/2019-11-12/blockchain-is-deadcrypto-geeks-debate-merits-of-once-dear-tech (accessed on 28 February 2021).
29. Hofmann, E.; Rüsch, M. Industry 4.0 and the current status as well as future prospects on logistics. *Comput. Ind.* **2017**, *89*, 23–34. [CrossRef]
30. Dias, G.C.; Hernandez, C.T.; De Oliveira, U.R. Supply chain risk management and risk ranking in the automotive industry. *Gestão Produção* **2020**, *27*. [CrossRef]
31. Juttner, U.; Peck, H.; Christopher, M. Supply chain risk management: Outlin ing an agenda for future re-search. *Int. J. Logist. Res. Appl.* **2003**, *6*, 197–210. [CrossRef]
32. 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]
33. Ivanov, D. Revealing interfaces of supply chain resilience and sustainability: A simulation study. *Int. J. Prod. Res.* **2018**, *56*, 3507–3523. [CrossRef]
34. Ghadge, A.; Weiß, M.; Caldwell, N.D.; Wilding, R. Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Manag. Int. J.* **2019**, *25*, 223–240. [CrossRef]

35. Chand, M.; Raj, T.; Shankar, R. Analysing the operational risks in supply chain by using weighted interpretive structure modelling technique. *Int. J. Serv. Oper. Manag.* **2014**, *18*, 378. [CrossRef]
36. Venkatesan, S.P.; Kumanan, S. Supply chain risk prioritisation using a hybrid AHP and PROMETHEE approach. *Int. J. Serv. Oper. Manag.* **2012**, *13*, 19. [CrossRef]
37. Ho, W.; Zheng, T.; Yildiz, H.; Talluri, S. Supply chain risk management: A literature review. *Int. J. Prod. Res.* **2015**, *53*, 5031–5069. [CrossRef]
38. Moustafa, N.; Adi, E.; Turnbull, B.; Hu, J. A New Threat Intelligence Scheme for Safeguarding Industry 4.0 Systems. *IEEE Access* **2018**, *6*, 32910–32924. [CrossRef]
39. Boyson, S. Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation* **2014**, *34*, 342–353. [CrossRef]
40. Sindhuja, P.N.; Kunnathur, A.S. Information security in supply chains: A management control perspective. *Inf. Comput. Secur.* **2015**, *23*, 476–496. [CrossRef]
41. Bartol, N. Cyber supply chain security practices DNA—Filling in the puzzle using a diverse set of disciplines. *Technovation* **2014**, *34*, 354–361. [CrossRef]
42. Windelberg, M. Objectives for managing cyber supply chain risk. *Int. J. Crit. Infrastruct. Prot.* **2016**, *12*, 4–11. [CrossRef]
43. Bode, C.; Wagner, S.M. Structural drivers of upstream supply chain complexity and the frequency of supply chain disruptions. *J. Oper. Manag.* **2015**, *36*, 215–228. [CrossRef]
44. Boyens, J.M.; Paulsen, C.; Bartol, N.; Winkler, K.; Gimbi, J. *Case Studies in Cyber Supply Chain Risk Management: Summary of Findings and Recommendations*; Technology Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020.
45. Davis, A. Building Cyber-Resilience into Supply Chains. *Technol. Innov. Manag. Rev.* **2015**, *5*, 19–27. [CrossRef]
46. Farahani, B.; Firouzi, F.; Luecking, M. The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. *J. Netw. Comput. Appl.* **2021**, *177*, 102936. [CrossRef]
47. Nakamoto, S. Bitcoin: A Peer-to-peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 11 February 2012).
48. Buterin, V. Bitcoin Network Shaken by Blockchain Fork. Bitcoinmagazine. 2013. Available online: https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork1363144448/ (accessed on 15 January 2020).
49. Buterin, V. DAOs, DACs, DAs and More: An Incomplete Terminology Guide. Ethereum Blog. 2014. Available online: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminologyguide/ (accessed on 2 March 2021).
50. Ackermann, J.; Meier, M. Blockchain 3.0—The next generation of blockchain systems. In Proceedings of the Advanced Seminar Blockchain Technologies, Munich, Germany, September 2018; pp. 1–7.
51. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Futur. Gener. Comput. Syst.* **2020**, *107*, 841–853. [CrossRef]
52. Pajooh, H.H.; Rashid, M.; Alam, F.; Demidenko, S. Hyperledger Fabric Blockchain for Securing the Edge Internet of Things. *Sensors* **2021**, *21*, 359. [CrossRef]
53. Swan, M. Climate Change 2013—The Physical Science Basis. In *Blockchain: Blueprint for a New Economy*; O'Reilly Media, Inc.: Newton, MA, USA, 2015.
54. Kamble, S.; Gunasekaran, A.; Arha, H. Understanding the Blockchain technology adoption in supply chains-Indian context. *Int. J. Prod. Res.* **2019**, *57*, 2009–2033. [CrossRef]
55. Liu, X.; Farahani, B.; Firouzi, F. Distributed Ledger Technology. In *Intelligent Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 393–431.
56. Van Engelenburg, S.; Janssen, M.; Klievink, B. Design of a software architecture supporting business-to-government information sharing to improve public safety and security. *J. Intell. Inf. Syst.* **2017**, *52*, 595–618. [CrossRef]
57. Merkle, R.C. A digital signature based on a conventional encryption function. In *Advances in Cryptology—CRYPT0 87, Lecture Notes in Computer Science*; Pomerance, C., Ed.; Springer: Berlin/Heidelberg, Germany, 1987; Volume 369. [CrossRef]
58. Luu, L.; Narayanan, V.; Baweja, K.; Zheng, C.; Gilbert, S.; Saxena, P. SCP: A Computationally-Scalable Byzantine Consensus Protocol for Blockchains. *IACR Cryptol. ePrint Arch.* **2015**, *20*, 1168.
59. Dinh, T.T.A.; Wang, J.; Chen, G.; Liu, R.; Ooi, B.C.; Tan, K.-L. BLOCKBENCH. In Proceedings of the 2017 ACM International Conference on Interactive Experiences for TV and Online Video, Hilversum, The Netherlands, 14–16 June 2017; ACM: New York, NY, USA, 2017.
60. Anderberg, A.; Andonova, E.; Bellia, M.; Calès, L.; Inamorato Dos Santos, A.; Kounelis, I.; Nai Fovino, I.; Petracco Giudici, M.; Papanagiotou, E.; Sobolewski, M.; et al. *Blockchain Now And Tomorrow*; EUR 29813 EN; Publications Office of the European Union: Luxembourg, 2019; ISBN 978-92-76-08977-3.
61. Tapscott, A.; Tapscott, D. How Blockchain is changing finance. Harvard Business Review. 1 March 2017. Available online: https://hbr.org/2017/03/howBlockchain-is-changing-finance (accessed on 5 April 2020).
62. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352. [CrossRef]
63. Yadav, S.; Singh, S.P. An integrated fuzzy-ANP and fuzzy-ISM approach using blockchain for sustainable supply chain. *J. Enterp. Inf. Manag.* **2020**, *34*, 54–78. [CrossRef]
64. Kissel, R. Glossary of Key Information Security Terms, NIST Interagency/Internal Report (NISTIR)–7298rev2. 5 June 2013.

65. Etemadi, N.; Borbon-Galvez, Y.; Strozzi, F.; Etemadi, T. Supply Chain Disruption Risk Management with Blockchain: A Dynamic Literature Review. *Information* **2021**, *12*, 70. [CrossRef]
66. Piscini, E.D.D. Blockchain & cyber security. Let's Discuss. Available online: https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf (accessed on 3 March 2021).
67. Pilkington, M. Blockchain technology: Principles and applications. In *Re-search Handbook on Digital Transformations*; Edward Elgar Publishing: Cheltenham, UK, 2016.
68. IBM. Blockchain. 2017. Available online: https://www.ibm.com/blockchain/what-is-blockchain.html (accessed on 9 February 2021).
69. Zeng, Z.; Li, Y.; Cao, Y.; Zhao, Y.; Zhong, J.; Sidorov, D.; Zeng, X. Blockchain Technology for Information Security of the Energy Internet: Fundamentals, Features, Strategy and Application. *Energies* **2020**, *13*, 881. [CrossRef]
70. 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.
71. Galvez, J.F.; Mejuto, J.; Simal-Gandara, J. Future challenges on the use of blockchain for food traceability analysis. *TrAC Trends Anal. Chem.* **2018**, *107*, 222–232. [CrossRef]
72. Abeyratne, S.A.; Monfared, R.P. Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger. *Int. J. Res. Eng. Technol.* **2016**, *5*, 1–10.
73. 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 Engi-neering, Bergamo, Italy, 9–11 September 2020.
74. Kshetri, N. Will blockchain emerge as a tool to break the poverty chain in the Global South? *Third World Q.* **2016**, *38*, 1710–1732. [CrossRef]
75. 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**, *260*, 121031. [CrossRef]
76. Ge, L.; Brewster, C.; Spek, J.; Smeenk, A.; Top, J.; Van Diepen, F.; Klaase, B.; Graumans, C.; Wildt, M.D.R.D.; FBR Supply Chain & Information Management. *Blockchain for Agriculture and Food: Findings from the Pilot Study*; Wageningen University and Research: Wageningen, The Netherlands, 2017.
77. Politou, E.; Casino, F.; Alepis, E.; Patsakis, C. Blockchain Mutability: Challenges and Proposed Solutions. *IEEE Trans. Emerg. Top. Comput.* **2019**, 1. [CrossRef]
78. Korpela, K.; Hallikas, J.; Dahlberg, T. Digital Supply Chain Transformation toward Blockchain Integration. In Proceedings of the Proceedings of the 50th Hawaii International Conference on System Sciences (2017), Waikoloa, HI, USA, 4–7 January 2017.
79. Yadav, S.; Singh, S.P. Blockchain critical success factors for sustainable supply chain. *Resour. Conserv. Recycl.* **2020**, *152*, 104505. [CrossRef]
80. Rathod, N.; Motwani, D. Security Threats on Blockchain and its Countermeasures. *Int. Res. J. Eng. Technol* **2018**, *5*, 1636–1642.
81. Treiblmaier, H. The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. *Supply Chain Manag. Int. J.* **2018**, *23*, 545–559. [CrossRef]
82. Wang, Y.; Han, J.H.; Beynon-Davies, P. Understanding blockchain technology for future supply chains: A systematic literature review and research agenda. *Supply Chain Manag. Int. J.* **2019**, *24*, 62–84. [CrossRef]
83. Sulkowski, A.J. Blockchain, Business Supply Chains, Sustainability, and Law: The Future of Governance, Legal Frameworks, and Lawyers? *SSRN Electron. J.* **2018**. [CrossRef]
84. Rouhani, S.; Pourheidari, V.; Deters, R. Physical Access Control Management System Based on Permissioned Blockchain. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; Institute of Electrical and Electronics Engineers (IEEE): Piscataway Township, NJ, USA, 2018; pp. 1078–1083.
85. Fernandez-Carames, T.M.; Fraga-Lamas, P. A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories. *IEEE Access* **2019**, *7*, 45201–45218. [CrossRef]
86. Sittón-Candanedo, I.; Alonso, R.S.; Corchado, J.M.; Rodríguez-González, S.; Casado-Vara, R. A review of edge computing reference architectures and a new global edge proposal. *Futur. Gener. Comput. Syst.* **2019**, *99*, 278–294. [CrossRef]
87. Kshetri, N. Can Blockchain Strengthen the Internet of Things? *IT Prof.* **2017**, *19*, 68–72. [CrossRef]
88. Gu, J.; Sun, B.; Du, X.; Wang, J.; Zhuang, Y.; Wang, Z. Consortium Blockchain-Based Malware Detection in Mobile Devices. *IEEE Access* **2018**, *6*, 12118–12128. [CrossRef]
89. Huang, J.; Kong, L.; Chen, G.; Wu, M.-Y.; Liu, X.; Zeng, P. Towards Secure Industrial IoT: Blockchain System With Credit-Based Consensus Mechanism. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3680–3689. [CrossRef]
90. Makhdoom, I.; Abolhasan, M.; Abbas, H.; Ni, W. Blockchain's adoption in IoT: The challenges, and a way forward. *J. Netw. Comput. Appl.* **2019**, *125*, 251–279. [CrossRef]
91. Mao, D.; Hao, Z.; Wang, F.; Li, H. Novel Automatic Food Trading System Using Consortium Blockchain. *Arab. J. Sci. Eng.* **2019**, *44*, 3439–3455. [CrossRef]
92. Sylim, P.; Liu, F.; Marcelo, A.; Fontelo, P. Blockchain Technology for Detecting Falsified and Substandard Drugs in Distribution: Pharmaceutical Supply Chain Intervention. *JMIR Res. Protoc.* **2018**, *7*, e10163. [CrossRef] [PubMed]

93. Salah, D.; Ahmed, M.H.; ElDahshan, K. Blockchain Applications in Human Resources Management. In Proceedings of the Proceedings of the Evaluation and Assessment in Software Engineering, Trondheim, Norway, 15–17 April 2020; ACM: New York, NY, USA, 2020.
94. Yi, C.S.S.; Yung, E.; Fong, C.; Tripathi, S. Benefits and Use of Blockchain Technology to Human Resources Management: A Critical Review. *Int. J. Hum. Resour. Stud.* **2020**, *10*, 131–140. [CrossRef]
95. Khan, S.; Khan, R. Multiple Authorities Attribute-Based Verification Mechanism for Blockchain Mircogrid Transactions. *Energies* **2018**, *11*, 1154. [CrossRef]
96. Weber, R.H. Internet of Things—New security and privacy challenges. *Comput. Law Secur. Rev.* **2010**, *26*, 23–30. [CrossRef]
97. Azbeg, K.; Ouchetto, O.; Andaloussi, S.J.; Fetjah, L.; Sekkaki, A. Blockchain and IoT for Security and Privacy: A Platform for Diabetes Self-management. In Proceedings of the 2018 4th International Conference on Cloud Computing Technologies and Applications (Cloudtech), Brussels, Belgium, 26–28 November 2018; pp. 1–5.
98. Acharjamayum, I.; Patgiri, R.; Devi, D. Blockchain: A Tale of Peer to Peer Security. In Proceedings of the 2018 IEEE Symposium Series on Computational Intelligence (SSCI), Bangalore, India, 18–21 November 2018; Institute of Electrical and Electronics Engineers (IEEE) Symposium Series on Computational Intelligence (SSCI): Piscataway Township, NJ, USA, 2018; pp. 609–617.
99. Sinha, U.; Hadi, A.A.; Faika, T.; Kim, T. Blockchain-Based Communication and Data Security Framework for IoT-Enabled Micro Solar Inverters. In *2019 IEEE CyberPELS (CyberPELS)*; Institute of Electrical and Electronics Engineers (IEEE): Piscataway Township, NJ, USA, 2019; pp. 1–5.
100. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Big Island, HI, USA, 13–17 March 2017; Institute of Electrical and Electronics Engineers (IEEE): Piscataway Township, NJ, USA, 2017; pp. 618–623.
101. 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]
102. Chawathe, S. Monitoring Blockchains with Self-Organizing Maps. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; Institute of Electrical and Electronics Engineers (IEEE): Piscataway Township, NJ, USA, 2018; pp. 1870–1875.
103. Miers, I.; Garman, C.; Green, M.; Rubin, A.D. Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In Proceedings of the 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 19–22 May 2013; Institute of Electrical and Electronics Engineers (IEEE): Piscataway Township, NJ, USA, 2013; pp. 397–411.
104. Ben Sasson, E.; Chiesa, A.; Garman, C.; Green, M.; Miers, I.; Tromer, E.; Virza, M. Zerocash: Decentralized Anonymous Payments from Bitcoin. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 18–21 May 2014; Institute of Electrical and Electronics Engineers (IEEE): Piscataway Township, NJ, USA, 2014; pp. 459–474.
105. Ucci, D.; Aniello, L.; Baldoni, R. Survey of machine learning techniques for malware analysis. *Comput. Secur.* **2019**, *81*, 123–147. [CrossRef]
106. Biryukov, A.; Khovratovich, D.; Pustogarov, I. Deanonymisation of Clients in Bitcoin P2P Network. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014; ACM: New York, NY, USA, 2014; pp. 15–29.
107. Crosby, M.; Pattanayak, P.; Verma, S.; Kalyanaraman, V. Blockchain technology: Beyond bitcoin. *Appl. Innov.* **2016**, *2*, 6–10.
108. Xie, J.; Tang, H.; Huang, T.; Yu, F.R.; Xie, R.; Liu, J.; Liu, Y. A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2794–2830. [CrossRef]
109. Yuan, R.; Xia, Y.-B.; Chen, H.-B.; Zang, B.-Y.; Xie, J. ShadowEth: Private Smart Contract on Public Blockchain. *J. Comput. Sci. Technol.* **2018**, *33*, 542–556. [CrossRef]
110. De Haro-Olmo, F.J.; Varela-Vaca, Á.J.; Álvarez-Bermejo, J.A. Blockchain from the Perspective of Privacy and Anonymisation: A Systematic Literature Review. *Sensors* **2020**, *20*, 7171. [CrossRef] [PubMed]
111. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 22–26 May 2016.
112. Veit, D.J.; Weinhardt, C. Enterprise, applications and services in the finance industry. *Inf. Syst. e-Business Manag.* **2007**, *5*, 139–141. [CrossRef]
113. Comelli, M.; Fenies, P.; Tchernev, N. A combined financial and physical flows evaluation for logistic process and tactical production planning: Application in a company supply chain. *Int. J. Prod. Econ.* **2008**, *112*, 77–95. [CrossRef]
114. Nguyen, Q.K. Blockchain—A Financial Technology for Future Sustainable Development. In Proceedings of the 2016 3rd International Conference on Green Technology and Sustainable Development (GTSD), Kaohsiung, Taiwan, 24–25 November 2016; pp. 51–54.
115. Augur, The Augur Project. Available online: https://augur.net/ (accessed on 16 May 2020).
116. Poon, J.; Buterin, V. Plasma: Scalable Autonomous Smart Contracts. *White Pap.* **2017**, *206*, 1–47.
117. Gnosis.io. Available online: https://gnosis.io/ (accessed on 27 July 2020).
118. Hewett, N.; Lehmacher, W.; Wang, Y. *Inclusive Deployment of Blockchain for Supply Chains: Part 5—A Framework for Blockchain Cybersecurity*; World Economic Forum: Geneva, Switzerland, 2019.

119. Kshetri, N. 1 Blockchain's roles in meeting key supply chain management objectives. *Int. J. Inf. Manag.* **2018**, *39*, 80–89. [CrossRef]
120. Wamba, S.F.; Queiroz, M.M.; Trinchera, L. Dynamics between blockchain adoption determinants and supply chain performance: An empirical investigation. *Int. J. Prod. Econ.* **2020**, *229*, 107791. [CrossRef]
121. 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]
122. Hackius, N.; Petersen, M. Blockchain in logistics and supply chain: Trick or treat? In *Proceeding of the Hamburg international conference of logistics*; HICL: Hamburg, Germany, 2017.
123. 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]
124. Kamble, S.S.; Gunasekaran, A.; Sharma, R. Modeling the blockchain enabled traceability in agriculture supply chain. *Int. J. Inf. Manag.* **2020**, *52*, 101967. [CrossRef]
125. Choi, D.; Chung, C.; Seyha, T.; Young, J. Factors Affecting Organizations' Resistance to the Adoption of Blockchain Technology in Supply Networks. *Sustainability* **2020**, *12*, 8882. [CrossRef]
126. Sahebi, I.G.; Masoomi, B.; Ghorbani, S. Expert oriented approach for analyzing the blockchain adoption barriers in humanitarian supply chain. *Technol. Soc.* **2020**, *63*, 101427. [CrossRef]
127. Dutta, P.; Choi, T.-M.; Somani, S.; Butala, R. Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transp. Res. Part E Logist. Transp. Rev.* **2020**, *142*, 102067. [CrossRef]
128. Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K. Where is current research on blockchain technology—A systematic review. *PLoS ONE* **2016**, *11*, e0163477. [CrossRef]
129. O'Leary, D.E. Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems. *Intell. Syst. Account. Financ. Manag.* **2017**, *24*, 138–147. [CrossRef]
130. Öztürk, C.; Yildizbaşi, A. Barriers to implementation of blockchain into supply chain management using an integrated multi-criteria decision-making method: A numerical example. *Soft Comput.* **2020**, *24*, 14771–14789. [CrossRef]
131. Cao, B.; Zhang, Z.; Feng, D.; Zhang, S.; Zhang, L.; Peng, M.; Li, Y. Performance analysis and comparison of PoW, PoS and DAG based blockchains. *Digit. Commun. Netw.* **2020**, *6*, 480–485. [CrossRef]
132. Brasil. Decreto—Lei nº 227, de 28 de fevereiro de Dá nova redação ao Decreto-lei nº 1.985, de 29 de janeiro de 1940 (Código de Minas). Brasília. Available online: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del0227.htm (accessed on 19 October 2020).
133. Baliga, A. Understanding Blockchain Consensus Models. Available online: https://pdfs.semanticschol-ar.org/da8a/37b10bc152 1a4d3de925d7ebc44bb606d740.pdf (accessed on 29 June 2017).
134. Karame, G. On the Security and Scalability of Bitcoin's Blockchain. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; ACM: New York, NY, USA, 2016; pp. 1861–1862.
135. Cho, S.; Park, S.Y.; Lee, S.R. Blockchain Consensus Rule Based Dynamic Blind Voting for Non-Dependency Transaction. *Int. J. Grid Distrib. Comput.* **2017**, *10*, 93–106. [CrossRef]
136. Geraci, A.; Katki, F.; McMonegal, L.; Meyer, B.; Lane, J.; Wilson, P.; Radatz, J.; Yee, M.; Porteous, H.; Springsteel, F. *IEEE Standard Computer Dictionary: Compilation of IEEE Standard Computer Glossaries*; IEEE Press: Piscataway Township, NJ, USA, 1991.
137. Scott, C.R. Benefits and Drawbacks of Anonymous Online Communication: Legal Challenges and Communicative Recommendations. *Free. Speech Yearb.* **2004**, *41*, 127–141. [CrossRef]
138. Gervais, A.; Karame, G.O.; Wüst, K.; Glykantzis, V.; Ritzdorf, H.; Capkun, S. On the Security and Performance of Proof of Work Blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; Association for Computing Machinery (ACM): New York, NY, USA, 2016; Volume 2016, pp. 3–16.
139. O'Leary, D.E. Open Information Enterprise Transactions: Business Intelligence and Wash and Spoof Transactions in Blockchain and Social Commerce. *Intell. Syst. Account. Financ. Manag.* **2018**, *25*, 148–158. [CrossRef]
140. Rahouti, M.; Xiong, K.; Ghani, N. Bitcoin Concepts, Threats, and Machine-Learning Security Solutions. *IEEE Access* **2018**, *6*, 67189–67205. [CrossRef]
141. Etemadi, N.v.G.P.; Strozzi, F. An ISM Modelling of Success Factors for Blockchain Adoption in a Cyber Secure Supply Chain. In Proceedings of the 4th International Conference on Computers in Management and Business, ICCMB 2021, Singapore, January 30–February 1 2021; ACM: New York, NY, USA. [CrossRef]
142. Al-Jaroodi, J.; Mohamed, N. Blockchain in Industries: A Survey. *IEEE Access* **2019**, *7*, 36500–36515. [CrossRef]
143. Khan, F. What is the "Oracle Problem" and How Does Chainlink Solve It? Available online: www.datadriveninves-tor.com/2019/06/15/what-is-the-oracle-problem-how-does-chainlink-solve-it/ (accessed on 23 February 2021).
144. Damjan, M. The interface between blockchain and the real world. *Ragion Pratica* **2018**. [CrossRef]
145. Kamilaris, A.; Fonts, A.; Prenafeta-Boldύ, F.X. The rise of blockchain technology in agriculture and food supply chains. *Trends Food Sci. Technol.* **2019**, *91*, 640–652. [CrossRef]
146. 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]
147. Kosmarski, A. Blockchain Adoption in Academia: Promises and Challenges. *J. Open Innov. Technol. Mark. Complex.* **2020**, *6*, 117. [CrossRef]

148. Li, J.; Maiti, A.; Springer, M.; Gray, T. Blockchain for supply chain quality management: Challenges and opportunities in context of open manufacturing and industrial internet of things. *Int. J. Comput. Integr. Manuf.* **2020**, *33*, 1321–1355. [CrossRef]
149. Siegfried, N.; Rosenthal, T.; Benlian, A. Blockchain and the Industrial Internet of Things. *J. Enterp. Inf. Manag.* **2020**. [CrossRef]
150. Zhou, Y.; Soh, Y.S.; Loh, H.S.; Yuen, K.F. The key challenges and critical success factors of blockchain implementation: Policy implications for Singapore's maritime industry. *Mar. Policy* **2020**, *122*, 104265. [CrossRef]
151. Chang, V.; Baudier, P.; Zhang, H.; Xu, Q.; Zhang, J.; Arami, M. How Blockchain can impact financial services—The overview, challenges and recommendations from expert interviewees. *Technol. Forecast. Soc. Chang.* **2020**, *158*, 120166. [CrossRef]
152. Shardeo, V.; Patil, A.; Madaan, J. Critical Success Factors for Blockchain Technology Adoption in Freight Transportation Using Fuzzy ANP–Modified TISM Approach. *Int. J. Inf. Technol. Decis. Mak.* **2020**, *19*, 1549–1580. [CrossRef]
153. Morkunas, V.J.; Paschen, J.; Boon, E. How blockchain technologies impact your business model. *Bus. Horiz.* **2019**, *62*, 295–306. [CrossRef]
154. Scott, B.; Loonam, J.; Kumar, V. Exploring the rise of blockchain technology: Towards distributed collaborative organizations. *Strat. Chang.* **2017**, *26*, 423–428. [CrossRef]
155. Holotiuk, F.; Pisani, F.; Moormann, J. Radicalness of blockchain: An assessment based on its impact on the payments industry. *Technol. Anal. Strat. Manag.* **2019**, *31*, 915–928. [CrossRef]
156. Abu-Elezz, I.; Hassan, A.; Nazeemudeen, A.; Househ, M.; Abd-Alrazaq, A. The benefits and threats of blockchain technology in healthcare: A scoping review. *Int. J. Med Inform.* **2020**, *142*, 104246. [CrossRef]
157. Ghode, D.; Yadav, V.; Jain, R.; Soni, G. Adoption of blockchain in supply chain: An analysis of influencing factors. *J. Enterp. Inf. Manag.* **2020**, *33*, 437–456. [CrossRef]
158. Upadhyay, A.; Ayodele, J.O.; Kumar, A.; Garza-Reyes, J.A. A review of challenges and opportunities of blockchain adoption for operational excellence in the UK automotive industry. *J. Glob. Oper. Strat. Sourc.* **2020**, *14*, 7–60. [CrossRef]
159. Tanwar, S.; Bhatia, Q.; Patel, P.; Kumari, A.; Singh, P.K.; Hong, W.-C. Machine Learning Adoption in Blockchain-Based Smart Applications: The Challenges, and a Way Forward. *IEEE Access* **2020**, *8*, 474–488. [CrossRef]
160. Kouhizadeh, M.; Saberi, S.; Sarkis, J. Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers. *Int. J. Prod. Econ.* **2021**, *231*, 107831. [CrossRef]
161. Chang, S.E.; Chen, Y.-C.; Lu, M.-F. Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process. *Technol. Forecast. Soc. Chang.* **2019**, *144*, 1–11. [CrossRef]
162. Mendling, J.; Weber, I.; Van Der Aalst, W.; Brocke, J.V.; Cabanillas, C.; Daniel, F.; Debois, S.; Di Ciccio, C.; Dumas, M.; Dustdar, S.; et al. Blockchains for Business Process Management—Challenges and Opportunities. *ACM Trans. Manag. Inf. Syst.* **2018**, *9*, 1–16. [CrossRef]
163. Saberi, S.; Kouhizadeh, M.; Sarkis, J. Blockchains and the Supply Chain: Findings from a Broad Study of Practitioners. *IEEE Eng. Manag. Rev.* **2019**, *47*, 95–103. [CrossRef]
164. Alkhater, N.; Walters, R.; Wills, G. An empirical study of factors influencing cloud adoption among private sector organisations. *Telemat. Inform.* **2018**, *35*, 38–54. [CrossRef]
165. Shin, N.; Park, S. Evidence-Based Resilience Management for Supply Chain Sustainability: An Interpretive Structural Modelling Approach. *Sustainability* **2019**, *11*, 484. [CrossRef]
166. Van Alstyne, M. Why Bitcoin has value. *Commun. ACM* **2014**, *57*, 30–32. [CrossRef]
167. Böhme, R. *Internet Protocol Adoption: Learning from Bitcoin*; IAB Workshop on Internet Technology Adoption and Transition (ITAT): Cambridge, UK, 2018.
168. Alharby, M.; Van Moorsel, A. Blockchain Based Smart Contracts: A Systematic Mapping Study. *arXiv* **2017**, arXiv:1710.06372.
169. Chen, G.; Xu, B.; Lu, M.; Chen, N.-S. Exploring blockchain technology and its potential applications for education. *Smart Learn. Environ.* **2018**, *5*, 1. [CrossRef]
170. Dolev, S.; Wang, Z. SodsBC: Stream of Distributed Secrets for Quantum-safe Blockchain. In Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, 2–6 November 2020; Institute of Electrical and Electronics Engineers (IEEE): Piscataway Township, NJ, USA, 2020; pp. 247–256.
171. Singh, A.; Teng, J.T. Enhancing supply chain outcomes through Information Technology and Trust. *Comput. Hum. Behav.* **2016**, *54*, 290–300. [CrossRef]
172. Chen, S.; Shi, R.; Ren, Z.; Yan, J.; Shi, Y.; Zhang, J. A Blockchain-Based Supply Chain Quality Management Framework. In Proceedings of the 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE), Shanghai, China, 4–6 November 2017; Institute of Electrical and Electronics Engineers (IEEE): Piscataway Township, NJ, USA, 2017; Volume 207, pp. 172–176.
173. Ghode, D.J.; Yadav, V.; Jain, R.; Soni, G. Blockchain adoption in the supply chain: An appraisal on challenges. *J. Manuf. Technol. Manag.* **2020**, *32*, 42–62. [CrossRef]
174. Seebacher, S.; Maleshkova, M. A Model-driven Approach for the Description of Blockchain Business Networks. In Proceedings of the 51th Hawaii International Conference on System Sciences, Waikoloa, HI, USA, 3 January 2018; pp. 3487–3496.
175. Helo, P.; Hao, Y. Blockchains in operations and supply chains: A model and reference implementation. *Comput. Ind. Eng.* **2019**, *136*, 242–251. [CrossRef]
176. Kurpjuweit, S.; Schmidt, C.G.; Klöckner, M.; Wagner, S.M. Blockchain in Additive Manufacturing and its Impact on Supply Chains. *J. Bus. Logist.* **2019**, 1–25. [CrossRef]

177. Gökalp, E.; Gökalp, M.O.; Çoban, S. Blockchain-Based Supply Chain Management: Understanding the Determinants of Adoption in the Context of Organizations. *Inf. Syst. Manag.* **2020**, 1–22. [CrossRef]
178. Kumar, R.; Tahir, M.F.; Kumar, S.; Zia, A.; Memon, H.; Mahmood, W. Challenges in Adoption of Blockchain in Developing Countries. In Proceedings of the 2019 4th International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST), Karachi, Pakistan, 10–11 December 2019; Institute of Electrical and Electronics Engineers (IEEE): Piscataway Township, NJ, USA, 2019; pp. 1–8.
179. Ramdani, B.; Kawalek, P.; Lorenzo, O. Predicting SMEs' adoption of enterprise systems. *J. Enterp. Inf. Manag.* **2009**, *22*, 10–24. [CrossRef]
180. Bernik, I.; Prislan, K. Measuring Information Security Performance with 10 by 10 Model for Holistic State Evaluation. *PLoS ONE* **2016**, *11*, e0163050. [CrossRef] [PubMed]
181. Wüst, K.; Gervais, A. Do you need a Blockchain? In Proceedings of the 2018 Crypto Val. Conf. Blockchain Technology, Zug, Switzerland, 20–22 June 2018; pp. 45–54. [CrossRef]
182. Lo, S.K.; Xu, X.; Chiam, Y.K.; Lu, Q. Evaluating Suitability of Applying Blockchain. In Proceedings of the 2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS), Fukuoka, Japan, 5–8 November 2017; Institute of Electrical and Electronics Engineers (IEEE): Piscataway Township, NJ, USA, 2017; pp. 158–161.
183. Mann, S.; Potdar, V.; Gajavilli, R.S.; Chandan, A. Blockchain Technology for Supply Chain Traceability, Transparency and Data Provenance. In Proceedings of the 2018 International Conference on Blockchain Technology and Application—ICBTA 2018, Xi'an, China, 10–12 December 2018; ACM: New York, NY, USA, 2018; pp. 22–26.
184. Luu, L.; Chu, D.-H.; Olickel, H.; Saxena, P.; Hobor, A. Making Smart Contracts Smarter. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; Association for Computing Machinery (ACM): New York, NY, USA, 2016; pp. 254–269.
185. NIST's Second Round Announcement Call for Proposals PostQuantum Cryptosystems. Available online: https://csrc.nist.gov/news/2019/pqc-standardization-process-2nd-roundcandidates (accessed on 3 March 2021).
186. 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.* **2020**. [CrossRef]
187. Hileman, G.; Rauchs, M. Global Blockchain Benchmarking Study. *SSRN Electron. J.* **2017**. [CrossRef]
188. Davies, S.; Likens, S. Blockchain is Here: What's Your Next Move? Pwc.com. 2019. Available online: https://www.pwc.com/gx/en/issues/blockchain/blockchain-in-business.html (accessed on 13 March 2021).
189. Govindan, K.; Kannan, G.; Haq, A.N. Analyzing supplier development criteria for an automobile industry. *Ind. Manag. Data Syst.* **2010**, *110*, 43–62. [CrossRef]
190. Toktaş-Palut, P.; Baylav, E.; Teoman, S.; Altunbey, M. The impact of barriers and benefits of e-procurement on its adoption decision: An empirical analysis. *Int. J. Prod. Econ.* **2014**, *158*, 77–90. [CrossRef]
191. Bolaños, R.; Fontela, E.; Nenclares, A.; Pastor, P. Using interpretive structural modelling in strategic decision-making groups. *Manag. Decis.* **2005**, *43*, 877–895. [CrossRef]
192. Govindan, K.; Azevedo, S.G.; Carvalho, H.; Cruz-Machado, V. Lean, green and resilient practices influence on supply chain performance: Interpretive structural modeling approach. *Int. J. Environ. Sci. Technol.* **2015**, *12*, 15–34. [CrossRef]
193. Warfield, J.N. Implication Structures for System Interconnection Matrices. *IEEE Trans. Syst. Man Cybern.* **1976**, *SMC-6*, 18–24. [CrossRef]
194. Pandey, V.; Garg, S. Analysis of interaction among the enablers of agility in supply chain. *J. Adv. Manag. Res.* **2009**, *6*, 99–114. [CrossRef]
195. Ruiz-Benítez, R.; López, C.; Real, J.C. The lean and resilient management of the supply chain and its impact on performance. *Int. J. Prod. Econ.* **2018**, *203*, 190–202. [CrossRef]
196. Prasad, S.; Shankar, R.; Gupta, R.; Roy, S. A TISM modeling of critical success factors of blockchain based cloud services. *J. Adv. Manag. Res.* **2018**, *15*, 434–456. [CrossRef]
197. Yadav, V.S.; Singh, A.; Raut, R.D.; Govindarajan, U.H. Blockchain technology adoption barriers in the Indian agricultural supply chain: An integrated approach. *Resour. Conserv. Recycl.* **2020**, *161*, 104877. [CrossRef]
198. Godet, M. *From Anticipation to Action: A Handbook of Strategic Prospective*; UNESCO Publishing: Paris, France, 1993.