future internet

Article

Leveraging the Internet of Things and Blockchain Technology in Supply Chain Management

Abderahman Rejeb [1], John G. Keogh [2] and Horst Treiblmaier [3,*]

1 Department of Logistics and Forwarding, Széchenyi István University, 9026 Győr, Hungary
2 Henley Business School, University of Reading, Greenlands, Henley-on-Thames, RG9 3AU, UK
3 Department of International Management, Modul University Vienna, 1190 Vienna, Austria
* Correspondence: horst.treiblmaier@modul.ac.at

Received: 27 May 2019; Accepted: 17 July 2019; Published: 20 July 2019

Abstract: Modern supply chains have evolved into highly complex value networks and turned into a vital source of competitive advantage. However, it has become increasingly challenging to verify the source of raw materials and maintain visibility of products and merchandise while they are moving through the value chain network. The application of the Internet of Things (IoT) can help companies to observe, track, and monitor products, activities, and processes within their respective value chain networks. Other applications of IoT include product monitoring to optimize operations in warehousing, manufacturing, and transportation. In combination with IoT, Blockchain technology can enable a broad range of different application scenarios to enhance value chain transparency and to increase B2B trust. When combined, IoT and Blockchain technology have the potential to increase the effectiveness and efficiency of modern supply chains. The contribution of this paper is twofold. First, we illustrate how the deployment of Blockchain technology in combination with IoT infrastructure can streamline and benefit modern supply chains and enhance value chain networks. Second, we derive six research propositions outlining how Blockchain technology can impact key features of the IoT (i.e., scalability, security, immutability and auditing, information flows, traceability and interoperability, quality) and thus lay the foundation for future research projects.

Keywords: Blockchain; Internet of Things; supply chain; transparency; value chain

1. Introduction

Supply chains are becoming increasingly heterogeneous and complicated due to a growing need for inter- and intra-organizational connectedness, which is enabled by advances in modern technologies and tightly coupled business processes [1,2]. To cope with this dynamic environment and the increasing need to digitize supply chains and enhance competitiveness, companies are applying novel technologies such as the Internet of Things (IoT), cloud computing, business analytics, artificial intelligence, machine learning, and Blockchain technology [3–5], as well as innovative concepts such as the so-called physical Internet [6]. The multiplicity of technologies, which are often simultaneously introduced, along with the ubiquity of connected devices, often labeled as 'smart' devices or things, allow value chain exchange (or trading) partners to reach new levels of effectiveness and efficiency [7]. These technologies promise to reshape the modus operandi of modern supply chains through enhanced data collection as well as information sharing and analysis between collaborating supply chain stakeholders [8]. Moreover, they enhance information transparency, leading to increased trust between the exchange partners [9,10]. The impact of these technologies on supply chains constitutes a research gap that is relevant for both practitioners and academics.

IoT is defined as a "group of infrastructures interconnecting connected objects and allowing their management, data mining and the access to data they generate" [11] (p. 73). It embodies the next phase toward mass digitization of supply chains to facilitate the so-called Industry 4.0 [12]. IoT encompasses devices such as sensors as well as passive, semi-passive (or semi-active), and active Radio Frequency ID tags (RFID), and other electronics which are connected over a network. Together, these technologies can perform numerous tasks, including functions such as sensing activity, movement, or temperature; actuating and collecting; processing, storing, and sharing data. For example, the food supply chain is particularly sensitive to environmental conditions during transportation and storage, such as light, humidity and temperature [13]. In the cold chain, time-temperature measurements with sensor devices connected to a wireless sensor network (WSN) can help to preserve the quality and safety of a food product and reduce the risk of spoilage [14]. WSNs represent a network or system of connected sensors which communicate to a base station through mobile networks such as 4G or GPRS (General Packet Radio Service) and informs supply chain exchange partners in real-time [14]. When the information is received, it can trigger an acceptance or rejection of the shipment based on the temperature parameters preset in a smart contract, which in turn can trigger payment if accepted. Moreover, when IoT-enabled sensor devices connected to a WSN provide time-temperature alerts on a real-time basis, an out of tolerance measurement (or a predictive out of tolerance measurement) can trigger a mid-shipment corrective action and intervention by the driver or shipper [8,9].

The growing economic importance of IoT reflects in its steadily increasing industry adoption. With the convergence of information and communication technologies (ICT) and machine automation, the use of IoT has become more pervasive, especially in supply chains and logistics. This trend is attributable to increased computational power and decreased costs of the connected devices. The International Data Corporation (IDC) forecasts that by 2021, 20% of the largest (G2000) manufacturers will depend on a secure infrastructure backbone of embedded intelligence to automate large-scale processes and enhance the speed of process execution by up to 25%. This backbone will mainly depend on IoT for enabling controls and actuators to take autonomous decisions [15]. In 2017, there was an estimated 5 billion IoT enabled devices, and this number is expected to reach 29 billion by 2022 [16]. Global connectivity will contribute further to new economic opportunities and business growth that may generate an additional USD 14 trillion in the global economy by 2030 [17].

Various researchers identified supply chains and logistics as essential areas for deploying IoT [18,19]. IoT can improve supply chain competitiveness through more effective tracking of the flow of materials, leading to improvements in the effectiveness and efficiencies of critical processes and timetables [20]. Within multi-exchange party supply chains, IoT can help to facilitate the sharing of more precise and timely information related to production, quality assurance, distribution and logistics [21–23]. Hofmann and Rüsch [24] posited an integrated solution for a Just-in-Time (JIT) production line where RFID tags act to trigger an alert when a specific station is empty. This warning signal notifies the supplier to replenish and deliver the stock directly to the specific station. Moreover, the use of IoT applications inside the production plant can increase the visibility of parts and processes, and by extension, using IoT devices along the supply chain can help to boost productivity, reduce operational costs, and enhance customer satisfaction [25].

Despite the growing potential to apply IoT in supply chains, there are numerous challenges ahead. For instance, IoT-related technical issues experienced when operating at the ecosystem level, such as security, authenticity, confidentiality, and privacy of all stakeholders [26]. From an IoT vulnerability perspective, practitioners and scholars consider security to be the most critical issue [27–29]. Existing security solutions are not well suited because current IoT devices may consume significant amounts of energy and may have significant processing overhead [30]. Moreover, problems such as counterfeiting, physical tampering, hacking, and data theft might raise trust concerns among supply chain exchange partners [31]. Tzounis et al. [26] (p. 42) therefore conclude that "IoT must be secure against external attacks, in the perception layer, secure the aggregation of data in the network layer and offer specific guarantees that only authorized entities can access and modify data in the application layer".

Necessary safeguards must be developed to leverage the value and enhance the trust of connected IoT devices in supply chains. For instance, Blockchain technology now offers several potential solutions to address known issues related to IoT. A Blockchain is a distributed network for orchestrating transactions, value, and assets between peers, without the assistance of intermediaries [32]. It is also commonly referred to as a 'ledger' that records transactions [33]. Another way to view a particular Blockchain is as a configuration of multiple technologies, tools and methods that address specific problems or use cases [8]. With the adopting of Blockchain technology, companies aim to enhance information transparency and improve trust in their supply chains while supporting the interoperability among the networked supply chain exchange partners. Blockchain technology has the potential to address several known supply chain issues [34]. As a result, it has gained considerable attention from scholars, firms, and technology developers who seek to combine IoT with other technologies [35,36]. Currently, supply chains are undergoing an evolutionary change through continued digitization. They are evolving into value-creating networks where the value chain itself turns into a vital source of competitive advantage. At the same time, developments are in progress to integrate Blockchain technology with IoT solutions, leading to novel structures of modern supply chains, new partnerships, as well as new ways of collaboration and value creation across supply networks [37].

In this paper, we explore how companies can leverage IoT in combination with Blockchain technology to streamline their supply chains and value-creating networks. When combined, these enabling technologies will help firms to overcome problems related to data acquisition and integrity, address security challenges, mitigate traceability concerns, and reduce information asymmetry. In the following section, we review IoT in the context of supply chain usage and present various benefits and vulnerabilities. Subsequently, we discuss the critical role of Blockchain technology in leveraging IoT-based supply chain applications. In the final section, we make some concluding remarks and present suggestions for future research. The propositions that we derive in this paper extend existing academic literature by providing a structured foundation for systematic research that investigates the combined impact of IoT and Blockchain technology on modern supply chains.

2. Methodology

In this paper, we conducted a narrative literature review with the goals of summarizing the existing body of literature, identifying essential research gaps and developing novel research propositions. Given that Blockchain technology is in a nascent stage, only a small number of papers have been published in top-tier academic journals so far, which ruled out a systematic literature review. In order to take into account recent developments, we also included "grey" literature in our study. Furthermore, we used EBSCO Business Source Premier, Scopus, IEEE Xplore, ScienceDirect, and Google Scholar as our primary sources, but also screened numerous conferences proceedings and references (snowballing) of published papers to find additional and related materials. We used the following search terms: ("Blockchain*" or "Blockchain technologies") and ("Internet of Things" or "IoT") and ("supply chain*" or "logistics"). The paper collection and analysis took place between February and May 2019. The authors screened each paper for relevance, and the core topics were briefly summarized. Subsequently, we combined all topics and derived research questions by creating a map in which we listed the potential impacts of Blockchain technology on various IoT characteristics.

3. The Internet of Things and Its Application in Supply Chains

The concept of the "Internet of Things" (IoT) was first coined in 1999 by British entrepreneur and startup-founder Kevin Ashton [38]. In essence, IoT refers to an information network that connects sensors on or in physical objects ('things') ranging from consumer goods, pallets of goods to everyday tools, household appliances, and industrial machinery. Furthermore, cloud computing and the more recent concept of fog computing (i.e., a decentralized computing structure, extending the concept of cloud computing through the local performance of computation, storage and communication through so-called 'edge devices') provide computing resources and scalability to connect, store and analyze IoT data (often labeled as big data) received from connected devices and sources including WSNs, global positioning systems (GPS), GPRS, and geographic information systems (GIS). The analysis of IoT data can assist firms to sense and then respond to situations in real-time and may lead to automation or value-creating predictive analytics capabilities [26]. Moreover, through the connection of a heterogeneous set of hardware devices (e.g., sensors) IoT streamlines critical business processes through the capture of data, such as the identification of human operators and environmental variables (e.g., temperature, humidity, vibration, air currents). IoT devices are often deployed to sense the physical world, communicate over a wireless signal and to actuate based on predefined conditions. According to Barreto et al. [39] the three distinguishing features of IoT are context, omnipresence and optimization. The context describes the capability of IoT to provide real-time monitoring, to interact, and to enable an instant response to specific situations that are controlled. Omnipresence lies in the pervasiveness of the technology and its broad applicability, while optimization refers to the specific functionalities and characteristics each physical object has [40]. These features pave the way for novel and innovative IoT use cases among exchange partners within both simple and complex supply chains and open up new business opportunities. With the shift towards 5G technology with faster data transmission rates, IoT is expected to mature rapidly with pervasive integration into society. Cisco, a leading network technology provider, predicts that the number of IoT devices connected to the internet will reach 500 billion by 2030 [41]. Additionally, IoT has a wide range of potential applications and use cases across multiple sectors, including healthcare, automotive, industrial activities, smart homes, agriculture, and construction [42].

According to Lee and Lee [43], there are five crucial IoT technologies predominately used in supply chains and logistics. They include RFID, wireless sensor networks (WSN), middleware, cloud computing, and IoT application software. RFID is a technology used in many supply chain activities (i.e., warehousing, manufacturing, transportation) [44]. Passive RFID tags (without a power source) in modern supply chains utilize the GS1 Electronic Product Code (EPC) UHF Gen 2 industry standard (see https://www.gs1.org/sites/default/files/docs/epc/GS1_EPC_TDS_i1_12.pdf). Passive tags rely on wireless radio waves from a reader/antenna to identify physical objects that the tags are attached to or associated with without the need for line of sight between the reader/antennae and the tags [45]. Some unique applications of UHF Gen 2 tags may extend the tag read range up to 300′. RFID tags can also be 'semi-active' with a power source and send an intermittent signal to a network or signal when physically moved (e.g., attached to a high-value asset). Active RFID tags or devices have a power source and send out an active beaconing signal to a network. When RFID devices are connected to an IoT network, the WSN is described as a cluster of nodes (i.e., connection points for data transmission within a network) that cooperatively sense and actuate physical or environmental conditions (e.g., temperature, humidity, light intensity, velocity), allowing interaction between persons or computers and the surrounding environment [46]. WSNs benefit supply chains with more effective real-time monitoring of logistics activities through smart sensing capabilities. This capability leads to a better allocation of critical resources due to the higher level of data granularity in decision making and resource allocation. The middleware serves as a hub for collecting and storing the data generated by the connected devices and structures the data in a usable format for IoT applications [47]. This layer enhances the availability of the data, offers more granular insights and can make data more accessible to operational staff and management for analysis and decision making. Cloud computing facilitates the ubiquitous and on-demand access to a shared pool of configurable computing resources such as computers, networks, servers, storage, applications, services, and software applications [43]. Cloud computing offers some benefits in orchestrating parts of the supply chain data and information flows between multiple fragmented entities, facilitating cooperation among all value chain exchange partners [48]. Typically, an IoT application resides in the cloud and is accessed either by mobile application-based (apps) running on smartphones, tablets or desktop computers [49]. These applications advance machine-to-machine and human-to-machine interactions, resulting in a seamless processing of data and timely transfer of information.

3.1. IoT in Supply Chains: Levers and Application Scenarios

The application of IoT promises significant improvements in supply chain performance and operational efficiency. The benefits result primarily from real-time information exchange, which can reduce time wastage caused by the bullwhip effect [50,51]. Moreover, IoT can help to mitigate the risk of counterfeiting and illicit trade when combined with covert, overt or forensic security features on physical products. Thus, IoT is set to revolutionize supply chains by improving operational efficiencies and creating revenue opportunities [52]. Three of the areas that can benefit from IoT deployment include (1) inventory management and warehouse operations, (2) production and manufacturing operations, and (3) transportation operations (see Table 1).

Table 1. IoT Levers in Supply Chains.

Inventory Management and Warehouse Operations	
Enablers	**Processes**
- Smart racks - Smart glasses - Monitoring cameras - Smart forklifts - Smart warehouse management system (WMS)	- Route optimization, elimination of in-process collisions - Fast, cost-efficient, and flexible operations - Better handling of items that are hard to reach or 'dark assets' (i.e., items that are difficult to detect on the shelf or racks) - Real-time visibility of inventory levels - Avoidance of stockouts - Agility and fast responsiveness to inadequacies (e.g., misplacement of items) - Workspace monitoring (e.g., for security purposes) - Stock keeping units (e.g., pallets) recognition and localization - Simultaneous threat detection and scanning for imperfections
Production and Manufacturing Operations	
Enablers	**Processes**
- Embedded machine sensors - Machine analytics	- Real-time condition monitoring - Remote maintenance - Predictive maintenance: Detection of physical stress levels, pile-ups, and prevention of failures - Improved measurement of throughput, setup-time, and overall productivity - Enhancement of both machine-to-machine and machine-to-human interactions
Transportation Operations	
Enablers	**Processes**
- GPRS sensors - RFID sensors - Routers - GPS satellites	- Continuous visibility of products along the supply chain - Real-time shipment tracking - Remote product sensing (e.g., temperature, humidity, vibrations) - Protection and preservation of product quality - Improve activity bottlenecks and outdoor traffic, transport mobility, road and driver safety - Maximizing fuel efficiency and optimize routing strategies - Improved service delivery

IoT paves the way for smarter inventory management where key processes in warehousing operations can be optimized, labour costs reduced, and throughput time improved [53]. Technical enablers include smart forklifts and racks but also novel usage of 'smart glasses' (i.e., wearables devices equipped with sensors and camera technologies to locate objects in the warehouse), monitoring cameras, and warehousing software. Within warehouse operations, reusable assets such as inventory storage totes and pallets can be tagged with IoT enabled tags or devices that assist in guiding and directing the warehouse picker to their storage locations. IoT not only aids in automating aspects of warehousing activities (e.g., picking and packing) but also leads to efficiencies by reducing manual effort spent on locating the exact position of products and materials in warehouses. Importantly, cost savings and error reductions are attainable through the use of IoT by automating the warehouse or distribution centre inventory receiving and order dispatch processes, which in turn reduces human intervention (and error) associated with manual storage management. This benefit results from deploying commercial RFID readers and antennas in receiving and shipping docks that send a radio signal to identify RFID tags attached to, or embedded on pallets, totes, or the product cartons leading to a reduction in the time spent in collecting, recording, and retrieving data [54,55]. Besides, RFID tags help to overcome the (occasional) problematic readability of barcodes in specific industrial environments and result in a higher read accuracy [56].

Production and manufacturing are the second area that can benefit from the implementation of IoT. Industrial machines with embedded sensors can be monitored in real-time and controlled by smart instruments, such as microcomputers, microcontrollers, microprocessors, and intelligent sensors. IoT-based solutions can enhance operational control over the processing capacity, set-up time, and throughput. Therefore, their usage can lead to more efficient machine utilization, reduction of bottlenecks in production and can help in optimizing production planning and scheduling at varying levels within a company. Moreover, Waller and Fawcett [57] point out that IoT enablement leads to greater agility and proactivity in the company by enabling quick identification of machine errors and enabling predictive maintenance. As a result, this enhanced insight into key manufacturing processes will enable stronger collaboration and value co-creation with suppliers [58] as well as improved machine-to-machine and machine-to-human interaction.

Finally, when it comes to transportation activities in supply chains, IoT can also provide potential benefits. For instance, IoT-enabled solutions usher in a well-defined and configured transportation management system (TMS) or "smart" TMS [39]. More specifically, a set of IoT devices can help to transform transportation processes and achieve more flexible and efficient operations. For example, a GPS helps to position refrigerated trucks from remote distribution centers and to optimize both routing and delivery time while preserving product quality [59]. In a broader sense, GPS, RFID, and other connected sensors increase the in-transit visibility by measuring conditions such as temperature, humidity, and by precisely localizing vehicles on public roads or at shipping terminals through large scale mapping, traffic data collection and analysis. The data gathered from these IoT devices will help to improve forecasting of delivery times, fleet availability, and routing efficiency [57]. Moreover, these devices can be used for enhancing the sharing of under-utilized resources among vehicles in the parking space or on the road [39].

3.2. IoT in Supply Chains: Weaknesses and Threats

IoT has the potential to 'connect the unconnected' and can help to optimize supply chain operations [60] substantially. It addresses several supply chain challenges including the growing business need to enhance supply chain information transparency and improve the integrity of production data and the identity of products (i.e., the right products, at the right time, place, quantity, condition, at the right cost) [39]. However, as IoT will generate massive volumes of data across the supply chain, this data often resides in silos, which are generally underutilized and fail to extract real-time business insights. As such, data silos can be seen as trapped or hidden sources of potential business insights and value. Global analysts firm Gartner refer to data silos as 'dark data' and suggest that firms are often guilty of data hoarding (https://www.gartner.com/smarterwithgartner/how-to-tackle-dark-data/).

Several issues regarding IoT security need to be addressed [61], including IoT device trust, access control, data integrity, physical tampering, and user privacy. One study revealed that 70% of IoT devices have vulnerabilities due to a lack of encryption, unprotected interfaces, poor software protection, and inadequate authorization [43]. In discussing various security and privacy challenges, Cam-Winget et al. [60] argue that contemporary security solutions are inadequate because of scalability issues to process and analyze data transmitted from large networks of heterogeneous devices and the need to satisfy real-time requirements. Conventional security and privacy approaches are considered inapplicable to IoT ecosystems due to their dynamic topology and distributed nature. Besides, the current Internet architecture with its server-based infrastructure might not be able to deal with a countless number of devices and large amounts of data because individual servers may pose a single point of failure for cyber-attacks and physical damage. For instance, IoT devices are at risk from DDoS attacks, data theft, and remote hijacking. Furthermore, Marjani et al. [62] assert that some IoT systems lack a service level agreement to protect personally identifiable information (PII) demanded by privacy laws. Hence, this can negatively affect data integrity and security and may lead to negative repercussions in privacy protection for both individuals and firms [63].

Additionally, supply chain exchange partners may have concerns regarding the physical security and confidentiality of product information as it moves along the supply chain. Even though IoT helps supply chain exchange partners to validate and verify the authenticity of items in the supply chain, there are still some concerns about the vulnerability of IoT devices to counterfeiting, cloning, and fraudulent practices, such as unauthorized access, tampering, and manipulation of content. For example, if RFID tags are compromised, it may be possible to bypass security measures and to introduce new vulnerabilities during automatic verification processes [64]. Moreover, the manual retrieval and storage of information regarding unique tag identities in a centralized database enables the reproducing or forging of this information at any time [65]. Therefore, it is difficult to identify counterfeit products accompanied by misleading provenance histories [59].

Finally, centralized systems may pose a weakness for IoT deployments in the supply chain for traceability purposes. The existence of centralized institutions may lead to distrust (or suspicion), which may limit the further improvement of supply chains [66]. A centralized approach for data hosting and control can lead to several business risks and operational issues related to data integrity, security, and privacy. For example, cloud-based solutions for monitoring IoT data may be subject to manipulation and privacy legislation issues that arise when exporting substantial amounts of confidential and highly sensitive information to external services in other jurisdictions [31,60]. Additionally, these solutions may cause opacity and increase information asymmetry between supply chain exchange partners. A compounding factor is that centralized systems act as a black box, and the participating nodes do not know how their data is stored, managed, utilized, and secured [67]. Blockchain technology can help to alleviate several of these problems.

4. Blockchain Technology

A Blockchain is defined as a “digital, decentralized and distributed ledger in which transactions are logged and added in chronological order with the goal of creating permanent and tamperproof records” [34] (p. 547). Essentially, it is a novel mechanism for storing, securing and sharing data between multiple nodes in a network [68]. A Blockchain breaks away from the traditional centralized approach by managing chain data across a distributed and interlinked network of nodes. The main characteristics of Blockchains are shared recordkeeping, immutability, decentralization, distributed trust, multiple-party consensus, independent validation, tamper evidence, and tamper resistance [69,70]. The term ‘Blockchain’ gained its popularity as the output of a combination of configured technologies, tools and methods underpinning the cryptocurrency Bitcoin. In itself, Bitcoin is a decentralized digital currency based on an open system of computer networks and online communication protocols [33] and was the first successful application built on an online Blockchain.

Blockchains can be configured to encrypt and store on-chain or off-chain data and record timestamped transactions. Furthermore, they can automate agreements through the utilization of smart contracts to run procedures based upon a set of conditions, terms, and rules that participants in the system have agreed upon [71]. A Blockchain platform can support multi-party exchange relationships in global supply chains by authenticating participant identities, authorizing their access and enhancing recordkeeping of transactions. This capability is possible by cryptographic mechanisms and recursive hashing of blocks. Each block contains a header and a body, the former of which contains the hash of the previous block, thus connecting the individual blocks. Any attempt to tamper with a block necessitates that the headers of previous and consecutive blocks be changed accordingly to avoid detection, and it gets progressively more difficult to tamper with as the chain gets longer. Since their pervasiveness and distributed nature characterize IoT networks, a centralized approach to collecting, storing, and analyzing all relevant supply chain data may cause delays and lead to a situation often referred to a single point of failure. A Blockchain, therefore, has the potential to address the challenges mentioned above and provide supply chain exchange partners with trust based on decentralization [31]. The lack of centralized controls in Blockchains ensures a high-level of scalability and robustness by using resources of all involved nodes and eliminating many-to-one traffic flows [30].

5. Combining IoT with Blockchain Technology: Emerging Research Areas

Blockchains allow for the decentralized aggregation of vast amounts of data generated from IoT devices and ensures that benefits are shared more equitably across supply chain exchange partners. In the following sections, we discuss the main research areas at the intersection between IoT and Blockchain technology including scalability, security, immutability and auditing, effectiveness and efficiency of information flow, traceability and interoperability, and quality as is shown in Figure 1. We end each section with a question for further research.

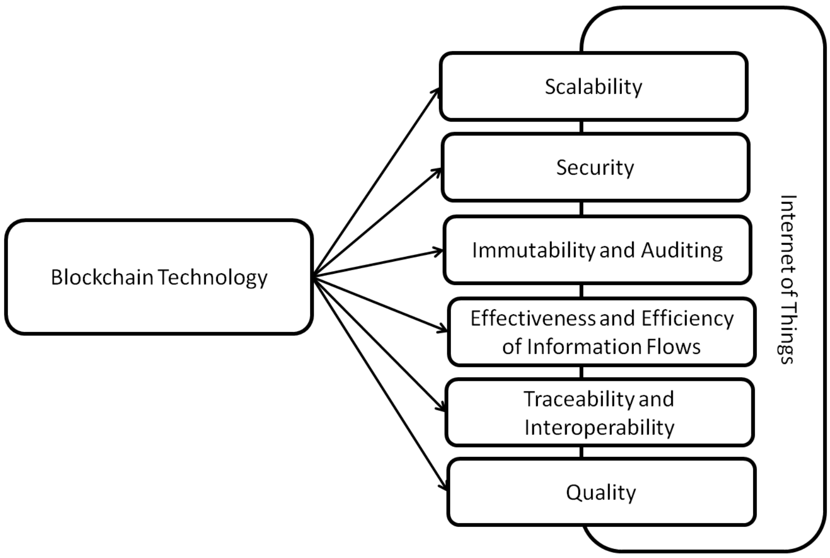

Figure 1. The impact of Blockchain technology on IoT characteristics

5.1. Scalability

Unlike mining nodes in cryptocurrencies, IoT devices such as sensors have limited computing ability, which is both difficult and computationally expensive to improve [72]. Several Blockchain solutions have been developed and introduced to address the scalability requirements of IoT in the supply chain. Depending on the industry type, consensus mechanisms and Blockchain structures might be more or less compatible with IoT applications. In this regard, private or consortium Blockchains are viewed as highly beneficial for many supply chain applications because they have a limited number of nodes and can apply IoT data filtering to increase the scalability of the Blockchain. Applications can integrate IoT networks with smart contracts and benefit from enhanced scalability with a capacity of tens of thousands of transactions per second [73].

The evolving Blockchain architecture leads to the emergence of 'off-chain' scaling solutions. These include so-called sidechains, which are chains that run in parallel to the Blockchain and allow the transfer of value between them [74]. The ever-increasing data generated from IoT devices in the supply chain can be encrypted and stored in the sidechains, and a reference to them can be added into the main Blockchain. This functionality helps to significantly reduce the storage complexity by offloading the data from a Blockchain in terms of transactions processed [75]. Moreover, although in its infancy and with a lack of interoperability standards, inter-Blockchain communication promises higher levels of scalability [76]. Examples of transactions that can run on the sidechains include fast payment systems, crowd sale and token distribution, transfer of digital assets, and ID generation. Off-chain models widen the scope of Blockchain uses by setting up networks which operate certain functions within the Blockchain model, but also localizing certain operations outside the Blockchain system [77]. These might include off-chain smart contracts, raw files of third-party food safety, quality, or faith-based certifications (e.g., HACCP, BRC, Halal, Kosher); third party analytical laboratory results and quality records.

A configured Blockchain could be administered in either a centralized database (e.g., MySQL) or in the form of Distributed Hash Table (DHT) technology [78,79]. In this way, (off-chain) transactions are performed faster, and scalability is enhanced [80]. Beyond this, off-chain solutions hold promise for being compatible with business infrastructures containing non-vital information [81]. More examples of off-chain methods include multi-chains (e.g., the Cosmos network powered by Tendermint [82]), the lightning network [83], payment channels (e.g., Raiden [84], and Sprites [85]).

Furthermore, Blockchain-enabled IoT applications in the supply chain are evolving to the specific network characteristics of IoT, such as heterogeneity, dynamic topology, complexity, scalability, throughput, and memory size. These methods aim to enhance the scalability by altering the core elements of the Blockchain transaction, including the increase of the block size, the use of new or specific lightweight network protocols for IoT devices [73–86], sharding techniques (i.e., splitting work between subsets of nodes in order to increase throughput) [87] editable Blockchains [88] and the Directed Acyclic Graph (DAG) [89,90]. Increasing the block size of public Blockchains can further enhance scalability and offer additional storage and processing capabilities but may slow down the propagation rate of blocks in the network. The development of Blockchain scalable protocols for IoT applications (e.g., Delegated Proof of Stake, Practical Byzantine fault tolerance, Proof of Assignment [91]) could significantly improve the scalability and the flexibility of the Blockchain system. Moreover, the design of IoT-specific consensus protocols would benefit the integration of a Blockchain in an IoT-based supply chain and create opportunities for developing content-oriented consensus protocols. Collectively, these advancements will enhance the integrity of sensory data through the cross-validation with the sensory data from other IoT nodes and historical data [92].

Sharding is a novel mechanism to alleviate scalability by distributing contents of a database across nodes in a network [93]. Partitioning a Blockchain might be especially suitable for IoT-enabled supply chains where the main chain handles less frequent global events (e.g., global transshipments, containers operations, disaster monitoring, and emergency plans) while secondary chains are established for recording frequent local transactions and logistical events of interest only to regional networks (e.g., inbound logistics, production monitoring, inventory control) [73]. However, the consistency and efficiency of inter-communication among Blockchain shards remain a challenging task to maintain. For example, the need for a scalable distributed ledger for IoT devices has resulted in the emergence of alternative data structures such as IOTA. Unlike traditional Blockchains, IOTA is a distributed architecture build upon a DAG called Tangle [90]. The tangle serves as a data structure that offers a set of significant advantages, including scalability, efficiency, fee-less, and real-time transactions [94]. Every node that registers a transaction has to verify two other transactions before its transaction is verified, which significantly speeds up the validation process. The Tangle meets the requirements of storing massive amounts of data and high-speed access to them. Moreover, its design introduces a new approach for reaching consensus and resolves the (often prohibitive) fees for microscale transactions required by IoT sensing and actuating use cases [95]. This implies that the applications of IoT in the supply chain will be enabled by a supporting platform that moves toward a more efficient and economic machine-to-machine interaction. In the case of multi-directional and tightly integrated supply chains, this might further lead to potential cost-savings and opportunities to generate new revenue streams. For instance, IOTA offers an IoT marketplace wherein sensor data can be bought and sold using Blockchain technology [96]. Various use cases illustrate the ability to transfer sensor data from the physical layer to the service layer more rapidly and securely, leading to real-time streamlining of transactions and better evaluations of different scenarios and tradeoffs (e.g., the choice of suitable protocols), and more increased micro-level IoT integration [97].

Even though existing proposals for enhancing scalability are confronted by the difficulty to combine decentralization, scalability, and security, the scalability of Blockchain technology is not necessarily an inherent problem for its integration with IoT-based supply chains. Likewise, many innovative and more scalable solutions are still under development to make Blockchain technology a key catalyst for transferring value and efficiently allocating resources among IoT networks in the foreseeable future. Parallel to this approach, Blockchain technology is reinventing cloud computing technology in that it facilitates greater levels of IoT scalability and mobility [98]. A practical use case that has emerged from coupling Blockchain with cloud storage is the IBM Watson IoT Blockchain which operates in a cloud environment and helps to process massive amounts of data among heterogeneous devices [31]. To empower IoT devices and sustain their operations in a completely trustless ecosystem, Ming et al. [99] propose the combination of service-centric networking (SCN) and Blockchain technology, in which the Blockchain is backed up by the ubiquitous IoT devices mobility and the global scalability offered by SCN. In sum, we put forward the following research proposition (RP):

RP 1: Blockchain technology positively impacts the scalability of IoT solutions.

5.2. *Security*

With the increasing complexity of supply chains and the proliferation of exchange partner relationships, firms are driven to secure their data and information exchanges as well as the integrity of their physical objects to protect against theft and various forms of illicit trade including diversion and counterfeiting. For example, companies need to keep pace with the continuous development of covert, overt, and forensic technologies to secure or monitor physical objects such as products, totes, pallets as well as supply chain operational events. In this regard, IoT and Blockchain are two emerging technologies that can enhance productivity and assist in assuring the integrity demanded by supply chain exchange partners. The combination of Blockchain technology with IoT is viewed as having substantial transformative power across several industries [100] since it shows a promising avenue for enabling the management of IoT devices [101,102]. The combination of Blockchains and IoT ushers in a more resilient, responsive, and distributed peer-to-peer system with the ability to interact with supply chain exchange partners in a 'trustless', secure and real-time manner. More importantly, Blockchain-enabled systems are capable of transforming the potential benefits of IoT and bridging the gap of device-data interoperability while maintaining security, privacy, and reliability.

Blockchain facilitates the resolution of several security challenges inherent in IoT devices and networks, such as unique device identification and trust management between different devices, data and information provenance tracking (to the authoritative source versus custodian sources), authentication and access control, and accountability in IoT-based applications [102]. The security mechanism under the Blockchain system mitigates the risk of a single point of failure due to its decentralization approach. In other words, Blockchain technology helps to eliminate the risk of network failure and collapse in case of a node crash. Woodside et al. [103] point out that Blockchain technology can foster the protection of a supply chain from most malicious attacks. Moreover, Preuveneers et al. [104] confirm the usefulness of the Blockchain protocol to secure an IoT network by enabling communication between trustworthy nodes while eschewing malicious nodes. Blockchain technology can restrict the access of some selected devices and minimize the possibilities of unauthorized access.

Similarly, IoT serves as a link between the physical and digital world. It enables supply chain exchange partners to receive reliable information directly from the physical objects tracked on the Blockchain. This capability, in turn, ensures the sharing of unique and authentic information from the device, which reduces the risk of deliberate fraud whereby misleading information is added to the Blockchain through a standard human interface. This enhances both transparency and trust because once data (or information) is entered into the Blockchain, it is considered immutable and tamper-proof. Any attempt at data manipulation will be quickly detected, and retrospectively traced back to its source. Consequently, the business risk will lower significantly due to effective fraud detection and audit enforced by Blockchain technology. However, human manipulation of data or information in non-IoT scenarios remains a challenge for the industry. Since the IoT ecosystem relies on several points of contact with the physical world, namely products, totes, pallets, this connection is subject to a particular risk of tampering, falsification, and exchange party collusion. Physical objects or IoT sensors can still be tampered with [105]. For instance, a product's IoT enabled tag links the physical product to its virtual identity (often called a 'digital twin') but does not necessarily reflect its complete traceability and a legitimate IoT device can be removed and placed on another physical object such as a counterfeit. An integrated system incorporating barcodes, RFID tags, sensors, and Blockchain could facilitate consumers to reject the purchase of counterfeits even with an authentic tag if the seller does not possess the (digital) ownership of products in the Blockchain system [106]. Consequently, Blockchain-based solutions can help to crosscheck and verify the identification and the authenticity of IoT devices. For example, Chronicled, a San Francisco-based technology startup, combines IoT sensors, NFC embedded adhesive seals, and QR codes in an Ethereum Blockchain platform [107]. IoT devices are protected against forging and counterfeiting thanks to the tamper-resistant nature of the Blockchain. Hence, we posit:

RP2: Blockchain technology positively impacts the security of IoT solutions.

5.3. Immutability and Auditing

The integration of Blockchain technology with IoT devices advances supply chain automation and creates an ecosystem consisting of immutable transactions that allow for improved audit. Supply chains exchange partners gain from the combined application of Blockchain and IoT through safe and auditable transactional data exchange within a massively heterogeneous and context-aware setting [108]. When connected on a network, smart IoT devices can consistently and autonomously push data into the Blockchain platform, creating an immutable and auditable transactional history which is useful for product traceability, recall, product provenance, and authentication purposes. Blockchain technology, thus, enables a fine-grained audit capability [109] where sensor values can add additional trust incorporating real-time and immutable data [110]. These characteristics sparked the attention of IoT technology providers who are adapting their IoT network-based solutions to Blockchain-based technology [111].

In automating several supply chain activities, Blockchains can include and leverage smart contracts, a term first coined by Nick Szabo in 1994 and predating Bitcoin's usage of Blockchain by more than a decade. A smart contract, such as an automated payment through a financial institution, is defined as a computerized protocol that executes the terms of a contract [112]. Intelligent contracts streamline processes, ensure privacy and enable supply chain exchange partners to take full advantage of automation efficiencies. This benefit is evident in the ability to process information streamed from IoT devices and networks without any downtime or human intervention and to support transactions between devices [100] safely. Smart contracts can be run and stored in the Blockchain system, and they guarantee the execution of rules in a pre-defined way. In doing so, they support auditing processes, and we postulate:

RP3-1: The immutability of Blockchain technology positively impacts the auditing of IoT solutions.

The idea of a 'mutable' (editable, redactable) Blockchain comes as a response to the ever-increasing complexity of the ledger, evolving business environments and the incremental accumulation of blocks. Moreover, it may be directly related to the overall poor quality of product data across supply networks [113]. Thus, the mutable Blockchain has been proposed to reverse, delete, and add new blocks in the Blockchain [88]. Since supply chains are experiencing the proliferation of IoT device usage, the use of editable Blockchains could address data errors caused during this nascent stage of IoT's evolution. As such, transactions generated from IoT sources and replicated across the Blockchain network could be edited or removed while still maintaining an immutable audit trail. Examples include IoT data for products already consumed, deactivated tags or sensors, reusable tags or sensors, damaged or faulty tags or sensors, and outdated or retired/unusable technologies. Currently, firms are exploring the possibility of mutable Blockchains, changing the way hash pointers link blocks so that only authorized parties can modify past blocks [114]. Despite being intuitively contradictory to immutability as a key attribute of Blockchain technology, these mutable Blockchains create new opportunities but also raise new questions related to the rules and governance for performing edits and corrective actions. Thus, we postulate:

RP3-2: Mutable Blockchain technology creates new application scenarios for IoT usage and management.

5.4. Effectiveness and Efficiency of Information Flows

Blockchain applications create new opportunities with respect to tracking physical assets and goods in multi-party supply chains. Verified supply chain exchange partners will be informed about relevant assets, products or merchandise, whether online, in-transit, or in-store [77]. When informed about the movement of physical assets (totes, pallets, shipping containers), raw materials or ingredients, components or end consumer products, firms attain better control of their supply chains. Subsequently, firms are increasingly facilitating consumer access to product related information online or through mobile devices. For instance, consumers can use a smartphone to scan a barcode or QR code on the primary packaging of a food product and access relevant data and information recorded on a Blockchain system. This could include information such as product and brand information, allergens, ingredients, product origin (provenance), traceability, processing method, transportation and its route to market. The product supplier's ability to assure transaction authenticity and record and provide an open report on the transfer of ownership remains one of the core benefits of Blockchain technology [115]. As an illustration, the use of IoT along with Blockchain in the cold chain for the storage and distribution of perishable food products is proving to be critical in reflecting the leverage achieved by utilizing IoT sensors and Blockchain technology together. For example, companies such as OriginTrail and ZetoChain use an open, standards-based Blockchain platform for the supply chain. The former company aligns with the global industry standards body GS1 to ensure its open source Blockchain protocol integrates and interoperates with the globally recognized and utilized industry-standard used to uniquely identify products, physical locations such as farms, factories or distribution centers and a firm's unique global identification. The latter company monitors every link of the cold chain based on the usage of IoT devices [116]. Any problem that occurs is immediately identified, and the supply chain exchange partners are notified accordingly to enable swift action to be taken. Sensors combining the usage of GPS, temperature data and smart contracts are harnessed to automate the process and update a product's digital profile whenever anomalies are detected during the distribution phase. Accordingly, mobile apps are increasingly being used by consumers to scan labels on products in order to locate a product's history [117].

Equally important, the combination of Blockchain technology and IoT provides a reliable infrastructure for improving supply chain information management, arranging legal agreements and securing the storage of IoT device identities throughout the product's life-cycle stages [118]. Critical threshold data captured with sensors and stored on the Blockchain are useful for managing plant equipment, predicting failures, and scheduling appropriate proactive repair and maintenance before breakdowns occur. Regulators, suppliers of machinery and spare parts,, as well as repair and maintenance service providers, could gain shared access to equipment records and provide inspections and certifications to achieve high equipment availability and utilization [119]. Therefore, it is anticipated that the integration of Blockchain technology with IoT will be a catalyst for increased remote machine diagnostics, reciprocal data analytics, and machine-to-supplier interactions resulting in improved spare parts replacement and overall maintenance practices [120]. We therefore propose:

> RP4: Blockchain technology positively impacts the effectiveness, efficiency, and integrity of information flows in IoT solutions.

5.5. Traceability and Interoperability

Blockchain technology is already used in combination with tamper-evident RFID-tags to aid in the verification of the provenance (e.g., geographic source or origin) and authenticity of bottles of fine wine. The tags are affixed to the cork and aim to eliminate attempts to refill wine bottles with a cheaper product. By logging the data on the Blockchain and crosschecking the traceability and provenance of the wine bottles, consumers can verify the history and authenticity of the purchased wine by inputting the product ID in the system [65]. It should be noted that absolute certainty on the authenticity of any food or drink product can only be achieved using science-based analytical testing methods of the product itself rather than relying on covert or overt security features on the outer package. Several projects are in development to apply a combination of Blockchain and IoT for enhanced traceability and interoperability. For example, firms such as UK-based Evrythng; Slovenian-based OriginTrail, a Blockchain protocol provider; and Ambrosus, a Swiss-based Blockchain startup, aim to combine the Blockchain and the IoT for the food, consumer goods, apparel, and pharmaceutical sector. In doing so, their Blockchain-powered IoT networks will enable a secure and frictionless dialogue between sensors, distributed ledgers, and databases to optimize supply chain visibility and quality assurance [121–123]. In another example, Skycell, a company developing containers for refrigerated biopharmaceuticals, uses IoT sensors along with the Blockchain to monitor temperature, humidity, and location, thereby reducing temperature deviations to a level of less than 0.1% [124]. Given these current developments, we propose:

> RP5: Blockchain technology positively impacts the traceability and interoperability of IoT solutions.

5.6. Quality

Apart from providing a decentralized migration path for IoT data, Blockchain technology addresses the problem of data and information quality existing in other information technology platforms. It complements the need for maintaining consistent data provenance that describes where the data of interest originates, who owns the data and what transformations were made to the data [125]. In this way, the metadata posted on the Blockchain is protected from compromise and unauthorized disclosure. For instance, Blockchain technology is suitable for distributed cloud storage. Blending the technology into the cloud environment can lead to improved data provenance where cloud nodes record data over a distributed network with a fault-tolerant ledger and strong cryptography [126]. Hence, the 'block cloud'—a combined usage of the Blockchain and cloud computing—paves the way to self-sovereign data management and ownership by allowing private and contextual access to IoT data hosted across cloud layers. In empowering IoT, Blockchain technology could be easily merged with the application of big data in supply chain use cases which implies a shift for supply chains from being digitally enabled to digitally-led and process-centric [127]. However, several shortcomings still exist in this infrastructural integration. For instance, big data is increasingly encountering three critical challenges, namely control (governance and monitoring of the data structure when several parties are involved), data authenticity (reliability and trustworthiness), and data monetization (transfer of the ownership of data and exchange in a universal data marketplace) [128]. Blockchain technology can be used to exert more control over IoT-based supply chain data, ensure their integrity and immutability, and establish a marketplace for data provided by IoT devices [129]. Moreover, a Blockchain-based big data system can facilitate aggregation of IoT data coming from scattered sources across the supply chain, thus creating a more suitable data sharing ecosystem and conducive analytics for business insights and decision making. Hence, we propose:

RP6: Blockchain technology positively impacts the quality and integrity of IoT solutions.

6. Discussion

Blockchain technology is gaining momentum in global supply chains and shows great potential in leveraging IoT as well as enhancing interoperability and governance of IoT devices. Supply chain exchange partners can reap many benefits from this convergence. The proliferation of IoT devices improves the connectivity within and between multiple organizations and generates a massive amount of valuable data. At the same time, firms strive to solve the issues of security, oversight, privacy, trust, and transparency between different stakeholders [130]. When operating under distributed digital ledger platforms such as a Blockchain, supply chain exchange partners will benefit from a new form of governance, enhanced information transparency and improvements in the integrity of IoT transaction data. During the physical transit of products and raw materials through supply chains, IoT devices can capture data concerning specific functions (e.g., product tracking, machine monitoring, environmental sensing) and transmit them to the Blockchain network. In turn, distributed ledgers will secure data storage and provide more oversight for supply chain exchange partners. Moreover, analytical tools can extract business insights from the data collection in real-time, allowing a business to sense and respond to supply chain anomalies more rapidly.

Blockchain facilitates machine-to-machine interaction where sensors and IoT devices attached to machinery will be synchronized, resulting in high flexibility and collaboration with exchange partners. The importance of this new capability lies in the secure communication, confidentiality, and integrity of the exchange transactions. Users can transact with the machines directly and engage in on-demand manufacturing services by sending transactions to a registered machine [131]. Blockchain-based distributed ledgers that harness smart contracts enable the embedding of business logic covering a wide range of purposes such as payment conditions, product acceptance, smart inventory replenishment, predictive maintenance, and repairs.

By combining Blockchain technology and IoT, exchange partners gain new and timely insights into their supply chain in real-time with more precise and reliable information about key processes, events, and product attributes—such as quality, performance and availability. This fusion of IoT and Blockchain technology can help to enhance end-to-end traceability and enable rapid recall capabilities of unsafe goods [33]. As a result, exchange partners will be informed about the products, the potential risks, and the preventive and corrective actions needed for sustaining the sufficient flow of safe products to the final consumers.

The confluence of IoT-driven data, Blockchain technology and mobility enables physical assets to become digitally active in the various stages of their lifecycles [132]. This implies that supply chains need to adapt to new rules and forms of governance shaped by the specific features of these emergent technologies, and new regulations should be created for addressing specific situations [133]. For example, a problem of synchronization between Blockchain and IoT-sensing devices in the cold chain leaves many open questions as to who will be legally accountable for any eventualities associated with the product journey in cross-border settings. The same goes for concerns regarding smart contracts used in a Blockchain–IoT combination (e.g., reliance on "off-chain" resources, unintended programming errors, conflicts between jurisdictions) [134]. To summarize, in this paper, we identified various areas in which the combination of IoT and Blockchain deserves further attention. Table 2 lists the research propositions that we derived in the previous sections.

Table 2. Summary of Research Propositions.

Proposition	Area
RP 1: Blockchain technology positively impacts the scalability of IoT solutions.	Scalability
RP2: Blockchain technology positively impacts the security of IoT solutions.	Security
RP3-1: The immutability of Blockchain technology positively impacts the auditing of IoT solutions.	Immutability & Auditing
RP3-2: Mutable Blockchain technology creates new application scenarios for IoT usage and management.	
RP4: Blockchain technology positively impacts the effectiveness, efficiency and integrity of information flows in IoT solutions.	Effectiveness and efficiency of information flow
RP5: Blockchain technology positively impacts the traceability and interoperability of IoT solutions.	Traceability and interoperability
RP6: Blockchain technology positively impacts the quality and integrity of IoT solutions.	Quality

7. Conclusions, Limitations, and Further Research

In this conceptual paper, we have shown how the combination of Blockchain technology with IoT can trigger new opportunities to enhance supply chain integrity and improve operational performance. Simultaneously, the technologies can potentially yield new problems. For example, a Blockchain provides the benefit of immutability, which is seen as a core feature. However, immutability can be viewed as a negative feature for various reasons which are now drivers of a renewed interest in creating 'mutable' Blockchains. Thus, additional academic research is therefore needed to explore, explain and predict different application scenarios rigorously. This includes the application of academic theories, which might help to gain further insights on why specific phenomena occur.

It is important to note that there are several limitations and challenges concerning Blockchain integration in an IoT environment [70]. The heightened increase in the complexity of IoT infrastructure puts the Blockchain at the front of managing growing amounts of data that require high scalability. Privacy and scalability issues can be mitigated by the use of permissioned Blockchains, which are less resource-intensive and the concept of 'Blockchain pruning' (i.e., deleting unnecessary data or obsolete transactions) has been suggested as a possible solution. Nevertheless, these alternatives fuel the discussion over the immutable nature of Blockchains and the monopolistic approach of consortium ledgers that creates barriers to entry and hinders innovation [135].

Beyond geographical boundaries, the combination of Blockchain with IoT can be delayed by both regulatory uncertainties and the lack of industry standards [136]. Although Blockchain technology could enhance peer-to-peer connectivity between supply chain exchange partners, the integration of Blockchain and IoT challenges some of the institutional assumptions common in international business [137]. Indeed, harmonization (or 'equivalency' between sovereign states) of data protection laws remains a problem, while stronger industry self-regulation to govern and control the access to data and organize their transmission both nationally and globally is a requirement [138–140]. It is still unclear how disparate Blockchain technologies and systems will interoperate with each other and integrate with other technological artifacts. This is compounded by the existence of unreliable and inefficient transmission standards and protocols that clog the arteries of information sharing between the exchange partners. Additionally, an IoT environment is inherently dynamic, unpredictable and affected by the ever-changing laws and regulations related to security and other interoperability requirements [141,142]. Such sudden variability and chaotic nature necessitate new laws and regulations urgently [143].

It is our goal in this paper to lay the foundation for further research by suggesting six different research propositions. They need to be operationalized, refined and adapted to specific research contexts by other researchers. In order to foster incremental research, we especially encourage researchers to carefully investigate the applicability of existing theories to better understand emerging phenomena at the confluence of Blockchain, the IoT, and supply chain management.

Author Contributions: Conceptualization, A.R.; methodology, A.R.; J.G.K.; H.T.; model validation, A.R.; J.G.K.; H.T.; review, A.R.; J.G.K.; H.T.; writing—original draft preparation, A.R.; J.G.K.; H.T.; writing—review and editing, A.R.; J.G.K.; H.T; supervision, J.G.K; HT.

Funding: The publication of this work was supported by: EFOP- 3.6.1-16-2016-00017 (Internationalisation, initiatives to establish a new source of researchers and graduates and development of knowledge and technological transfer as instruments of intelligent specialisations at Széchenyi István University).

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

References

1. Sahin, F.; Robinson, E.P., Jr. Information sharing and coordination in make-to-order supply chains. *J. Oper. Manag.* **2005**, *23*, 579–598. [CrossRef]
2. Fayezi, S.; Zomorrodi, M. Supply Chain Management: Developments, Theories and Models. In *Handbook of Research on Global Supply Chain Management*; IGI Global: Hershey, PA, USA, 2015; pp. 313–340.
3. Zantalis, F.; Koulouras, G.; Karabetsos, S.; Kandris, D. A Review of Machine Learning and IoT in Smart Transportation. *Future Internet* **2019**, *11*, 94. [CrossRef]
4. Svorobej, S.; Takako Endo, P.; Bendechache, M.; Filelis-Papadopoulos, C.; Giannoutakis, K.M.; Gravvanis, G.A.; Tzovaras, D.; Byrne, J.; Lynn, T. Simulating Fog and Edge Computing Scenarios: An Overview and Research Challenges. *Future Internet* **2019**, *11*, 55. [CrossRef]
5. Li, Y. An Integrated Platform for the Internet of Things Based on an Open Source Ecosystem. *Future Internet* **2018**, *10*, 105. [CrossRef]
6. Treiblmaier, H. Combining Blockchain Technology and the Physical Internet to Achieve Triple Bottom Line Sustainability: A Comprehensive Research Agenda for Modern Logistics and Supply Chain Management. *Logistics* **2019**, *3*, 10. [CrossRef]
7. Kharlamov, A.; Parry, G. Advanced Supply Chains: Visibility, Blockchain and Human Behaviour. In *Innovation and Supply Chain Management*; Moreira, A.C., Ferreira, L.M.D.F., Zimmermann, R.A., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 321–343. ISBN 978-3-319-74303-5.
8. Rejeb, A.; Sűle, E.; Keogh, J.G. Exploring new technologies in procurement. *Transp. Logist. Int. J.* **2018**, *18*, 76–86.
9. Hofstede, G.J. Trust and transparency in netchains: A contradiction? In *Supply Chain Management: Issues in the New Era of Collaboration and Competition*; Wang, W.Y.C., Heng, M.S.H., Chau, P.Y.K., Eds.; Idea Group Inc.: Hershey, PA, USA; London, UK, 2007; pp. 105–126.
10. New, S. The transparent supply chain. *Harv. Bus. Rev.* **2010**, *88*, 1–5.
11. Dorsemaine, B.; Gaulier, J.-P.; Wary, J.-P.; Kheir, N.; Urien, P. Internet of things: A definition & taxonomy. In Proceedings of the 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, UK, 9–11 September 2015; pp. 72–77.
12. Lelli, F. Interoperability of the Time of Industry 4.0 and the Internet of Things. *Future Internet* **2019**, *11*, 36. [CrossRef]
13. Hsiao, H.-I.; Huang, K.-L. Time-temperature transparency in the cold chain. *Food Control* **2016**, *64*, 181–188. [CrossRef]
14. Óskarsdóttir, K.; Oddsson, G.V. Towards a decision support framework for technologies used in cold supply chain traceability. *J. Food Eng.* **2019**, *240*, 153–159. [CrossRef]
15. Knickle, K. Manufacturing and Manufacturing Technologies–Evolutions in Convergence. Available online: https://www.i-scoop.eu/industry-4-0/manufacturing-sector-manufacturing-technology-evolutions/ (accessed on 21 November 2018).

16. Barboutov, K.; Furuskär, A.; Inam, R.; Lindberg, P.; Öhman, K.; Sachs, J.; Sveningsson, R.; Torsner, J.; Wallstedt, K. *Ericsson Mobility Report*. Niklas Heuveldop, Sweden. 2017. Available online: https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-june-2017.pdf (accessed on 25 June 2019).
17. World Economic Forum. The Internet of Things and Connected Devices: Making the World Smarter. Available online: http://wef.ch/2ihHIY2 (accessed on 29 April 2019).
18. Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A survey. *Comput. Netw.* **2018**, *54*, 2787–2805. [CrossRef]
19. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [CrossRef]
20. Shrouf, F.; Ordieres, J.; Miragliotta, G. Smart factories in Industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm. In Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management, Bandar Sunway, Malaysia, 9–12 December 2014; pp. 679–701.
21. Chen, R.; Guo, J.; Bao, F. Trust management for service composition in SOA-based IoT systems. In Proceedings of the 2014 IEEE Wireless Communications and Networking Conference (WCNC), Istanbul, Turkey, 6–9 April 2014; pp. 3444–3449.
22. Cui, Y. Supply Chain Innovation with IoT. In *Multi-Criteria Methods and Techniques Applied to Supply Chain Management*; IntechOpen: London, UK, 2018.
23. Yan-e, D. Design of intelligent agriculture management information system based on IoT. In Proceedings of the 2011 Fourth International Conference on Intelligent Computation Technology and Automation, Shenzhen, China, 28–29 March 2011; Volume 1, pp. 1045–1049.
24. 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]
25. Deloitte. *Digital Procurement: New Capabilities from Disruptive Technologies*; Deloitte Development LLC: Stamford, CT, USA, 2017.
26. Tzounis, A.; Katsoulas, N.; Bartzanas, T.; Kittas, C. Internet of things in agriculture, recent advances and future challenges. *Biosyst. Eng.* **2017**, *164*, 31–48. [CrossRef]
27. Ahlmeyer, M.; Chircu, A.M. Securing the Internet of Things: A review. *Issues Inf. Syst.* **2016**, *17*, 21–28.
28. Gou, Q.; Yan, L.; Liu, Y.; Li, Y. Construction and strategies in IoT security system. In Proceedings of the 2013 IEEE international Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, Beijing, China, 20–23 August 2013; pp. 1129–1132.
29. Rahman, R.A.; Shah, B. Security analysis of IoT protocols: A focus in CoAP. In Proceedings of the 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, Oman, 15–16 March 2016; pp. 1–7.
30. 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), Kona, HI, USA, 13–17 March 2017.
31. Kshetri, N. Can Blockchain Strengthen the Internet of Things? *It Prof.* **2017**, *19*, 68–72. [CrossRef]
32. Mougayar, W. *The Business Blockchain*; John Wiley & Sons, Inc.: Hoboken, NJ USA, 2016.
33. Fosso Wamba, S.; Kamdjoug, K.; Robert, J.; Bawack, R.; G Keogh, J. Bitcoin, Blockchain, and FinTech: A Systematic Review and Case Studies in the Supply Chain. *Prod. Plan. Control* **2018**. Forthcoming.
34. 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]
35. Lima, A.C.E.S.; De Castro, L.N.; Corchado, J.M. A polarity analysis framework for Twitter messages. *Appl. Math. Comput.* **2015**, *270*, 756–767. [CrossRef]
36. Redondo-Gonzalez, E.; De Castro, L.N.; Moreno-Sierra, J.; Maestro De Las Casas, M.L.; Vera-Gonzalez, V.; Ferrari, D.G.; Corchado, J.M. Bladder carcinoma data with clinical risk factors and molecular markers: A cluster analysis. *BioMed Res. Int.* **2015**, *2015*, 168682. [CrossRef]
37. Pérez, L.; Dos Santos Paulino, V.; Cambra-Fierro, J. Taking advantage of disruptive innovation through changes in value networks: Insights from the space industry. *Supply Chain Manag. Int. J.* **2017**, *22*, 97–106. [CrossRef]

38. Keertikumar, M.; Shubham, M.; Banakar, R.M. Evolution of IoT in smart vehicles: An overview. In Proceedings of the 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, India, 8–10 October 2015; IEEE: Noida, India; pp. 804–809.
39. Barreto, L.; Amaral, A.; Pereira, T. Industry 4.0 implications in logistics: An overview. *Procedia Manuf.* **2017**, *13*, 1245–1252. [CrossRef]
40. Witkowski, K. Internet of Things, Big Data, Industry 4.0—Innovative Solutions in Logistics and Supply Chains Management. *Procedia Eng.* **2017**, *182*, 763–769. [CrossRef]
41. Griffiths, F.; Ooi, M. The fourth industrial revolution-Industry 4.0 and IoT [Trends in Future I&M]. *IEEE Instrum. Meas. Mag.* **2018**, *21*, 29–43.
42. Celestine, A.; Peter, J.D. An IoT based modified graph cut segmentation with optimized adaptive connectivity and shape priors. *Sustain. Comput. Inform. Syst.* **2018**. [CrossRef]
43. Lee, I.; Lee, K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Bus. Horiz.* **2015**, *58*, 431–440. [CrossRef]
44. Lu, W.; Huang, G.Q.; Li, H. Scenarios for applying RFID technology in construction project management. *Autom. Constr.* **2011**, *20*, 101–106. [CrossRef]
45. Rejeb, A. The Potentialities of RFID-Based Traceability System in the Olives Post-Harvest Stage. *J. Bus. Manag. Econ. Res.* **2018**, *2*, 13–25. [CrossRef]
46. Verdone, R.; Dardari, D.; Mazzini, G.; Conti, A. *Wireless Sensor and Actuator Networks: Technologies, Analysis and Design*; Elsevier: Amsterdam, The Netherlands, 2008.
47. Chaudhuri, A.; Dukovska-Popovska, I.; Chan, H.K.; Subramanian, N.; Bai, R.; Pawar, K.S. Development of a framework for big data analytics in cold chain logistics. In Proceedings of the International Symposium on Logistics, Kaohsiung, Taiwan, 3–6 July 2016; Centre for Concurrent Enterprise, Nottingham University Business School: Nottingham, UK, 2016; pp. 498–506.
48. Li, X.; Wang, Y.; Chen, X. Cold chain logistics system based on cloud computing. *Concurr. Comput. Pract. Exp.* **2012**, *24*, 2138–2150. [CrossRef]
49. Saragih, L.R.; Dachyar, M.; Zagloel, T.Y.M.; Satar, M. The Industrial IoT for Nusantara. In Proceedings of the 2018 IEEE International Conference on Internet of Things and Intelligence System (IOTAIS), Bali, Indonesia, 1–3 November 2018; pp. 73–79.
50. Wang, S.J.; Liu, S.F.; Wang, W.L. The simulated impact of RFID-enabled supply chain on pull-based inventory replenishment in TFT-LCD industry. *Int. J. Prod. Econ.* **2008**, *112*, 570–586. [CrossRef]
51. Zhou, Z. Applying RFID to reduce bullwhip effect in a FMCG supply chain. In Proceedings of the Advances in Computational Environment Science, Australia, Melbourne, 15–16 January 2012; Springer: Berlin/Heidelberg, Germany, 2012; pp. 193–199.
52. Newman, D. How IoT Will Impact The Supply Chain. Available online: https://www.forbes.com/sites/danielnewman/2018/01/09/how-iot-will-impact-the-supply-chain/#28322c3e37b1 (accessed on 23 December 2018).
53. Georgakopoulos, D.; Jayaraman, P.P.; Fazia, M.; Villari, M.; Ranjan, R. Internet of Things and Edge Cloud Computing Roadmap for Manufacturing. *IEEE Cloud Comput.* **2016**, *4*, 66–73. [CrossRef]
54. Amador, C.; Emond, J.P.; Nunes, M.C. do N. Application of RFID technologies in the temperature mapping of the pineapple supply chain. *Sens. Instrum. Food Qual. Saf.* **2009**, *3*, 26–33. [CrossRef]
55. Jedermann, R.; Ruiz-Garcia, L.; Lang, W. Spatial temperature profiling by semi-passive RFID loggers for perishable food transportation. *Comput. Electron. Agric.* **2009**, *65*, 145–154. [CrossRef]
56. Goyal, S.; Hardgrave, B.C.; Aloysius, J.A.; DeHoratius, N. The effectiveness of RFID in backroom and sales floor inventory management. *Int. J. Logist. Manag.* **2016**, *27*, 795–815. [CrossRef]
57. Waller, M.A.; Fawcett, S.E. Data science, predictive analytics, and big data: A revolution that will transform supply chain design and management. *J. Bus. Logist.* **2013**, *34*, 77–84. [CrossRef]
58. Obitko, M.; Jirkovský, V.; Bezdíček, J. Big data challenges in industrial automation. In Proceedings of the International Conference on Industrial Applications of Holonic and Multi-Agent Systems, Prague, Czech Republic, 26–28 August 2013; Springer: Berlin/Heidelberg, Germany, 2013; pp. 305–316.
59. Rejeb, A. Blockchain Potential in Tilapia Supply Chain in Ghana. *Acta Tech. Jaurinensis* **2018**, *11*, 104–118. [CrossRef]
60. Cam-Winget, N.; Sadeghi, A.-R.; Jin, Y. INVITED: Can IoT be Secured: Emerging Challenges in Connecting the Unconnected. In Proceedings of the 53rd Annual Design Automation Conference (DAC '16), Austin, TX, USA, 5–9 June 2016.

61. Yang, K.; Forte, D.; Tehranipoor, M.M. Protecting endpoint devices in IoT supply chain. In Proceedings of the IEEE/ACM International Conference on Computer-Aided Design, Austin, TX, USA, 2–6 November 2015; pp. 351–356.
62. Marjani, M.; Nasaruddin, F.; Gani, A.; Karim, A.; Hashem, I.A.T.; Siddiqa, A.; Yaqoob, I. Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges. *IEEE Access* **2017**, *5*, 5247–5261.
63. Suresh, P.; Daniel, J.V.; Parthasarathy, V.; Aswathy, R.H. A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. In Proceedings of the International Conference on Science Engineering and Management Research (ICSEMR), Chennai, India, 27–29 November 2014; pp. 1–8.
64. Xiao, Q.; Gibbons, T.; Lebrun, H. RFID Technology, Security Vulnerabilities, and Countermeasures. In *Supply Chain the Way to Flat Organization*; Intech: Vienna, Austria, 2009; pp. 357–382.
65. Biswas, K.; Muthukkumarasamy, V.; Tan, W.L. Blockchain Based Wine Supply Chain Traceability System. In Proceedings of the Future Technologies Conference (FTC), Vancouver, Canada, 29–30 November 2017; pp. 1–7.
66. Cekerevac, Z.; Prigoda, L.; Maletic, J. Blockchain Technology and Industrial Internet of Things in the Supply Chains. *Mest J.* **2018**, *6*, 39–47. [CrossRef]
67. Fabiano, N. Internet of Things and Blockchain: Legal issues and privacy. The challenge for a privacy standard. In Proceedings of the 2017 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), Exeter, UK, 21–23 June 2017; pp. 727–734.
68. Atlam, H.F.; Wills, G.B. Intersections between IoT and distributed ledger. *Adv. Comput.* **2019**, 1–41. [CrossRef]
69. 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*; Cambridge Center for Alternative Finance: Judge Business School, Cambridge, UK, 2018.
70. Treiblmaier, H. Toward More Rigorous Blockchain Research: Recommendations for Writing Blockchain Case Studies. *Front. Blockchain* **2019**, *2*, 1–15. [CrossRef]
71. Dodd, N. The Social Life of Bitcoin. *Theory Cult. Soc.* **2018**, *35*, 35–56. [CrossRef]
72. Yang, C.; Li, X.; Yu, Y.; Wang, Z. Basing Diversified Services of Complex IIoT Applications on Scalable Block Graph Platform. *IEEE Access* **2019**, *7*, 22966–22975. [CrossRef]
73. Wang, X.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Niu, X.; Zheng, K. Survey on Blockchain for Internet of Things. *Comput. Commun.* **2019**. Forthcoming. [CrossRef]
74. Bashir, I. *Mastering Blockchain*; Packt Publishing—Ebooks Account: Birmingham, UK, 17 March 2017.
75. Gazi, P.; Kiayias, A.; Zindros, D. Proof-of-stake sidechains. In Proceedings of the IEEE Symposium on Security & Privacy, San Francisco, CA, USA, 20–22 May 2019; pp. 1–36.
76. Croman, K.; Decker, C.; Eyal, I.; Gencer, A.E.; Juels, A.; Kosba, A.; Miller, A.; Saxena, P.; Shi, E.; Sirer, E.G.; et al. On scaling decentralized Blockchains. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 22–26 February 2016; pp. 106–125.
77. Dujak, D.; Sajter, D. Blockchain Applications in Supply Chain. In *SMART Supply Network*; Springer: Cham, Switzerland, 2019; pp. 21–46. [CrossRef]
78. Lu, Q.; Xu, X. Adaptable Blockchain-based systems: A case study for product traceability. *IEEE Softw.* **2017**, *34*, 21–27. [CrossRef]
79. Makhdoom, I.; Abolhasan, M.; Ni, W. Blockchain for IoT: The Challenges and a Way Forward. In *Proceedings of the 15th International Joint Conference on e-Business and Telecommunications—Volume 2: SECRYPT, Porto, Portugal, 26–28 July 2019*; INSTICC: Setúbal, Portugal, 2018.
80. Back, A.; Corallo, M.; Dashjr, L.; Friedenbach, M.; Maxwell, G.; Miller, A.; Poelstra, A.; Timón, J.; Wuille, P. Enabling Blockchain Innovations with Pegged Sidechains. White Paper. 2014. Available online: https://blockstream.com/sidechains.pdf (accessed on 10 May 2019).
81. de Kruijff, J.; Weigand, H. Understanding the Blockchain using enterprise ontology. In Proceedings of the International Conference on Advanced Information Systems Engineering, Essen, Germany, 12–16 June 2017; pp. 29–43.
82. Cosmos Network. Available online: https://cosmos.network/ (accessed on 20 May 2019).
83. Poon, J.; Dryja, T. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Available online: https://www.bitcoinlightning.com/wp-content/uploads/2018/03/lightning-network-paper.pdf (accessed on 25 May 2019).

84. Raiden Network. Available online: https://raiden.network/ (accessed on 20 May 2019).
85. Miller, A.; Bentov, I.; Kumaresan, R.; McCorry, P. Sprites: Payment channels that go faster than lightning. *arXiv* **2017**, arXiv:170205812.
86. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
87. Luu, L.; Narayanan, V.; Zheng, C.; Baweja, K.; Gilbert, S.; Saxena, P. A secure sharding protocol for open Blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 17–30.
88. Ateniese, G.; Magri, B.; Venturi, D.; Andrade, E. Redactable Blockchain–or–rewriting history in bitcoin and friends. In Proceedings of the 2017 IEEE European Symposium on Security and Privacy (EuroS&P), Paris, France, 26–28 April 2017; pp. 111–126.
89. Gramoli, V. From Blockchain consensus back to byzantine consensus. *Future Gener. Comput. Syst.* **2017**. [CrossRef]
90. Popov, S. The tangle. *Cit* **2018**, 131. Available online: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf (accessed on 25 May 2019).
91. IOTW. IOTW A Blockchain-Enabled IoT Data Platform. Available online: https://iotw.io/ (accessed on 20 May 2019).
92. Romero, D.; Ioannidis, V.N.; Giannakis, G.B. Kernel-based reconstruction of space-time functions on dynamic graphs. *IEEE J. Sel. Top. Signal Process.* **2017**, *11*, 856–869. [CrossRef]
93. Gencer, A.E.; van Renesse, R.; Sirer, E.G. Short paper: Service-oriented sharding for Blockchains. In *Proceedings of the International Conference on Financial Cryptography and Data Security*; Springer International Publishing: Cham, Switzerland, 2017; pp. 393–401.
94. Atlam, H.F.; Alenezi, A.; Alassafi, M.O.; Wills, G. Blockchain with Internet of Things: Benefits, challenges, and future directions. *Int. J. Intell. Syst. Appl.* **2018**, *10*, 40–48. [CrossRef]
95. Evrythng. *The Ledger of Every Thing What Blockchain Technology Can (and Cannot) Do for the IoT*; Blockchain Research Institute: Toronto, ON, Canada, 2017.
96. IOTA. Foundation IOTA. Available online: https://www.iota.org/ (accessed on 20 May 2019).
97. Strugar, D.; Hussain, R.; Mazzara, M.; Rivera, V.; Afanasyev, I.; Lee, J. An architecture for distributed ledger-based M2M auditing for electric autonomous vehicles. In Proceedings of the Workshops of the International Conference on Advanced Information Networking and Applications, Matsue, Japan, 27–29 March 2019; pp. 116–128.
98. Anomelechi, N.; Cooper, W.; Duncan, B.; Lamb, J.D. A Management View of Security and Cloud Computing. *CLOUD Comput.* **2018**, *2018*, 35.
99. Ming, Z.; Yang, S.; Li, Q.; Wang, D.; Xu, M.; Xu, K.; Cui, L. Blockcloud: A Blockchain-based Service-centric Network Stack. 2019, 1–19. Available online: https://static.coinpaprika.com/storage/cdn/whitepapers/448429.pdf (accessed on 25 May 2019).
100. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
101. Pilkington, M. Blockchain technology: Principles and applications. In *Research Handbook on Digital Transformations*; Edward Elgar: Cheltenham, UK, 2016; pp. 1–39.
102. Perboli, G.; Musso, S.; Rosano, M. Blockchain in Logistics and Supply Chain: A Lean approach for designing real-world use cases. *IEEE Access* **2018**, *6*, 62018–62028. [CrossRef]
103. Woodside, J.M.; Augustine, F.K., Jr.; Giberson, W. Blockchain Technology adoption status and strategies. *J. Int. Technol. Inf. Manag.* **2017**, *26*, 65–93.
104. Preuveneers, D.; Joosen, W.; Ilie-Zudor, E. Trustworthy data-driven networked production for customer-centric plants. *Ind. Manag. Data Syst.* **2017**, *117*, 2305–2324. [CrossRef]
105. Carson, B.; Romanelli, G.; Walsh, P.; Zhumaev, A. *Blockchain beyond the Hype: What Is the Strategic Business Value?* Mckinsey Co.: New York, NY, USA, 2018.
106. Toyoda, K.; Takis Mathiopoulos, P.; Sasase, I.; Ohtsuki, T. A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain. *IEEE Access* **2017**, *5*, 17465–17477. [CrossRef]

107. Chronicled Our Mission is to Create the World's Most Trusted IoT Ecosystem. Available online: http://chronicledtest.net/platform.html (accessed on 20 May 2019).
108. Casino, F.; Azpilicueta, L.; Lopez-Iturri, P.; Aguirre, E.; Falcone, F.; Solanas, A. Optimized wireless channel characterization in large complex environments by hybrid ray launching-collaborative filtering approach. *IEEE Antennas Wirel. Propag. Lett.* **2016**, *16*, 780–783. [CrossRef]
109. Ma, M.; Shi, G.; Li, F. Privacy-Oriented Blockchain-Based Distributed Key Management Architecture for Hierarchical Access Control in the IoT Scenario. *IEEE Access* **2019**, *7*, 34045–34059. [CrossRef]
110. Malik, S.; Kanhere, S.S.; Jurdak, R. ProductChain: Scalable Blockchain Framework to Support Provenance in Supply Chains. In Proceedings of the 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 1–3 November 2018; pp. 1–10.
111. Maroufi, M.; Abdolee, R.; Tazekand, B.M. On the Convergence of Blockchain and Internet of Things (IoT) Technologies. *arXiv* **2019**, arXiv:190401936.
112. Szabo, N. Smart Contracts. Available online: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (accessed on 20 May 2019).
113. GS1 UK; The Institute for Grocery Distribution; Cranfield School of Management (KTP Project). Value Chain Vision. In *Data Crunch Report: The Impact of Bad Data on Profits and Customer Service in the UK Grocery Industry*; GS1 UK & Cranfield School of Management: London & Bedford, UK, 2009; Available online: https://dspace.lib.cranfield.ac.uk/bitstream/handle/1826/4135/Data_crunch_report.pdf?sequence=1&isAllowed=y (accessed on 25 May 2019).
114. Lumb, R.; Treat, D.; Jelf, O. Editing the Uneditable Blockchain—Why Distributed Ledger Technology must Adapt to an Imperfect World. Available online: https://newsroom.accenture.com/content/1101/files/Cross-FSBC (accessed on 30 March 2019).
115. Mao, D.; Hao, Z.; Wang, F.; Li, H. Novel Automatic Food Exchange System Using Consortium Blockchain. *Arab. J. Sci. Eng.* **2019**, *44*, 3439–3455. [CrossRef]
116. Zeto Accelerating Blockchain for the Supply Chain. Available online: https://www.zetochain.com/ (accessed on 3 November 2018).
117. Kamilaris, A.; Fonts, A.; Prenafeta Boldu, F.X. *The Rise of the Blockchain Technology in Agriculture and Food Supply Chain*; ICT Update, CTA: Wageningen, The Netherlands; 2018; Available online: https://cgspace.cgiar.org/bitstream/handle/10568/97525/ICTUpdate_88EN.pdf?sequence=1&isAllowed=y (accessed on 25 May 2019).
118. Turk, Ž.; Klinc, R. Potentials of Blockchain Technology for Construction Management. In Proceedings of the Procedia Engineering, Primosten, Croatia, 19–22 June 2017; Volume 196, pp. 638–645.
119. Miller, D. Blockchain and the internet of things in the industrial sector. *It Prof.* **2018**, *20*, 15–18. [CrossRef]
120. Dogo, E.M.; Salami, A.F.; Aigbavboa, C.O.; Nkonyana, T. Taking Cloud Computing to the Extreme Edge: A Review of Mist Computing for Smart Cities and Industry 4.0 in Africa. In *Edge Computing*; Springer: Cham, Switzerland; 2019; pp. 107–132.
121. Ambrosus. Available online: https://ambrosus.com/#mission (accessed on 16 March 2019).
122. Moon, J. *Evrythng Opens Blockchain to Every Consumer Product Brand*. 2019. Available online: https://evrythng.com/press-releases/evrythng-opens-Blockchain-to-every-consumer-product-brand/ (accessed on 25 May 2019).
123. OriginTrail OriginTrail. Available online: https://origintrail.io/ (accessed on 9 January 2019).
124. Dobrovnik, M.; Herold, D.; Fürst, E.; Kummer, S. Blockchain for and in Logistics: What to Adopt and Where to Start. *Logistics* **2018**, *2*, 18. [CrossRef]
125. Ramachandran, A.; Kantarcioglu, D. Using Blockchain and smart contracts for secure data provenance management. *arXiv* **2017**, arXiv:170910000.
126. Shetty, S.; Red, V.; Kamhoua, C.; Kwiat, K.; Njilla, L. Data provenance assurance in the cloud using Blockchain. In Proceedings of the Disruptive Technologies in Sensors and Sensor Systems, Anaheim, CA, USA, 11–12 April 2017.
127. Aryal, A.; Liao, Y.; Nattuthurai, P.; Li, B. The emerging big data analytics and IoT in supply chain management: A systematic review. *Supply Chain Manag. Int. J.* **2018**. [CrossRef]
128. McConaghy, T. Blockchains for Big Data. Available online: https://bravenewcoin.com/insights/Blockchains-for-big-data (accessed on 21 May 2019).
129. Mišura, K.; Žagar, M. Data marketplace for Internet of Things. In Proceedings of the 2016 International Conference on Smart Systems and Technologies (SST), Osijek, Croatia, 12–14 October 2016; pp. 255–260.

130. Abeyratne, S.A.; Monfared, R.P. Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger. *Int. J. Res. Eng. Technol.* **2016**, *5*, 1–10.
131. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and IoT integration: A systematic survey. *Sensors* **2018**, *18*, 2575. [CrossRef]
132. Brous, P.; Janssen, M.; Herder, P. Internet of Things adoption for reconfiguring decision-making processes in asset management. *Bus. Process Manag. J.* **2018**. [CrossRef]
133. Goguen, M.; Campbell-Verduyn, M. The mutual constitution of technology and global governance: Bitcoin, Blockchains, and the international anti-money-laundering regime. In *Bitcoin and Beyond*; Routledge: London, UK, 2017; pp. 69–87.
134. Levi, S.D.; Lipton, A.B. An introduction to Smart Contracts and Their Potential and Inherent Limitations. In *Harvard Law School Forum on Corporate Governance & Financial Regulation*. 2018. Available online: https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/ (accessed on 14 June 2019).
135. Dib, O.; Brousmiche, K.-L.; Durand, A.; Thea, E.; Hamida, E.B. Consortium Blockchains: Overview, applications and challenges. *Int. J. Adv. Telecommun.* **2018**, *11*, 51–64. Available online: https://www.researchgate.net/profile/Omar_Dib/publication/328887130_Consortium_Blockchains_Overview_Applications_and_Challenges/links/5be99602299bf1124fce0ab9/Consortium-Blockchains-Overview-Applications-and-Challenges.pdf (accessed on 25 May 2019).
136. Ganne, E. *Can Blockchain Revolutionize International Trade?* World Trade Organization: Geneva, Switzerland, 2018.
137. Müllner, J.; Filatotchev, I. The Changing Face of International Business in the Information Age. In *International Business in the Information and Digital Age*; Emerald Publishing Limited: Bingley, UK, 2018; pp. 91–121.
138. Rose, K.; Eldridge, S.; Chapin, L. The internet of things: An overview. *Internet Soc. ISOC* **2015**, *80*, 1–50.
139. Weber, R.H. Internet of Things–New security and privacy challenges. *Comput. Law Secur. Rev.* **2010**, *26*, 23–30. [CrossRef]
140. Weber, R.H. Internet of things—Governance quo vadis? *Comput. Law Secur. Rev.* **2013**, *29*, 341–347. [CrossRef]
141. Vermesan, O.; Friess, P. *Building the Hyperconnected Society: Internet of Things Research and Innovation Value Chains, Ecosystems and Markets*; River Publishers: Aalborg, Denmark, 2015; Volume 43.
142. Wu, D.; Arkhipov, D.I.; Asmare, E.; Qin, Z.; McCann, J.A. UbiFlow: Mobility management in urban-scale software defined IoT. In Proceedings of the 2015 IEEE Conference on Computer Communications (INFOCOM), Kowloon, Hong Kong, 26 April–1 May 2015; pp. 208–216.
143. De Filippi, P.; Wright, A. *Blockchain and the Law: The Rule of Code*; Harvard University Press: Cambridge, MA, USA, 2018.