logistics

Article

Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment

Antonios Litke [1,*], Dimosthenis Anagnostopoulos [2] and Theodora Varvarigou [1]

[1] Electrical and Computer Engineering school, National Technical University of Athens, 157 73 Athens, Greece; dora@telecom.ntua.gr
[2] Department of Informatics and Telematics, Harokopio University of Athens, 176 76 Athens, Greece; dimosthe@hua.gr
* Correspondence: litke@mail.ntua.gr; Tel.: +30-210-772-2568

Received: 19 November 2018; Accepted: 16 January 2019; Published: 18 January 2019

Abstract: Blockchains are attracting the attention of stakeholders in many industrial domains, including the logistics and supply chain industries. Blockchain technology can effectively contribute in recording every single asset throughout its flow on the supply chain, contribute in tracking orders, receipts, and payments, while track digital assets such as warranties and licenses in a unified and transparent way. The paper provides, through its methodology, a detailed analysis of the blockchain fit in the supply chain industry. It defines the specific elements of blockchain that affect supply chain such as scalability, performance, consensus mechanism, privacy considerations, location proof and cost, and details on the impact that blockchains will have in disrupting the supply chain industry. Discussing the tradeoff between consensus cost, throughput and validation time it proceeds with a suggested high-level architectural approach, and concludes as a result with a discussion on changes needed and challenges faced for an in-vivo deployment of blockchains in the supply chain industry. While the technological features of modern blockchains can effectively facilitate supply chain uses cases, the various challenges that still remain, bring in front of us a wide set of needed changes and further research efforts for achieving a global, production level blockchain for the supply chain industry.

Keywords: Blockchains; supply chain management; distributed ledgers; consensus

---

1. Introduction

Blockchains are regarded as public (and lately also private) ledgers containing transactional data within their decentralized data structures, which form a series of tightly connected blocks. Asymmetric cryptography and distributed consensus algorithms are being deployed for achieving ledger consistency, data integrity, auditability, non-repudiation, and authentication as part of the basic security primitives [1]. The distributed and decentralized nature of blockchains makes them immutable in the sense that transactions cannot be tampered once they are officially validated by the peers of the network and registered in the block of the chain. At the same time, reliability and robustness are ingredients that constitute blockchains as highly trusted platforms implemented on open, trustless networks of peers.

During the last years, we experience significant research and development efforts utilizing blockchains in financial services such as digital assets and payment systems [1,2], smart contracts [3], logistics [4] Internet of Things (IoT) [5,6], and reputation systems [7,8]. This is mainly due to the fact that blockchains can allow transactions and payments to be implemented without any intermediary, thus effectively disrupting the way traditional businesses are working to date.

Logistics and supply chain management are regarded as domains where blockchains are good fits for a series of reasons. During the lifecycle of the product, as it flows in the value chain (from the production to consumption) the data generated in every step can be documented as a transaction creating, and thus, a permanent history of the product. Among others, blockchain technology can effectively contribute to: (i) Recording every single asset (from product to containers) as it flows through the supply chain nodes, (ii) tracking orders, receipts, invoices, payments, and any other official document, and (iii) track digital assets (such as warranties, certifications, copyrights, licenses, serial numbers, bar codes) in a unified way and in parallel with physical assets, and others. Moreover, the blockchain can contribute effectively, through its decentralized nature, in sharing information about the production process, delivery, maintenance, and wear-off of products between suppliers and vendors, bringing new modalities of collaboration in complex assembly lines.

Any system, in order to achieve traceability, is required for a flow of information that records and follows the flow of products. The interconnected structure of the supply chain makes it difficult to introduce a centralized system in control of a third party, since a high level of trust is required. The limited amount of trust concludes in separate systems that restrain the possibility to accomplish traceability throughout the full supply chain. In today's world, supply chains end up to be complicated structures with multiple involved participants and with a plethora of activities. Security and organizational issues tend to enhance the need to build a supply chain management system leveraging blockchain ledger technology.

Regardless of the particularities of the specific supply chain related application, blockchain can offer a wide set of advantages. By registering and documenting a product's lifecycle across the supply chain nodes increases the transparency and the trust of the participating actors. Moreover, elimination needs to have a trusted third party that can allow for greater scalability, as any number of participants can virtually participate in the chain with the appropriate level of trust, and increased innovation by deploying the dynamics of blockchains as enablers of instant payments (through cryptocurrency), smart contracts, and low transaction fees without having the cost overheads of third parties. Last, but not least, a shared, immutable ledger with codified rules can potentially eliminate the audits required by internal systems and processes.

While today we experience various research efforts on the analysis of the blockchains in logistics and supply chain management and the adoption of distributed ledger technologies and smart contracts, there has been no detailed methodological approach on what elements of the blockchain are effecting the particular stakeholders and what are the blockchain technical features that someone has to pay special attention to for the wider real-life blockchain adoption in the related business domain. At the same time, some high level conceptual considerations on a blockchain based architecture for the supply chain management is missing and needs to be the subject of further discussions so as to have a reference blueprint for a potential further articulation with the legacy systems owned by the related supply chain stakeholders.

The remaining paper is structured as follows: Section 2 provides an analysis on related work with respect to supply chain management over blockchain technology and investigates, among others, recent literature and implementations that try to utilize such technologies in the area of logistics, product origin tracking, and supply chain management. Section 3 discusses the general concept and elements of blockchains that affect the supply chain and its actors. Scalability, performance, consensus mechanisms, privacy, location, and cost are further investigated, while an analysis of blockchain features tradeoffs for supply chain is being presented. Section 4 provides architectural assumptions and considerations for a generic modular and layered architecture and how blockchain layer and a generic middleware layer have to be placed and interact with each other for facilitating the needs of supply management actors. Section 5 provides a discussion on current findings, challenges that blockchains imply, and possible solutions that may be engineered for achieving a global scale blockchain adoption for the supply chain and logistics industry. Section 6 provides the final conclusions of the paper.

2. Review of Literature

Blockchain technology has been successfully used in several industries, such as energy and finance. For the supply chain, solutions have been proposed in a theoretical manner without significant results in real-world conditions. In particular, recent literature studies have various aspects of the specific domain. In Reference [9], the authors identify characteristic use cases described for blockchain in the field of logistics and supply chain management and analyze them regarding their mindful technology use based on five mindful technology adoption principles: Engagement with the technology; technological novelty seeking; awareness of local context; cognizance of alternative technologies; and anticipation of technology alteration. Most cases demonstrate high engagement with the technology, but there are significant differences when it comes to the other mindful use principles. In Reference [10], the authors use the methodology 'attributes of innovation framework' to identify the potential blockchain applications and present a framework explicating four transformation phases to subsequently categorize the identified areas of application according to their effects on organizational structures and processes. Using academic and practitioner literature, the authors classify possible applications for adoption and provide a framework to identify blockchain opportunities in the logistics industry. Such research studies can be particularly beneficial for high level business executives to assess where to start building organizational capabilities in order to successfully adopt and deploy blockchain technology.

A fully transparent and decentralized traceability system for the supply chain is proposed in another paper called TRADE [4], which displays that it is feasible to apply blockchain technology for the supply chain to obtain traceability. Consumers and other participants can view all the system information and verify the product assertions derived from actors. The authors focus on the trust aspect and a transparent, decentralized traceability system for the supply chain. Each role (actor) creates a transaction according to a product identifier (pid) that consists of the full product data. A role signs the transactions they issue (digital signature—providing non-repudiation, authenticity, integrity). All the legitimate transactions are combined in a block and are broadcasted to the blockchain network. End users are allowed to view the full life cycle of a product. Uniformity is enforced in TRADE because each transaction, depending on the corresponding actor, has an appropriate series of validation processes. In this study, various open research questions for specific use cases are expressed, including, among others, privacy. For certain supply chains, roles might compete with each other and not approve the use of a transparent system, consequently, a privacy-preserving traceability system should be designed.

In 2016, Kim et al. presented a smart contract design based on ontologies of an incepted traceability supply chain system using blockchain technology. In this work, emphasis is given on the appliance of ontologies in their context, rather than on blockchain technology for the supply chain in the real-world [7]. RFID tags and blockchain technology is deployed in order to create a traceability system for an agri-food supply chain in China. Authors claim that a decentralized suggestion for traceability could solve the problems in an approach that is centralized, particularly: Trust, fraud, corruption, tampering, and falsifying information. While this analysis examines blockchain technology and traceability as separate features, their combination might present flaws concerning feasibility and performance [11].

Abeyratne et al. presented a deep dive in traceability and transparency [1]. In their work, transparency is discussed based on the child labor scandal of Nike (1996), whereas freight sustainability is built with an emphasis on the product life-cycle [2,3]. While Abeyratne et al. support that the blockchain technology attributes can enhance trust through traceability and transparency in supply chain use cases, their work discusses an example, rather than a practical application of blockchain technology in the supply chain.

The applicability of blockchain technology in the Internet of Things sector is examined in Reference [12]. Scalability and high costs issues of the IoT sensor networks are mentioned and blockchain is suggested as a solution. Advantages that come from the connection of IoT sensors to the blockchain include, among others, the access to a convenient (existing) billing layer, which paves the way for a marketplace of data sharing and services between devices. According to this study, there are various limitations and issues still to be resolved. One issue is that a blockchain solution will generally underperform, resulting in lower transaction processing throughput and higher latencies, compared to a centralized database solution. Another issue that may come up concerns privacy on the blockchain, since blockchains by design expose information to everyone.

The ZERV Commerce Platform [13], enabled by an asset-based token and blockchain technology, plans to be a decentralized trading platform. It intends to allow for frictionless transactions between all key participants within the defense industry, including manufacturers, suppliers, distributors, retailers, and consumers. However, as of today, there is still no white paper describing any of the implementation details of their suggested approach. 300Cubits [14] aims at revolutionizing the shipping business by tokenizing the contract between customer and container liner. As a solution to this supply chain issue, 300Cubits proposes a token deposit system, which is organized as a tamper-proof Blockchain intermediary and utilizes a smart contract. Bext360 [15] is an organization focused on developing technologies to improve social sustainability in a supply chain. For that purpose, they developed a blockchain to track and trace coffee beans on the complete route from farmer to consumer. IBM and Walmart have developed and started testing a solution for a more efficient data exchange, which is based on blockchain technology and enables them to identify and track products faster (from six days to 2 s) and to remove recalled goods from their shelves [16]. The solution requires data input for every product into a private blockchain.

Last but not least, an ongoing discussion is taking place besides the technical aspects of supply chain management (whether fueled by blockchain or not), which has to do with other societal goals. The articulation between supply chain and ethics (as for example the discussion in Reference [17]) is something that is receiving significant attention in modern business ethics and where blockchains can contribute through the traceability of the products and the means of manufacturing.

3. General Concept

3.1. Conceptual Diagram

By definition, supply chain management constitutes the management of goods and services progress path, including the transfer and deposit of natural resources (raw materials), of ongoing processes backlog and of completed products from genesis to use. Supply chain logistics involve the design, planning, execution, control, and monitoring of goods and services journey activities adding value to the final product. Eventually built on intercommunication business networks, supply chains manage to provide the final product to the consumers through a series of actions, such as raw material extraction, manufacturing to build the product, distributing the product to middle-men (wholesalers, retailers), and allocating the product to the public. These kinds of activities are conveniently assumed in our solution as transactions of a blockchain network and the participants of the supply chain interact with each other through this network. Below are the different actors of a supply chain that are described briefly in order to give a typical perspective.

To begin with, the starting point of a supply chain is constituted from the extraction of raw materials (natural resources) and how they are firstly processed (pre-processed) by the suppliers or vendors in order to be delivered to the next stage. The next stage is called manufacturing where the process of converting the raw materials into products that are ready to sell takes place. Following this, the constructed products are passed to the distributors who are responsible for allocating them to multiple different intermediaries, such as wholesalers and retailers. The distributors also maintain an active inventory of the products since the prior are connected with the suppliers. Subsequently, the wholesalers do not sell products directly to the public, but to other retailers instead, whereas the retailers dispose the purchased products to end users. Lastly, the consumers are the ones who purchase or receive goods or services for personal needs or use and not for business purposes of resale or trade. Below is a figure combining blockchain technology with supply chain functionalities, which is described and analyzed.

Figure 1 illustrates, conceptually, how the different actors of a supply chain can cooperate and interact under a blockchain network. Each participant submits transactions on the blockchain network in a specific way, depending on the completed activity. In the raw materials step, the suppliers that pre-process the natural resources are submitting transactions on the ledger concerning that initial process. These transactions include tags such as raw material name, quantity, quality, origin geo-location, and others. The moment the raw materials are starting their journey to manufacturer, the appropriate transactions are submitted. In this manner, every network party can verify important details about the specific raw material they have received or that their product is made from. Similarly, on the manufacturing stage, the manufacturer has a similar interaction with the blockchain and the next chain participant.

Figure 1. Supply Chain Roles (Actors) interacting with Blockchain Distributed Ledger Technology.

The manufacturer is able to validate crucial information about the natural resources they collected by reading and verifying all the tags the latter includes in their transactions, and then, proceed to the proper execution of the manufacturing step. New transactions with new information tags, such as manufacturer name, field experience and others, are submitted after the completion of the stage. Following this, the products are handed to the distributors. The distributors manage to sell the products to wholesalers and retailers. This process is represented by blockchain transactions that display important data tags, such as the merchant and customer address, exchange amount, product raw material quality, and others. The distributors task is defined as to sell products to middle-men, which means not end user. At this point, as in every step of the supply chain, the distributor (generally every stage party) can check valuable tag information about the product progress route until that stage; information such as the raw material origin geolocation, the manufacturer company popularity, the distributor name, and others. For instance, a retailer can audit the product's natural resource quality right away and get the appropriate feedback before selling it to the consumer. Subsequently, when a distributor delivers the product to a wholesaler by submitting a corresponding transaction, the latter acts in a similar way. They check the transaction tags for extra data and then execute their selling to the next wholesaler or retailer company and submit a new transaction. The same applies to the retailer organizations. Lastly, the end user receives the final product followed by a submitted transaction (with appropriate tags included) and is able to check and verify its every aspect from the beginning of its supply chain journey until that moment. The following table (Table 1) gives an overview of the current limitations supply chain actors face and what is the positive impact introduced through blockchain adoption.

Table 1. Supply Chain actors, current limitations faced and blockchain impact.

Supply chain actor	Current limitations	Blockchain impact
Raw material/Producer	Ability to prove in a global and transparent way the origin and quality metrics of products.	Benefits from increased trust of keep track of the production raw material and value chain from the raw material to the end consumer.
Manufacturer	Limited ability to monitor the product to the final destination. Limited capabilities of checking quality measured from raw material.	Added value from shared information system with raw material suppliers and distribution networks.
Distributor	Custom tracking systems with poor collaboration capabilities. Limited certification ability and trust issues.	Ability to have proof-of-location and conditions certifications registered in the ledger.
Wholesaler	Lack of trust and certification of the products' path.	Ability to check the origin of the goods and the transformation/transportation conditions.
Retailer	Lack of trust and certification of the products' path.	Track of each individual product between the end consumer and the wholesaler. Ability to handle effectively return of malfunctioning products.
End user/Consumer	Lack of trust regarding the compliance of the product with respect to origin, quality and compliance of the product to the specified standards and origin.	Full and transparent view on the product origin and its whole journey from raw material to final, purchased product.

3.2. Elements of Blockchains that Affect Supply Chain

Supply chains typically raise various issues that are highly dependent on freight failure, human error, intended fraud, and others, thus security is one of the cornerstone aspects that have to be addressed. In a supply chain, all circulated data happens to obtain different forms and ought to satisfy different needs that both lead to a much more demanding and complex course of controlling and ensuring immutability and secure transparency between transactions and their data, without even such guarantee most of the times. For instance, a malicious party that participates in the supply chain could tamper invoice information and alter paid or due values illegitimately. Thus, it is crucial to endorse a mechanism that enhances immutability and assures transaction confidentiality in supply chain use cases. Blockchain technology provides a decent solution to the security problems presented along the supply chain and guarantees integrity control and transparency of the products and their content. In the following subsections, different elements of blockchain technology that affect, explicitly or implicitly, the supply chain are presented and analyzed.

3.2.1. Scalability

A very large number of stakeholders are participating in modern supply chains, which are of global range, together with a massive flow of newly created and time sensitive information. All this data is poorly handled by modern supply chain management systems since there does not exist in any shared common database. Blockchain can contribute significantly in scaling up by providing a networked and decentralized database in order for all supply chain parties to join. In this manner, any single point of failure disappears while, at the same time, all supply chain data is recorded on a ledger, shared among all participating network peers. For instance, when different parties of the supply chain flow need to intercommunicate or learn information for one another, the blockchain ledger offers such a procedure on a global scale with ease.

3.2.2. Performance

Various actions and procedures occur during a product's or freight's journey inside the supply chain. They are often prone to human errors or even fraud or ware failure, which as a result, diminish system performance. With blockchain, the majority of activities can be represented as electronic transactions submitted on the ledger. In that case, they execute faster and without errors increasing system performance. For instance, a smart contract can automatically pay custom parties the correct amount when triggered in a few minutes independently of their geo-location. Moreover, processes such as ensuring data validity and integrity or confidentiality last a significant amount of time in traditional supply chain systems, whereas blockchain can provide these attributes as built-in. For example, digital signatures of a recipient party are automatically checked and verified along a freight's journey, lightening a system's workload, though improving performance limits.

3.2.3. Consensus

Blockchain platforms possess a specific mechanism that ensures data immutability along the ledger called consensus. The particular scope of the consensus is to keep a general agreement between the nodes of the network about all submitted transactions information. Such transaction information can be the timestamp, thus the order they occurred, the addresses of sender and of receiver, the amount transacted, the tags or electronic seal that accompany the ware and others. The essence of blockchain technology innovation and uniqueness originates from the use of consensus mechanisms. Today, blockchain platforms support different types of general agreement tools depending on the ledger level of access. A ledger can be public or private and typical consensus algorithms constitute proof-of-work and proof-of-stake, practical byzantine fault tolerance and proof of elapsed time, or proof of authority matched, respectively. Apparently, there exists no common tool on modern supply chains that organizes and secures each step of the product, hence errors, fraud, and ware failure are possible. Consensus algorithms constitute the core of the blockchain trust and node general agreement, with well-known methods known as "mining". On the contrary, such techniques hide dangers, such as 51% attack [18] and reveal problems such as selfish mining [19].

3.2.4. Privacy

In contradiction with the modern supply chains where any kind of data is available and can be tampered, blockchains offer a powerful contribution when it comes to privacy. Blockchain ledgers not only contain immutable information, but at the same time, users' privacy is highly respected. Public blockchains offers pseudonymity to its users in the sense that each user is able to interact with the ledger through a newly created address without revealing their real identity. Furthermore, permissioned and private blockchains can provide total anonymity inside the network in the following way. Inside a consortium or private blockchain, it is possible that parties are joining in an anonymized way while being authenticated in advance by an off-chain system of the supply chain. In this manner, the supply chain works properly, while their real identity is a safely kept secret from the other parties of the network and it is assured that they are legal participants.

3.2.5. Location

Blockchain technology offers all its functionalities and attributes independently of the geo-location of its users. Since the offered decentralized network can be shared over the Internet, any legal party of a supply chain can contribute to a freight's lifecycle from anywhere. Thus, a supply chain network enhanced with blockchain technology can be even broader globally than a traditional one, since stakeholders and companies from inconvenient-to-do-business parts of the globe could participate and offer their services or purchase wares. The most important effect that flexibility of location, offered by blockchain technology, can have on the supply chain is obviously the time efficiency. For example, when bank transacting happens between distant parts of the world, payment mobility becomes much slower—it could even take months, depending always on the laws and the interrelationships of the countries. On the contrary, when transacting happens with cryptocurrency through a global blockchain network, the transaction confirmation and the payment completion is reduced to minutes.

3.2.6. Cost

In a like manner with location, cost is significantly reduced with blockchain technology in a supply chain system. Mainly due to large distance transactions being slower through banks than with cryptocurrency technology, blockchain provides an economic solution for the supply chain. Additionally, since most activities can be represented as transactions, the entire workflow of the supply chain can be substantially faster than the traditional case. For instance, the whole blockchain network can be aware in a matter of minutes that the raw material extraction is completed, and thus, the next step is in its infancy, since the extraction will be submitted as a transaction on the shared ledger. An overview of the blockchain elements that affect supply chain logistics along with the scope of their roles is presented in Table 2.

Table 2. Blockchain Elements that affect Supply Chain Logistics with Roles Scope.

	Relation and impact to the Supply Chain roles
Scalability	Scalability is improved since the suppliers are participating in a general system of the supply chain (not different ones depending on the different companies as in traditional supply chain architecture). The Peer-to-Peer nature of blockchains is by design more robust and scalable given the fact that the there is no single point of interaction (as compared to centralized solutions). Distributors scalability is improved since in a common ledger all their customers (wholesalers, retailers) can be effortlessly accessed (no need for different supply chains for different customers). Blockchain scalability improves consumers experience since they are more aware of the supply chain size and functionalities through transaction tag information and their trust towards the system increases.
Performance	Blockchain performance enhances this step since transaction submission and verification high speed (comparing to traditional bank methods) provides quick and trustful liquidity of payments. Recent blockchain implementations are being designed as to facilitate a high throughput of transactions per second.
Consensus	Blockchain consensus offers trust to the whole supply chain system. Country origin, quality and other details are recorded as tags on the ledger, adding value to the final product. It benefits the Distributors stage since the raw materials are validated and the manufacturer signature is checked, which all together add value to the final product. It also helps vitally this stage since the retailers are assured that the final product which is about to be sold to the end users has all the exact natural resources and passed through all the manufacturers, distributors and wholesalers that the ledger confirms. Consumers are confident that the product quality and general characteristics are the ones that the blockchain ledger confirms they are; value is added to the product.
Privacy	Although blockchains are considered public ledger, privacy can be engineered in a way to facilitate access control to who is going to have access to the information contained in the blocks. Blockchain provides privacy in the sense that private transactions are not visible (but are legitimately verified) by parties that transaction issuers might not want to display. It also helps keep identity of users private when it is needed, but still verifying values that are essential for the consistency of a products journey, such as raw material quality, distributor geolocation and others.
Location	Supply chain dependency on location becomes flexible. Raw materials are transferred around the world while transactions are not dependent on country regulations and laws; with rapid submission and validation rates. Manufacturers are cooperating with different supplier and distribution companies around the world while transactions are country regulation and law independent with rapid submission and validation rates. Distributors are cooperating with different wholesale and retail companies around the world while transactions do not depend on country regulations and laws and are accomplished with rapid submission and validation rates. Additional measures and methods for proof-of-location mechanisms are being considered these days as a way to prove the location through its registration to a blockchain that cannot be disputed.
Cost	Blockchain transaction costs can be significantly reduced comparing to traditional payments with banks. In contrast with banks, crypto-payment fees are negligible, especially when transferring funds between countries with different regulations and economy laws. Suppliers are paid faster for the natural resources that the sell to manufacturers, while the later are charged subtly on their purchase. Distributors are compensated quicker for their offered products, while the wholesalers or retailers benefit from the low fees. The final product overall value is increased while at the same time its price is substantially decreased which both leave the consumer happier than in the traditional supply chain system in terms of quality and price.

3.3. Blockchain Features Tradeoffs in Supply Chain Management

When it comes to a preliminary analysis on the production level public blockchains that can potentially form the basis for real world deployment for supply chain facilitation, the core analysis is focused on the tradeoff between the consensus mechanism, bandwidth (Transactions Per Second, TPS), and validation speed (Transaction Confirmation Time, TCT). While such characteristics have not been validated in all blockchains and for a global commercial oriented deployment, there are many research studies that have tackled this issue even within the literature approach [20].

As of today, there have been proposed many distributed consensus protocols which function on top of the blockchain data structure. Proof-Of-Work (PoW) consensus protocol is based on the solution of an extremely difficult cryptographic puzzle in order for the nodes to compete and eventually to come to an agreement as far as the new block is concerned. This type of consensus method is regarded as having high trust, but comes with the energy consumption overhead as it requires very high computational power from the nodes and nowadays it also requires expensive dedicated hardware based on Application Specific Integrated Circuits (ASIC). The Proof Of Stake (PoS) consensus protocol suggests that the new block's publication should be based on how much stake each peer has stored in the network. Such consensus methods are definitely less expensive than the PoW, however, it comes with other weaknesses such as the "Nothing at Stake" problem. Other alternative consensus mechanisms such as the Practical Byzantine Fault Tolerance (PBFT), functions efficiently on top of permissioned blockchains like Hyperledger Fabric. PBFT works on the assumption that less than one-third of the peers are faulty (f), which means that the network should consist of at least n=3f+1 peers to tolerate f faulty peers. Eventually, the network requires 2f+1 peers to agree on the block of the transactions. Such approaches are commonly referred to as federated consensus mechanisms and can be regarded as voting methods where peers vote through random and transparent processes on which the block is the next to be confirmed to be added on the chain.

Permissionless blockchains [34] do not require pre-established identities or any identity management from a third party and are thus fully decentralized as anyone can join the peer-to-peer network and run a full node, while permissioned blockchains [35] enables a third-party to identity management in order for a user to be part of the blockchain network. It has to be noted that Table 3 contains public, permissionless blockchains based on the assumption that a global scale supply management blockchain would require such an approach. Alternative, cross-organizational and consortium based blockchains (permissioned) could be deployed to overcome performance limitations. For instance, Quorum, as an enterprise flavor of Ethereum, has reported dozens to hundreds of transactions per second (TPS) depending on the configuration of the transactions, while Hyperledger Fabric has likewise reported figures as high as 3500 TPS, which most likely include transactions occurring and concluding across the entire network.

Table 3. Comparison of blockchain performance characteristics and assessment of suitability for supply chain management (at the time of writing this paper).

Blockchain Name	Consensus Protocol	Transactions per Second (TPS)	Transaction Confirmation Time (TCT)	Supply Chain Suitability
Bitcoin (BTC) [21]	PoW	3–7	25 min	Expensive, low bandwidth (TPS), high TCT.
Ethereum (ETH) [22]	PoW	15–20	2 min	Expensive with viable, for commercial deployment TCT
Ripple (XRP) [23]	RCPA	1.500	4 s	High bandwidth, low cost and high TCT
Bitcoin Cash (BCH) [24]	PoW	60	60 min	Expensive and not suitable for real-time
Litecoin (LTC) [25]	PoW	56	30 min	Expensive, not well suited for real-time
EOS(EOS) [26]	DPoS [27]	millions	6 min	Inexpensive, high throughput, low TCT
Cardano (ADA) [28]	PoS	5–7	3–5 min	Inexpensive, moderate throughput, low TCT
Stellar (XLM) [29]	PoS	1000	2–5 s	Inexpensive, high throughput, low TCT
NEO (NEO) [30]	DBFT	10.000	15–20 s	Inexpensive, high throughput, low TCT
Monero (XMR) [31]	DAG(Tangle)	4	30 min	Inexpensive, low TPS, low TCT
Tether (USDT) [32]	Various Consensus mechanisms	Ethereum-based token	15–30 s	Inexpensive with moderate TPS and low TCT.
NEM (XEM) [33]	PoI	4000	1–2 min	Inexpensive with moderate TPS and low TCT.

Blockchain protocols are commonly engineered as a tradeoff among consensus cost, speed, bandwidth, and security (including trust). This three-way tradeoff, however, is not inherent in decentralized cryptocurrencies. While there are some efforts such as the GHOST protocol [36] that demonstrate that fairness and mining power utilization can be improved by changing the chain selection rule, in particular, by being inclusive to forks outside the main chain as well, it tends to be that not many degrees of freedom are available in public decentralized ledger technologies.

4. Suggested Architecture and Blockchain Approach

4.1. Overview and Assumptions

Due to the high number of stakeholders involved in large scale supply chains of global range, the relationships between them end up to be complex. Modern supply chain management carries many trust-based concerns that constitute the main cause why a blockchain solution is essential and seems mandatory. First of all, there exists a lack of trust among the participants of a supply chain. Every party needs to trust that true data is issued and exchanged by another party in their intercommunication. Unfortunately, this does not occur in contemporary supply chains where freight failure, human error, or intended fraud prospers. Furthermore, it is essential that such systems need to effectively gather valid data, record it securely and provide exact information to several other systems. Failures on these processes occur frequently and, as a result, a global end-to-end supply chain system depends highly on its fragile links that slow down, alter or impede information flow. In addition, lack of both high standards and end-to-end integration leads to information inconsistency among stakeholders. Each party needs to collect and confirm the data validity in order to ensure integrity and effectiveness that decreases system performance. Additionally, limitations on the efficient information flow manipulation exist due to the current supply chain system structure. Due to the complex architecture, the system is additionally changed with hard tasks such as product traceability and monitoring that crucially impair performance and efficiency. For example, tracking the complete system starting from raw material extraction to factory-produced ware ready to be purchased has become a significantly complex procedure in modern supply chains.

Supply chains will benefit from blockchain innovative science through numerous ways. Blockchain will essentially contribute to transparency and auditability that will support large extent freight conditions violations and human error and fraud detection (the cost of global fraud was evidenced in a report by PwC [37], where it is indicated that 49% of organizations globally said they have been a victim of fraud and economic crime). Product conditions will be controlled and reported on the ledger when they overcome the proper thresholds, as well as any human error that could damage the goods of the chain's procedures. In order to reduce reputation risks, human rights, and conduct codes will be respected along the chain by being recorded on the ledger. Intended fraud will be detected and reported on the blockchain as a transaction as well, while notifications and messages could be broadcasted inside the blockchain network in order to inform other parties about the participant that tried to commit fraud. Additionally, blockchain will provide continuity of information through its well-known properties of immutability and irrevocability. Secure sharing of data between different stakeholders that participate in a global supply chain will be essential in order to guarantee freight traceability and reduce the risk of errors or frauds and will easily be implemented inside a public or permissioned blockchain network that ensures trustless party intercommunication and tamperproof data. Further, properly authorized accessibility to information will be achieved with important benefits for future references. Agile and transparent blockchains will offer access to ledger data retrospectively in order to benefit from the massive volume of the information produced.

4.2. Blockchain Ledger Layer

The Blockchain Layer of the architecture describes its core low-level blockchain network functionalities. The modules that constitute this layer are mainly for achieving consensus among the peers and manage the transactions that are going to be registered in the ledger.

The Consensus Module confirms data authenticity and the proper execution of operations inside the blockchain network. It is responsible for transactions validation and verification and the overall agreement on current ledger state among different nodes that participate in the blockchain network. This module is directly connected with the Transactions Handling module of the Blockchain Layer and they all together form the blockchain data structure. Permissioned blockchain platforms utilize new consensus protocols in contrast with public blockchains that use traditional ones. Algorithms for permissioned blockchains tend to reach consensus faster and more efficiently in a private environment. In order for the different peers of a blockchain network to co-operate and agree on the validity of the transaction data, a protocol needs to be adopted. This is the responsibility of a consensus algorithm that offers trust-less node interaction and decentralized applications implementation inside a blockchain network.

The Transactions Handling Module is another core blockchain network module. Its main responsibility is to store the transaction data on the blockchain ledger. It is directly connected with the previously mentioned Consensus Module of the Blockchain Layer together forming the blockchain data structure. The two modules interact with each other and together communicate with the Middleware Layer as a whole blockchain scheme. When a transaction is being submitted to the blockchain network, all of its information is recorded on the ledger. Data such as the transaction hash, the address of the sender, the address of the receiver, the timestamp, the value of the transaction and other information are grouped and committed on the ledger. The Transactions Module is absolutely necessary in order to properly handle and forward this information of any happening transaction inside the blockchain network.

4.3. Middleware Layer

The "Middleware Layer" is the core layer of the infrastructure since it is the substantial connecting tier between the Blockchain Layer and the top layers that are closer to the supply chain management such as Enterprise Resource Planning (ERPs) and other related software packages. The Middleware Layer each consists of the following modules:

Upload Handler: The "Upload Handler" regulates document uploading such as e-invoices, receipts or other official documents associated with every step of the value chain. When a new document (e.g., e-invoice) needs to enter the infrastructure, certain operations need to be followed in order to handle it and guide it through the architecture. The Upload Handler module interacts with the top layers (Application Layer) through appropriate APIs for controlling and managing the initial uploading of information. For instance in order to upload an e-invoice a smart contract is created and deployed through the "Smart Contract Manager" module. After that, the e-invoice is stored on the corresponding distributed data storage, as described on the "Data Orchestrator" module below.

Data Orchestrator: The "Data Orchestrator" Module is responsible for storing efficiently an e-invoice in a secure distributed manner with low latency. Highly distributed storage and file systems are very suitable for such implementations and approaches such as the InterPlanetary File System (IPFS) [38]. This module retrieves and stores securely the e-invoice, either 'Required' or 'Paid', provided from the Upload Handler module.

Smart Contract Manager: The Smart Contract Manager is a crucial module of the Middleware Layer since most operations go through its functionalities and approval mechanisms. The automatic creation, deployment, and triggering of smart contracts constitute its main responsibility. It is a module with core functionalities that interacts with the Upload Handler and the Transactions Handler. When a merchant or customer is uploading an e-invoice, either 'Required' or 'Paid', the Smart Contract Manager processes the respective inputs collected from the Upload Handler (sender and receiver addresses, e-invoice due date and value, and other e-invoice information) and creates a new smart contract. After that, the module deploys it to the blockchain network through the Transactions Handler. If a 'Required' e-invoice is uploaded, this new smart contract emits an event inside the blockchain network in order to trigger a customer's smart contract that eventually informs their ERP that they need to pay this 'Required Invoice'.

Application level Transactions Handler: This module regulates transactions managing inside the supply chain management infrastructure of the participating actors and is responsible for all the interactions between the Application level and Middleware Layer. It can be regarded as the external Application Programming Interface (API) with the middleware services that need to further process this request to the blockchain ledger. Interacting with the Smart Contract Manager module is also foreseen as many times the different transactions are going to be bound to specific conditions imposed by the smart contract upon which they are based. As clearly explained previously in the Smart Contract Manager, every smart contract related functionality creates a new transaction that is controlled by the Transactions Handler and forwarded to the Blockchain Layer.

Figure 2 illustrates information about the integration of blockchain technology and supply chain by introducing a blockchain architecture scheme which handles each product stage with similar respect. As can be seen from the figure, every supply chain stage is approached as a step of the freight journey which is recorded thoroughly on the blockchain ledger. On each step, two parties are engaging together with the blockchain service which automates the procedures of the step, such as submitting any necessary transactions on the ledger. More specifically, on stage n+1 there exists a party that inputs data (party n) and a party that receives the step's output information (party n+1). This procedure is completely automated through the Middleware Blockchain Service which handles data properly and submits the necessary step transactions on the blockchain ledger. For instance, at the end of the legitimate completion of a particular step, special smart contracts would be triggered in order to distribute payments to custom parties.

On the proposed schema of Figure 2, each party prepares the next step (stage) of the supply chain by confirming the previous one. In particular, the confirmation takes place by inputting the proper hashes and other proof material output from the previous step. After that, custom smart contracts could be triggered depending on the step, and then, the Middleware confirms the validity of the input and initiates next stage's procedures. Such procedures would be to gather appropriate transaction hashes, tags or electronic seals, and other ledger information of previous steps, as shown in the figure. The Middleware interacts directly with the blockchain ledger and its blocks that include transactions and all the important tamperproof data. Following this, the supply chain step is eventually executed through the Middleware in an environment that ensures a continuous data validation. After the stage completion, the actions are reported by submitting one or more new transactions on the ledger that includes the appropriate product tags or electronic seals. The new transactions prove in the legitimate circumstances under which the supply chain stage was finished and allow the next stage to be initiated.

The possible case of any product failure, human error or intended fraud will immediately be detected since the appropriate hashes and other crypto material will not match for the next step to get started. Since all values are reported on the blockchain ledger, any mismatch would trigger smart contracts that encounter matters of such kind and would inform both step parties as well as other participants of the whole chain if necessary for the error. For instance, cold medical bottles' temperature on a specific truck raised about 40% above the threshold during the transportation, and thus, they are currently useless since they are able to cause serious problems to patients.

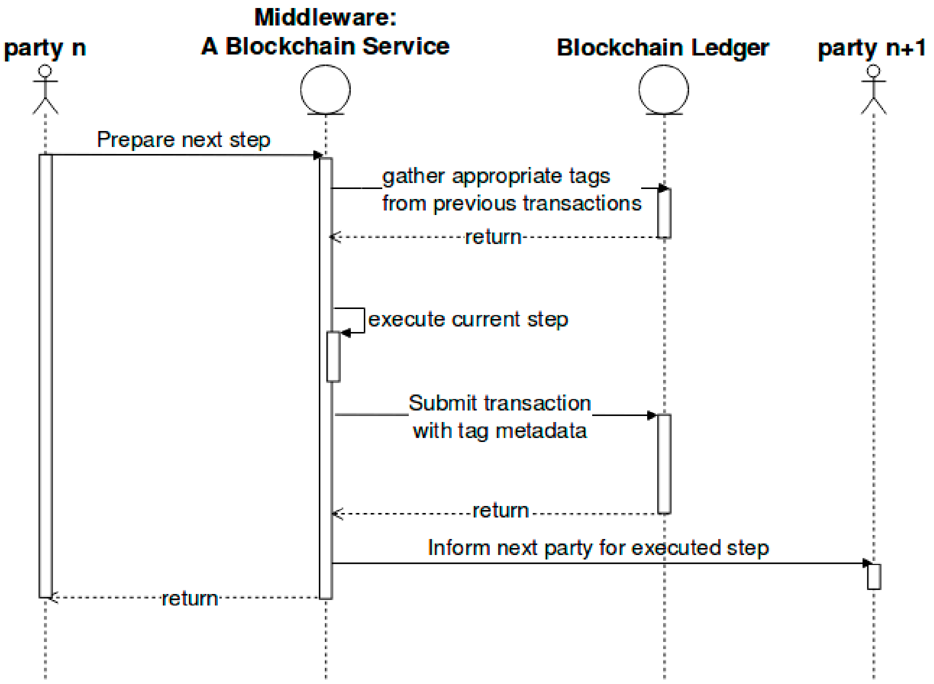

Figure 2. One supply chain freight stage (***stage number n*+1**) as a blockchain transaction. Every stage's functionality is automated by the "Middleware", and thus, the parties that participate in each stage (a single one in the input and another one in the output) have a small interaction with it; for instance, the driver confirms that the transportation was completed by receiving the appropriate transaction hash, or the employee confirms that certain materials were kept refrigerated, as expected, by collecting the corresponding transaction hashes and others. Here, ***party n*** participates in ***stage n*+1** input (and already in stage n output) while ***party n*+1** participates on ***stage n*+1** output (and stage n+2 input).

5. Discussion: Challenges and Possible Solutions

While modern blockchains present a great potential for building the internet systems of the future, they face several technical challenges nowadays. Thus, the choice between the most suitable platforms for the supply chain use case should be decided after wise and thorough consideration and research. To begin with, an extremely important issue is the mechanism with which consensus will be reached in order for the peers of a supply chain peer-to-peer network to decide what the next block will be in the chain. While we can argue that the simplicity and directness of the proof of work mechanism has been fundamental in the success of the Bitcoin protocol and in its great resonance, today we are already dealing with a huge issue concerning the high-energy intensity of the mechanism. Indeed, proof of work has contributed in the democratization of the general agreement between the network participants about the transaction and block validity, but there are also other kinds of problems. One of these issues is selfish mining, where a sub-group of miners agree to mine the next block privately and eventually result in their own custom chain that ends up attacking the network. This fact is contradictory to the fundamental and intrinsic feature of blockchains as being enablers of trust in open, trustless networks. Such a lack of trust however would be hindering the further adoption of blockchains in the logistics industry having disastrous impact consequences in the market and the consumer trust on the brands.

Hence, an important issue when combining blockchain and supply chain use case is the decision on the consensus mechanism to be used, which introduces several concerns to be addressed. For instance, a proof of work consensus algorithm tends to be very energy-intensive and therefore, costly to support the supply chain use case. This would result in a significant overhead in supply chain costs. On the other hand, consensus mechanisms such as proof of stake show that they have their own issues that need further investigated, apart from that they are not applied yet on a real large scale use case, for example, a Bitcoin equivalent, that would eventually present new possible issues. Other implementations, for instance, Linux Foundation Hyperledger implements Practical Byzantine Fault Tolerance consensus mechanism; an enabling blockchain mechanism that on the one hand does not require energy consumption, and on the other hand, solves the general agreement problem in large-scale blockchain networks. In such consensus mechanisms, all peer nodes in the system make a joint decision in a twofold consensus based on both a selection mechanism and a process, through which the various nodes that will be called upon to choose the final block to enter the chain, will compulsorily demonstrate their credibility in the system. However, even these mechanisms have problems that could be very critical. Recently, such a blockchain based on delegated (federated) consensus was put out of order for several hours, bringing the utmost darkness in transactions and trade. This would be virtually unacceptable in the production environment of supply chains. Other consensus algorithms use server-client architecture, such as Ripple [23] sub networks, in order to separate transaction logic from consensus logic. In particular, there are the so-called "servers" that are involved in the consensus process, and "clients" who actually manage transactions. It is clear that, for a plethora of supply chain use cases, it is necessary to consider various parameters in choosing which consensus mechanism will be suitable to be implemented in a blockchain. They certainly have to be inexpensive, yet transparent, simple, and fair enough to avoid selfish behavior and guarantee an increased level of trust upon which the business relationships of the supply chain stakeholder rely on.

On the one hand, it is easily understood that a large-scale supply chain application will probably need to use an open and public blockchain platform and not a permissioned or private one. On the other hand, a supply chain that does not have a specific value for both the consumer and the producer could permit the consolidation of permissioned or private blockchains. Undoubtedly, this would entail an additional management cost for all actors in the supply chain, and thus, for the final consumer who should be a participant of a particular blockchain to purchase a particular good and for those who would be involved as intermediary relatives. In addition, a permissioned or private blockchain brings its associated management costs especially when we have more complex blockchain architectures such as when separating the consensus mechanism from transaction management. It is also crucial to understand how various smart contracts will be implemented in such complex multilevel architectures of corresponding implementations. Obviously, in the supply chain, the overall cost should be allocated equally to all participants as it happens in trade agreements. For example, the proof of stake consensus mechanism would be unfair for those with a lower share in the value chain, even though their added value is particularly important for the final product. Therefore, although today we have a plethora of alternative consensus mechanisms, it appears that there is still a great deal of research to find those algorithms that are flexible enough to support a wide range of applications and use cases for the different use cases of supply chain.

As far as it concerns scalability and performance, a corresponding physical limit for these features is the bandwidth in the communications networks, the size of blocks (blockchain bandwidth) and the overall time it takes for a transaction to be regarded as validated (transaction confirmation time). For example, Bitcoin's blockchain, the largest and oldest blockchain in use, has already reached its limits in the production environment, even though Bitcoin itself has not yet taken a significant share in e-commerce. This of course may be purely due to the fact that originally it was designed with other conditions and other assumptions that could exist. However, we understand that production level public blockchains have their own dynamics and the market adoption potential can cause an impact which cannot be easily foreseen and handled in a dynamic on-the-fly way. It seems that modern blockchain implementations take into considerations such limits at their design phase as to be able to follow large scale global deployments, however up to now there is no real world experimentation with the real limitations of blockchains. As for the scalability issue, and since space within a block can only be limited, it becomes apparent that a physical limit for a blockchain is the number of transactions each block can contain. Since blocks are displayed and produced in a specified interval, obviously, this constitutes a natural limit. Another technique for achieving higher levels of scaling is to create hierarchies of "consensus instances," commonly referred to as "sidechains" [39]. While this can affect the decentralization nature of blockchains, it has the benefit that sidechains may also run non-proof-of-work consensus protocols, such as BFT. Sidechains, however, come along with their own technical challenges. Among others mining coordination is mentioned [40], which otherwise introduces further complexity and vulnerabilities, the need for inter-chain transactions with further technical and administrative burden caused, and delays on the total confirmation time. In the multi-stakeholder world of logistics and supply chains industries we envisage that technical approaches with sidechains and inter-blockchain transactions are worth being further investigated and explored.

Privacy and security issues on blockchains [41,42] are important features for the logistics industry as they concern the information of the products, the consumers and the interactions between them. The blockchains rely on digital signatures (based on cryptography) to define the identities of the participants in the network. In the Bitcoin network for instance the wallet ID is the one which defines the identification of the participant and, through this someone can search for specific transactions are interact with him/her. In the supply chain use cases blockchains are supposed to be used also as a distributed way of storing data. But the irreversibility and transparency of blockchains mean they are probably unsuitable for privacy sensitive data (data that can reveal physical identities and disclose for instance consumer habits, privacy, and proof of location, etc.). Data stored in blockchains cannot be changed, and so it is very important that we design blockchains to protect users' privacy. One approach could be to have blockchains used only to provide a timestamp for information of the supply chain workflow held elsewhere (in external data repositories). This approach of using blockchains purely as a timestamping mechanism and not as a data store has the additional benefit of being more likely to scale in the face of large amounts of data needing to be recorded. Finally, additional encryption of data before pushed into the blockchain can be possible. The main problem with this approach is that if the decryption key for encrypted data is ever made public, the encrypted content is readable by anyone with that key; there is no way of encrypting the data with a different key once it is embedded within the blockchain. Regardless of the approach taken to designing blockchains, every blockchain contains transaction data and thus all privacy, by design principles, have to be taken into consideration before letting any transaction in the ledgers of public/private blockchain implementations.

6. Conclusions

The road to a global supply chain management framework relying on blockchains passes through many phases and many challenges that have to be faced. While the discussion on features such as scalability, performance, consensus mechanism, public vs. permissioned blockchain cannot be exhausted in the frame of an individual study it is necessary to invest further research on topics that will pave the intermediate steps towards the blockchain adoption in the supply chain industry. An intermediate step of having consortium-based, permissioned ledgers, which can be applied on specific cross-organizational domains, can be regarded a s starting point for tackling the research challenges and facilitate the necessary changes based on controlled private ledger environments, where such blockchain features can be managed effectively. Permissioned blockchains raise many barriers that have to do with energy efficiency, cost of transactions, total confirmation time, as well as security and privacy issues. Nevertheless, such approaches cannot be regarded as totally decentralized as they still have to rely on central trusted parties who will be responsible to validate the identity of the participating actors and assign the necessary credentials of the blockchain. As the research progresses in inter-domain and inter-chain blockchain implementations, the path to public blockchains will be paved with more concrete ideas and the implementation will be facilitated with more concreted design principles and adoption maturity from the respective stakeholders of the supply chain industry. The specific paper presented, among others, an analysis on the blockchain adoption for a large-scale deployment on the supply chain management industry. It is within the future research priorities of the authors to proceed with detailed analysis on specific blockchain implementations (both permissioned and permissionless) for particular supply chain management use cases (such as the retail industry) and focus on performance monitoring and measuring.

Author Contributions: The authors collaborated on all sections of the paper and all authors participated in all writing and revising.

Funding: This research received no external funding.

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

References

1. Abeyratne, S.A.; Monfared, R.P. Blockchain ready manufacturing supply chain using distributed ledger. *Int. J. Res. Eng. Technol.* **2016**, *5*, 1–10.
2. Baier, A. Organic Certification Process. National Sustainable Agriculture Information Service, 2005. Available online: https://attra.ncat.org/attra-pub-summaries/?pub=163 (accessed on 21 March 2018).
3. Elder, S.D.; Zerriffi, H.; le Billon, P. Is Fairtrade certification greening agricultural practices? An analysis of Fairtrade environmental standards in Rwanda. *J. Rural Stud.* **2013**, *32*, 264–274. [CrossRef]
4. el Maouchi, M.; Ersoy, O.; Erkin, Z. TRADE: A Transparent, Decentralized Traceability System for the Supply Chain. 2018. Available online: http://dx.doi.org/10.18420/blockchain2018_01 (accessed on 10 November 2018).
5. Peters, G.W.; Panayi, E.; Chapelle, A. Trends in Crypto-Currencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective. 2015. Available online: http://dx.doi.org/10.2139/ssrn.2646618 (accessed on 10 November 2018).
6. Zhang, Y.; Wen, J. An IoT electric business model based on the protocol of bitcoin. In Proceedings of the 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 17–19 February 2015; pp. 184–191.
7. Kim, H.M.; Laskowski, M. Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance. 2016. Available online: https://dx.doi.org/10.2139/ssrn.2828369 (accessed on 17 January 2019).
8. Sharples, M.; Domingue, J. The blockchain and kudos: A distributed system for educational record, reputation and reward. In *Proceedings of the 11th European Conference on Technology Enhanced Learning (EC-TEL 2015), Lyon, France, 2015*; Springer: Cham, Switzerland, 2015; pp. 490–496.
9. Verhoeven, P.; Sinn, F.; Herden, T.T. Examples from Blockchain Implementations in Logistics and Supply Chain Management: Exploring the Mindful Use of a New Technology. *Logistics* **2018**, *2*, 20. [CrossRef]
10. Dobrovnik, M.; Herold, D.M.; Fürst, E.; Kummer, S. Blockchain for and in Logistics: What to Adopt and Where to Start. *Logistics* **2018**, *2*, 18. [CrossRef]
11. Tian, F. An agri-food supply chain traceability system for China based on RFID & blockchain technology. In Proceedings of the 2016 13th International Conference on Service Systems and Service Management (ICSSSM), Kunming, China, 24–26 June 2016; pp. 1–6.
12. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
13. ZERV Commerce Platform. Available online: https://zervnetwork.com// (accessed on 31 October 2018).
14. 300Cubits, TEU Tokens—Bitcoin for Shipping. 2018. Available online: https://300cubits.tech/ (accessed on 31 October 2018).
15. Bext360, Transparency That's Good for Everyone. 2018. Available online: https://www.bext360.com/ (accessed on 31 October 2018).
16. IBM, Let's Put Smart to Work. 2018. Available online: https://www.ibm.com/industries/retail-consumer-products/supply-chain (accessed on 31 October 2018).
17. Haotanto, A.V. Modern-day Slavery in the Supply Chain: What You Can Do. Available online: https://www.freemalaysiatoday.com/category/leisure/2018/11/22/modern-day-slavery-in-the-supply-chain-what-you-can-do/ (accessed on 7 January 2019).
18. Bae, J.; Lim, H. Random Mining Group Selection to Prevent 51% Attacks on Bitcoin. In Proceedings of the 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), Luxembourg, 25–28 June 2018.
19. Eyal, I.; Sirer, E.G. Majority is not enough: Bitcoin mining is vulnerable. In Proceedings of the International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 9 November 2014; pp. 436–454.
20. Bach, L.M.; Mihaljevic, B.; Zagar, M. Comparative analysis of blockchain consensus algorithms. In Proceedings of the 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 21–25 May 2018; pp. 1545–1550.

21. Nakamoto, S. Bitcoin: A Peer-to-peer Electronic Cash System, 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 31 October 2018).
22. Ethereum Introduction. Available online: http://ethdocs.org/en/latest/introduction/index.html (accessed on 31 October 2018).
23. David, S.; Noah, Y.; Arthur, B. The Ripple Protocol Consensus Algorithm, Ripple Labs Inc., 2014. Available online: https://ripple.com/files/ripple_consensus_whitepaper.pdf (accessed on 31 October 2018).
24. Bitcoin Cash. Available online: https://www.bitcoincash.org/ (accessed on 31 October 2018).
25. Litecoin wiki. Available online: https://litecoin.info/index.php/Main_Page (accessed on 31 October 2018).
26. EOS.IO Technical White Paper. 2017. Available online: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md (accessed on 31 October 2018).
27. Larimer, D. DPOS Consensus Algorithm—The Missing Whitepaper, Steemit, 2018. Available online: https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper (accessed on 31 October 2018).
28. Russell, K.A.; David, B.; Oliynykov, R. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. In Proceedings of the Advances in Cryptology—CRYPTO 2017, Santa Barbara, CA, USA, 20–24 August 2017; pp. 357–388.
29. Mazieres, D. The Stellar Consensus Protocol: A Federated Model for Internet-Level Consensus. 2016. Available online: https://www.stellar.org/papers/stellar-consensus-protocol.pdf (accessed on 31 October 2018).
30. NEO White Paper. Available online: http://docs.neo.org/en-us/ (accessed on 31 October 2018).
31. Monero White Paper. Available online: https://whitepaperdatabase.com/monero-xmr-whitepaper/ (accessed on 31 October 2018).
32. Tether White Paper. Available online: https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf (accessed on 31 October 2018).
33. NEM Technical Reference, Version 1.2.2018. Available online: https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf. (accessed on 31 October 2018).
34. Neudecker, T.; Hartenstein, H. Network Layer Aspects of Permissionless Blockchains. *IEEE Commun. Surv. Tutor.* **2018**. [CrossRef]
35. Tsai, W.-T.; Yu, L. Lessons Learned from Developing Permissioned Blockchains. In Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, 16–20 July 2018; pp. 1–10.
36. Sompolinsky, Y.; Zohar, A. Secure High-Rate Transaction Processing in Bitcoin. In *Financial Cryptography and Data Security*; Lecture Notes in Computer Science; Böhme, R., Okamoto, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2015; Volume 8975.
37. PwC Report: Pulling Fraud out of the Shadows, Global Economic Crime and Fraud Survey 2018. Available online: https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf (accessed on 7 January 2019).
38. Interplanetary File System IPFS. Available online: https://ipfs.io (accessed on 31 October 2018).
39. Croman, K.C.; Eyal, I.; Gencer, A.E.; Juels, A.; Kosba, A.E.; Miller, A.; Saxena, P.; Shi, E.; Sirer, E.G.; Song, D.X.; et al. On Scaling Decentralized Blockchains. In *Financial Cryptography and Data Security*; Lecture Notes in Computer Science; Clark, J., Meiklejohn, S., Ryan, P., Wallach, D., Brenner, M., Rohloff, K., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9604.
40. Back, A.; Corallo, M.; Dashjr, L.; Friedenbach, M.; Maxwell, G.; Miller, A.; Poelstra, A.; Timón, J.; Wuille, P. Enabling Blockchain Innovations with Pegged Sidechains. Available online: https://www.blockstream.com/sidechains.pdf (accessed on 31 October 2018).
41. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 839–858.
42. Noyes, C. Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning. *arXiv*, 2016; arXiv:1601.01405.