computers

Review

Distributed Interoperable Records: The Key to Better Supply Chain Management

Annegret Henninger [1,*] and Atefeh Mashatan [2]

[1] Ted Rogers School of Management, Ryerson University, 55 Dundas Street W, Toronto, ON M5G 2C3, Canada
[2] Cybersecurity Research Lab, Ryerson University, 350 Victoria Street, Toronto, ON M5B 2K3, Canada; amashatan@ryerson.ca
[*] Correspondence: annegret.henninger@ryerson.ca

Abstract: The global supply chain is a network of interconnected processes that create, use, and exchange records, but which were not designed to interact with one another. As such, the key to unlocking the full potential of supply chain management (SCM) technologies is achieving interoperability across participating records systems and networks. We review existing research and solutions using distributed ledger technology (DLT) and provide a survey of its current state of practice. We additionally propose a holistic solution: a DLT-based interoperable future state that could enable the interoperable, efficient, reliable, and secure exchange of records with integrity. Finally, we provide a gap analysis between our proposed future state and the current state, which also serves as a gap analysis for many fractional DLT-based SCM solutions and research.

Keywords: records; record management; blockchain; DLT; identity management; supply chain management; interoperability; information sharing

Citation: Henninger, A.; Mashatan, A. Distributed Interoperable Records: The Key to Better Supply Chain Management. *Computers* **2021**, *10*, 89. https://doi.org/10.3390/computers10070089

Academic Editor: Hossain Shahriar

Received: 31 May 2021
Accepted: 9 July 2021
Published: 19 July 2021

1. Introduction

Supply chain management (SCM) is the backbone of most trades; it is a distribution system that facilitates the flow of items through the supply chain until they are consumed by and disposed of by consumers [1]. However, with globalization, supply chains have grown to be supersized, complex networks of facilities, actors, and processes with many constantly moving parts and exchanges of information. It is no wonder that SCM is a heavily researched area of business. A recently popular focus of research in SCM is the application of blockchain technology, particularly for introducing transparency and end-to-end visibility. However, due to the vast, expansive, and complex nature of the supply chain, interoperability of records systems and other interacting systems remains a barrier, preventing the application of blockchain from reaching its full potential.

Within the opaque, continuous exchange of interdependent information, exist records which act as evidence of business activity and are thus information assets which reflect transactions [2]. They can, for instance, show an exchange of values between parties or provide evidence of a signed business contract. The integrity, authenticity, reliability, and usability of these records are necessary to lay a factual foundation for improving SCM. Improved flow of records and interoperability of records systems in supply chains could provide improvements in the handling of damages, real-time location, source origins, temperatures during shipment, etc. [3]. Increased record reliability, authenticity, integrity, and usability throughout all the events in the supply chain could help reduce double-spending, financial discrepancies, increase efficiencies, and help to identify issues and their causes in real-time.

Ideally, global supply chains would be interoperable and able to seamlessly trade or share any amount of data, information or computational capacity. However, due to a lack of interoperability, enterprises, networks, and records systems in the supply chain look more similar to digital islands in Figure 1: Disconnected Digital Islands (Figure 1 was created by the authors of this paper, Henninger and Mashatan, for this paper, and should be cited as such). Each island has varying levels of technological abilities designed to meet their needs, but which are not designed to communicate with the technology of or share records with other organizations. Regardless of the level of technological sophistication of these organizations, they are limited by their inability to seamlessly integrate with and exchange records with other records systems.

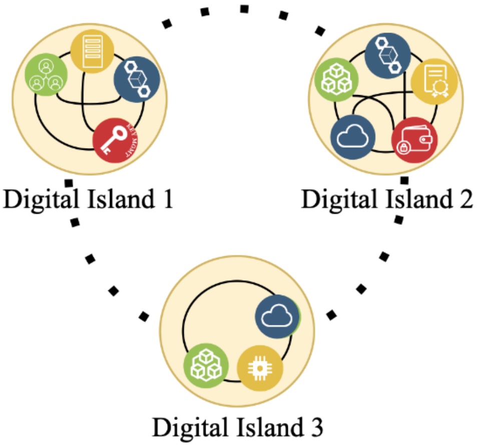

Figure 1. Disconnected digital islands.

For example, as goods travel across the supply chain, between multiple actors who each require varying data formats, the associated records become fragmented, converted, migrate across hardware and software configurations, and even migrate between manual and automatic data processing functions that create room for human error. This slows down the supply chain process, is inefficient, can introduce errors, and can impact the reliability of records. The full potential cannot be reached without supply chain interoperability whereby all stakeholders have access to and contribute to the data [4].

Before determining a future state of supply chain interoperability, using DLT-based records systems, the current state of practice needs to be determined. To the best of our knowledge, there exists no survey, review, or systematic literature review of the current state of DLT-based supply chain recordkeeping solutions. To fill that gap, we provide a review article which is a type of academic paper based on existing published articles, very similar to a systematic literature review [5]. Review papers summarize the existing literature on a topic in order to explain the current state of knowledge, progress, and practice on the topic and identify significant gaps in the state of the art [6]. Review papers are instrumental in communicating and understanding the progress of scientific work my presenting otherwise isolated scientific findings in relation to one another [7]. Additionally, review articles offer a window into the mechanisms involved as "ideas move from tentative propositions to accepted knowledge" [7] (p. 341).

- We additionally provide our novel proposed future state of interoperable supply chains using DLT-based records systems, and a gap analysis between our proposed future state and the current state which also serves as a gap analysis for many proposed, fractional DLT-based SCM solutions. The purpose of a gap analysis to locate the gaps and identify the differences between the current situation and "what ought to be" [6]. Gap analyses have been established for some time and adopted in several fields, e.g., Mineraud, Mazhelis, Su, and Tarkoma's 2016 gap analysis of Internet of Things platforms [8], Scott et al.'s 1993 gap analysis of biological diversity [9], or Brown and Swartz's 1989 gap analysis of professional service quality [10].

This paper provides the following. An overview of the overarching topics covered in this paper is provided in Section 2 under background: Section 2.1 identifies the requirements for authoritative record management as defined by the International Standards Organization which are used as the foundations of our review, Section 2.2 provides an overview of SCM and issues there within, and Section 2.3 provides an overview of DLT and blockchain as well as a survey the landscape of development in the areas of DLT solutions for SCM. An extensive literature review is provided in Section 3 under Emerging Technology Layers, where we identify and review the six emerging technology layers of SCM: ID management, IoT, analytics, events, finances, and privacy. Additionally, we propose a future state, enabled by Decentralized Records Systems (DRSs). The business implications of implementing DRSs across the technology layers are provided in Section 4 under Business Implications of Emerging Technology Layers. Finally, the gaps currently standing in the way of achieving a future state are identified in Section 5 under Gaps and the paper is summarized in Section 6 under Conclusion.

2. Background

The following provides a foundational overview of records, SCM, and DLT and DLT efforts in SCM.

2.1. Records

This paper recognizes records, their concepts, and their principles as defined by the International Standards Organization [2]. Records provide evidence of business activities and information assets that are of a transactional nature and rely on metadata to provide context and to be managed. Any piece or set of information can be managed as a record regardless of its structure including documents, data collection, digital or analogue information, etc. Records metadata should describe the record content, its structure, the business context, identifiers and other information needed to locate and use the record (e.g., format and storage information), the business actions that involve the record, and any relationships. The metadata should identify relationships to legal or social contexts, to agents who create, use, and manage records, and any relationships or dependencies to other records and records systems.

The characteristics of authoritative records, as defined by the ISO, include authenticity, reliability, integrity, and usability [2].

Authenticity. An authentic record must provide evidence that it is what it claims to be, was created or sent by the agent that claimed to do so, and that it was sent when it claimed to have been sent.

Reliability. A reliable record has contents that can be trusted to be the full and accurate representation of the transaction or information it represents and can be depended upon in subsequent transactions. Records should be created at the time of the event which it represents or soon after.

Integrity. Records should be protected against any unauthorized alteration. Alterations should be traceable, and policies and procedures should specify what alterations should be made to a record after its creation and under what circumstances.

Usability. To be usable, records should be located, retrieved, presented, and interpreted by stakeholders within a reasonable time as defined by the stakeholders.

Authentic, reliable, unaltered, and usable records have the potential to enable (1) increased transparency and accountability, (2) effective policy formation, (3) improved decision-making, (4) risk management, (5) business continuity (in the event of a disaster), (6) protection of rights, (7) litigation support, (8) compliance, (9) corporate responsibility support, (10) increased efficiency capable of reducing costs, (11) intellectual property protection, (12) development activities, and (13) the protection of personal, corporate, and collective memory [2]. These attributes are universally valuable for business transactions and are particularly valuable in the supply chain whereby goods and their associated records change hands a multitude of times, creating an opportunity to undermine one or several of the attributes with each transition.

The ISO principles for managing records include the protection of their authenticity, integrity, reliability, and usability, and extend to the creation of records so that they meet the requirements for them to act as evidence. The ISO guidelines also recommend a records system that enables accountability and organizational success by establishing a framework for the objectives, policies, and directives of records [2]. A records system establishes requirements for systematic processes, monitoring and evaluation, review and improvement, and role and responsibility definitions [2].

The ISO finds that digital environments and new business models provide increased opportunities for record use. However, they also find that capabilities and requirements for digital records need to be extended beyond traditional organizational boundaries to support multi-jurisdictional, collaborative work. This is particularly true of supply chain management.

2.2. Supply Chain Management

Supply chain management (SCM) is notably dynamic and complex since a supply chain distribution system usually encompasses an expansive network of actors and facilities with a multitude of ever-changing functions [11]. These functions include logistics, payments, shipping, transportation, financing, auditing, route changes, item location tracking, inspection, due diligence procedures, compliance with regulating bodies, and ever-increasing consumer expectations [12] Each of the functions, and their underlying work processes, generate a multitude of records needed for the operation of the functions and processes and also provides evidence of the proper operation supply chain.

In addition to the flow of items, a complex synchronic flow of records representing the transactions and business activities throughout the supply chain must also be managed. Reliable records are needed for reporting by shippers/forwarders, international regulators, customs agents, food or safety inspectors, law enforcement, insurance companies, anti-smuggling, and Non-Government Organization (NGO) observers, etc. The reporting data include documentation needed at border crossings, custody or ownership transfers, the contents of a shipment, safety information, insurance information, national origin, license to move, certifications, etc. [13].

Well researched challenges of SCM include achieving transparency, item provenance, end-to-end visibility, and real-time monitoring [11,14]. A resulting challenge is that of traceability which depends on these factors and has even been defined as "a record-keeping system", or "record identification" in supply chains [15–17]. The biggest challenge is the lack of interoperability among processes that cross national and industry boundaries, and the technologies used to complete the processes. Supply chains cross borders and jurisdictions and must adhere to the industry-wide, global, national, and local laws and regulations of each area [13].

The technologies used in supply chain processes require various data formats, protocols, and standards. While they are designed to connect and support Industry 4.0, a lack of standardization (i.e., standard protocols, standard data formats, and transaction structures) prevents them from reaching seamless connectivity with all relevant stakeholders [13,18]. For supply chain logistics, local leading companies are able to specialize in particular jurisdictions and industries, but dual global and local demands and the lack of standardization prevents the emergence of a leading provider of cross-industry or cross-jurisdiction logistics [13].

2.3. Distributed Ledger Technology

Distributed ledger technology (DLT) is a decentralized ledger with multiple actors and nodes. The decentralized nature of DLT eliminates the possibility of a single point of failure to appear in centralized systems [19]. Because a DLT holds multiple copies of a record, it is difficult for any single party to make an unauthorized change to a record without the support and agreement of all parties who store a copy [20]. This increases trust across a network of interacting actors, such as in the case of a supply chain, since each actor has access to a canonical transparent and verifiable record about the status of the supply chain.

Blockchain technology is a type of DLT running on a network of nodes that can function as a public, private, or consortium blockchain [19]. In a blockchain, the distributed "ledger" is an append-only, tamper-evident, and tamper-resistant series of sequential blocks that hold digitally signed transactions [19,20]. Transactions are the smallest unit of a work process that involves an exchange between entities. They can be in the form of financial transactions, executable code known as smart contracts, or a recording of digital assets [21]. Transactions are hashed and digitally signed, and then, if validated, formed into blocks that are time-stamped into the ledger and cryptographically linked to the previous block [22].

The cryptographically linked blocks make for tamper-evident records stored in the transactions. This is a result of the hash function used. If anything were changed, the resulting new hash function would not match the original ones, making the change evident to the network [23]. As a result, the ledger is append-only. The two main types of blockchains are public and private. Public blockchains can be further divided into permissioned and permissionless. Permissionless chains are open to everyone, and any user can read, write, and use the blockchain (e.g., Bitcoin and Ethereum). Public-permissioned blockchains are readable by everyone but only permissioned users can write to them (e.g., corporate supply chains viewable to the public) [24]. Private blockchains are either private-permissioned or consortium. Private chains have a selected group of authorized nodes with reading permissions, and only the network operator can write to the ledger [24]. Consortium blockchains grant authorized groups read and/or write access (e.g., multiple banks on a shared ledger). There is a type of blockchain suitable for any organizational need.

Many solutions are being developed and introduced for DLT-enabled SCM [25]. reviewed current IoT solutions in SCM and found a concentration in the following applications: warehousing, order management, inventory management, and transportation. The benefits found in these areas were categorized into condition, tracking, costing, pricing, and dynamic optimization [25]. Overall, they found a concentration of work in production, inventory, and order management capabilities, and a gap in the long-term impacts and models of facility and supply chain network design. [26] found that there has been a recent and increasing focus on potential blockchain solutions in logistics-specific solutions.

We have surveyed current DLT-based innovation and technological solutions for the challenges facing SCM and identified 15 projects that propose promising SCM solutions. Table 1, below, provides the list of 15 blockchain-based SCM solutions and the problems which they address, the industries covered, and blockchain technology used. Three efforts, Tradelense, Unisot, and Walton Chain are reviewed in-depth after the table, but a brief overview of all projects in Table 1 is provided in Appendix A.

As seen in Table 1, existing blockchain-based solutions for SCM are particularly concentrated on ID management and IoT, followed by Analytics, events, finance, privacy, proof of origin, and proof of quality. Proof of origin and proof of quality, rather than being technology layers, are viewed as outcomes that can be achieved using the capabilities of the other factors which we have thus identified as the six, critical technology layers of SCM.

With the development of several platforms and services incorporating blockchain technology into logistics and SCM, it raises the challenge of interoperability among these platforms and services [26]. Most of the technologies addressing interoperability propose validators to bridge between different blockchain networks [27]. Two notable projects addressing interoperability and creating a network of blockchains are The Polkadot and The Cosmos Network [28,29]. Regulatory uncertainty, data/records security concerns, and collaborations of parties have been mentioned as SCM challenges across current literature as well—with interoperability being the barrier to collaboration.

There are a few noteworthy projects, particularly TradeLense, Unisot, and Walton Chain. TradeLens provides a comprehensive example of what a DLT-based supply chain could do. While these projects and other supply chain projects do not mention records specifically, the data they work with are of a transactional nature, pertaining to items and services being sold, is needed for reference, and necessary to provide evidence of the complete, multiple transactions as goods travel through the supply chain.

Table 1. Current Innovation and Technical Solutions.

Solution	**Blockchain Technology**	**Proof of Origin**	**Proof of Quality**	**IoT**	**ID Management**	**Finance**	**Events**	**Analytics**	**Privacy and Confidentiality**	**Industries Covered**
TradeLens	Hyperledger	●	●			●	●	●		SCM in general
Unisot	Bitcoin SV	●	●	●	●			●		SCM in general
Mojix	Quorum	●	●	●						Retail, oil, and gas
SustainBlock	BetterChain	●	●		●				●	Mining
Modum	Proprietary	●	●	●				●	●	Pharmacy, medical, perishable, and construction materials
Everledger	Ethereum	●	●		●	●				Diamonds
SKUChain	Proprietary	●	●			●	●			Aerospace, auto, agriculture, energy, mining, banking, commodities, electronics, insurance
Treum	Ethereum/Quorum	●	●			●	●			Food, consumer products, energy, healthcare, land, and art
Scantrust	Hyperledger/GoodChain	●	●					●		SCM in general
Things Lab	IOTA Ledger/The Tangle	●	●				●			SCM in general
WaltonChain	Proprietary		●		●		●			Agriculture and retail
Blockchain in Transportation Alliance	N.A.			●						Not specific
OrgBook BC	VON/ Hyperledger Indy				●					Not specific
Zcash	Zcash								●	Cryptocurrency
Zengo	Proprietary				●					Cryptocurrency

Tradelense is an IBM-Maersk collaboration using Hyperledger. It is a service that coordinates customs agencies, government planners, and financial service providers for large shipping concerns, and provides an audit trail for the entire shipping lifecycle in the supply chain. Stakeholders can obtain access to key shipping data throughout the shipping which can be used with artificial intelligence (AI) to improve operational efficiencies. This includes timeline changes, impacted by vessel changes, weather, and harbour issues [30].

Unisot, in Norway, runs on Bitcoin SV, and provides Contracting-as-a-Service to big corporate clients. They provide real-time tracking throughout the supply chain to reduce costs. Their Digital Twin and Product DNA solutions create digital representations of supply chain items enabling stakeholders to track and trace them quickly and securely, from origin to disposal [31].

Unisot also focuses on automating the process with blockchain data interchange (BDI) automatically processing orders, deliveries, customs clearances, etc. Unisot even enables small companies to sell small bits of information for AI applications and analytics. The feature of enabled micropayments incentivizes stakeholders to sell typically siloed data by micro-features such as temperatures, location, and weight for as small a unit as cents (Euro/dollar). Unisot extends to the retail stage of supply chain management and integrates digital tokens which support global customer loyalty programs and linked customer applications to provide further information related to the goods in the supply chain.

The WaltonChain is used in China, backed by Alibaba, and uses their proprietary WaltonChain DLT. It relies on RFID technology to integrate information from IoT devices in the supply chain to provide full traceability. They allow for child chains to be created to monitor logistics, warehousing, retail circulation and production. They use a self-developed reader chip and tag which is secure with hash and signature-based encryption. They focus on (a) data reliability and (b) data value circulation. The reader and tag chips enable automation of the supply chain reducing human interference and better reliability of the events in the supply chain. This, combined with the tamper-proof record of the data, reduces the opportunity for double-spend as well as the introduction of counterfeits into the supply chain. To help with the data verification issue, the WaltonChain has child chains that accurately store their own data and upload them to the parent chain for cross-chain queries [32].

Unisot, TradeLense, and WaltonChain are sophisticated examples of blockchain-based SCM solutions and they address different technology layers. However, it can be argued that while they use blockchain technology, they have a certain level of centralization and do not change the current status of siloed solutions. From the viewpoint of full decentralization, blockchain service providers having control over the blockchain and/or enterprise blockchains with control over their own ledger is still a centralized system made up of siloes of blockchain-based computing capabilities. However, the focus of this paper is not to achieve full decentralization, but to address the issue of siloes by introducing interoperability across the ledgers.

While interoperability could theoretically be addressed in solutions built on traditional systems, these systems were not designed to communicate with one another, and the integrity of the record or data that will populate components of a record is at risk as they are exchanged between systems. Blockchain technologies and DLTs, on the other hand, are designed to run off a multitude of distributed nodes that communicate with one another. While this does not translate to interoperability directly, the concept of the distributed architecture is designed with cross-boundary interaction and communication in mind. DLTs are thus designed to provide greater security of the record travelling across systems through their tamper-evident, tamper-resistant designs. Furthermore, DLTs are still evolving, meaning that there is still an opportunity to design a network of decentralized (at some level) SCM solutions that are interoperable by design.

The target state is to have a network of interoperable, DRS-enabled global supply chains that can seamlessly interact and communicate with one another. To achieve interoperability across the supply chains, interoperability across the ledgers and existing information communication technology (ICT) needs to be achieved [4]. In other words, we need to create digital highways that can connect the current digital islands that are limited by their network of connectivity. Below, Figure 2: Digital Islands Connected Through Interoperable DLTs, illustrates how DLT can be used to facilitate digital highways between each digital island that hosts their own set of records systems and other interacting applications. Meanwhile, Figure 3: A Connected Supply Chain Using Interoperable DLTs, illustrates that all actors need to be interoperable, e.g., by using interoperable DLTs to create a connected supply chain (Figures 2 and 3 were created by the authors of this paper, Henninger and Mashatan, for this paper, and should be cited as such).We propose using DLT as a foundational technology for decentralized records systems (DRSs) to enable interoperability and thereby supporting the necessary characteristics of authentic, reliable, and usable records that have integrity. Interoperability in this way is necessary for integrating various current and legacy blockchain technologies systems [33]. Enabling this sort of connectivity will enable a single source of authoritative evidence about the status of the supply chain from end to end, i.e., the same knowledge of records across integrated DRSs.

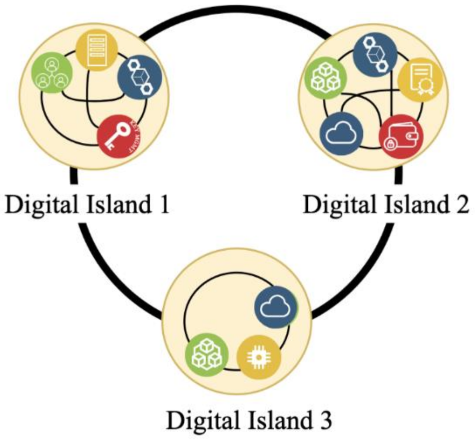

Figure 2. Digital Islands Connected through Interoperable DLTs.

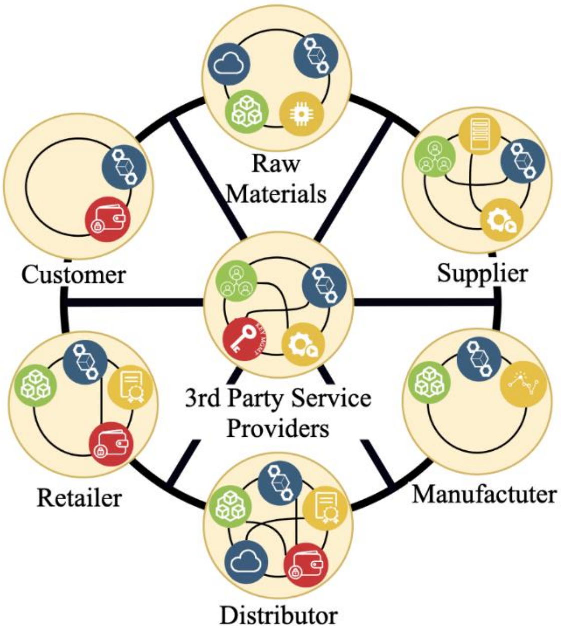

Figure 3. A Connected Supply Chain Using Interoperable DLTs.

3. Emerging Technology Layers

In Section 2.3, six main emerging technology layers of decentralized SCM initiatives were identified: ID management, IoT, analytics, finance, and privacy and confidentiality. The following is an overview of the current state of each of these layers and how it applies to our proposed future state of using decentralized records systems to enable interoperability and the essential characteristics of authentic, reliable, and usable records that have integrity.

3.1. Events

Blockchain technology is immutable, reliable, and addresses the double-spend problem present in the exchange of goods online [20]. However, it does not automatically reflect real-world events and cannot ensure the authoritativeness of data manually inputted into a system [34]. This is what's known as the "Oracle Problem". Blockchains can provide reliable information about the current state of digital reality, however, they are blind to the real world [35]. Thus, blockchains depend on "Oracles" which communicate information from the real world to the blockchain.

The provenance of items is particularly important for high-value items that can be exploited for fraud, used for money laundering, or to introduce products originating from conflict areas (i.e., diamonds, expensive handbags, watches, and expensive wines) [36].

Hidden damages in the supply chain are another area that would benefit from clear provenance. A failure to track all the events throughout the process makes it impossible to prove where and when the damages occurred, preventing the stakeholder from being able to claim compensation.

As more records of events are recorded on the blockchain, there is increased visibility in the supply chain and the window for hidden fraudulent activity is thus reduced. Events range from a shipping container reaching a harbour to a continuous stream of small events such as temperature reports for temperature-controlled goods such as the Pfizer-BioNTech COVID-19 vaccine, for which the recommended storage temperature is -70 ± 10 °C [37].

If all events were recorded in a series of interoperable ledgers, a complete traceable chain of custody would be created for the products and actors in the supply chain, enabling full transparency, traceability, and dynamic and streamlined due diligence tasks [24]. For example, if evidence existed that a located source in the supply chain is linked with irremediable human rights violations, the time and costs required to target the products originating from that source to take corrective action would be significantly reduced [24].

One of the most significant benefits of introducing blockchain technology is that it enables automation through the use of smart contracts. The idea of smart contracts was first introduced in 1994 by Nick Szabo [38]. However, they were not practical until blockchain. When on a blockchain, smart contracts are tamper-evident which provides the necessary trust model [38,39]. The tamper-evident nature of blockchain and the self-execution of smart contracts reduce possibilities for human error or tampering, affording the potential to introduce increased authority of records.

Smart contracts are software with encoded contract clauses which automate the enforcement of predefined contract rules [38]. The executable code enables smart contracts to execute automatically enabling the automation of many events creating a map of actors, relationships, and exchanges involved [40]. Smart contracts enable the automation of business functions that would usually have to be performed manually, such as the review of reports. After the automatic processing of the smart contracts, recipients can be notified of progress or issues, and records are securely stored on a decentralized ledger and can be used for audits.

Currently, the provenance of goods in the supply chain often relies on paper certificates which can be misplaced, forged or tampered with, making the authenticity and origin of products difficult to determine. Areas in the supply chain where there are manipulated, fake or missing records often result from the context of heightened supply chain risks such as areas where there are human rights violations, bribery, tax evasion, armed groups putting pressure on production sites, unacceptable labour conditions, environmental damage, and regulation violations (i.e., organic, fair trade, and pharmaceuticals) [24]. In such uncontrolled environments, removing opportunities for human creation and handling of records by the introduction of automated event execution on a blockchain using smart contracts can increase the likelihood that records will be reliably made and have integrity and thus be trusted as sources of proof of thebe authenticity of supply chain items.

3.2. ID Management

Records in various formats exist on products as they travel through the supply chain from raw material sources to the suppliers, manufacturers, retailers, consumers, and the end of their life cycle. To manage them, all entities which use them or to which they refer need to be identified including actors, products, components, data models, etc. Identities in digital systems are traditionally established, managed, authenticated, authorized, and terminated using identity management systems (IDMSs). However, traditional, centralized IDMSs are vulnerable to single points of failure, interoperability issues, and privacy risks inherent in the associated data gathering and tracking [19].

Blockchain technology is a popular candidate solution for managing these challenges. Current DLT-based ID management solutions are improving supply chains by introducing decentralized identities for real-time tracking and increasing the traceability of products.

ZenGo has additionally introduced the use of threshold signatures which removes the need for a password while maintaining security [41].

An outstanding issue with DLT solutions, however, is that they depend on centralized certificate authorities. For DRSs to be truly decentralized, identifiers for entities in the system should be created, managed and used to share information independent of centralized certificate authorities [42]. Decentralized identifiers (DIDs) and verifiable credentials (VCs) can exist and function independently from central registries and authorities [43].

A DID can be explained as being a random public string, that maps to (a) specific public information, which is stored in a registry, and (b) to specific, private information stored by the owner of the DID [44]. The public information is used to verify the private information used to construct ownership proofs [44].

Verifiable credentials are a distributed method to provide tamper-evident identifiers, to communicate and cryptographically prove certain attributes about an entity while remaining decentralized [45]. Similar to DIDs, verifiable credentials are associated with specific information that is stored in a public registry and with specific information that is stored by the credential holder [44]. Both DIDs and VCs enable the holder to provide a claim about something which can be cryptographically proved using information held in a public registry, that could, for example, be blockchain-based. They are persistent, portable, interoperable, and usable [46].

Verifiable credentials and DIDs could enable entities in the supply chain to verify claims about attributes using cryptographic proofs. This includes operational supply chain information such as location, destination, parties involved as well as product information (i.e., certified data including organic, fair trade, labour, and trade agreements) [47]. Actors in the supply chain could disclose their identity, records, and reporting data on a need-to-know basis, and businesses could rely on verifiable records without taking on the liability of identity management.

DLT is able to support decentralized digital identities with built-in credentials and control mechanisms and can act as decentralized registries for identity information or the public information associated with verifiable credentials [44].

Verifiable credentials and DIDs enabled by a distributed ledger will allow records to be used to track the life cycle of the product from raw materials to the end of its life cycle so it can be identified for recalls and proper disposal to manage the environmental impact of the product. They will enable all stakeholders to access and append data to the supply chain and enable harmonized synchronic tracking by allowing smaller companies to include their data in the supply chain system [13]. Additionally, blockchain has the potential to scale digital identities at a low cost [47].

3.3. IoT

The Internet of Things (IoT) refers to the web of connected devices that provides a flow of information to facilitate operations. The concept actually stems from supply chain applications, originating in the 1990s at the Auto-ID Centre at MIT where Kevin Ashton considered using radio-frequency identification (RFID) tags to track goods through Procter and Gamble's supply chain [19]. Presently, IoT networks encompass smartphones, GPS devices, smart devices, cloud computing, and online social networks. In Europe, the proliferation of IoT objects has enabled Industry 4.0 marked by the integration of ICTs with industrial technology [19]. In SCM today, IoT enables the continuous and autonomous coordination and gathering of records throughout the supply chain, providing increased visibility, agility, and reduced time between data capture and decision making [25,48].

Beyond identifying an entity or commodity in the supply chain, reporting is also needed on factors such as vibration, humidity, and/or minimum and maximum temperatures reached during transit for items such as food [32]. For example, using smart thermometers, a purchaser of salmon could know that the fish was kept at safe temperatures throughout the trip. Using RFID scanners, logistics companies could be immediately notified if a shipment was loaded into the wrong container. The use of IoT devices increases the information coverage and reduces the window for inputting false information that would not line up with previous or subsequent records.

Given the vast applications for IoT objects (e.g., GPS-enabled vehicles/ships, RFID tags, smart thermostats, surveillance, etc.), logistics use cases are one of the most promising applications for IoT and blockchain technology [36,49].

An interoperable network with interconnected IoT nodes would generate massive amounts of time-varying, polymorphic data, which would provide near real-time records. This would reduce the time delay between data capture and decision making thereby increasing agility and responsiveness in the supply chain [24]. The use of IoT would also enable remote management of supply chain processes as managers could be able to rely on timely information and react accordingly from their interface [25].

These IoT applications are further enhanced when integrated with blockchain technology. Smart contracts can access relevant records and events from IoT devices/nodes and autonomously take actions with executable code. In an interoperable network of DRSMs, a smart contract could be triggered to mark goods as received when a location sensor reports that the goods have reached their destination. The smart contract could further adjust subsequent schedules and arrival times accordingly and trigger re-routing needs if necessary. Contractual penalties from delays could also be enforced with the executable code of a smart contract.

Interoperability would improve the records handling of IoT devices to enable harmonized synchronic tracking and support complete supply chain visibility; records would be tamper-evident, and fraudulent actions could be prevented.

3.4. Analytics

Traditionally, data analytics has been a manual process of teams of statisticians, analysts, and data modellers exploiting data to gain a competitive advantage [50]. IoT and Industry 4.0 have led to the emergence of big data business analytics in the supply chain which facilitates the exploitation of data to gain a competitive advantage [21,51]. However, big data are too large to process manually. Increased computing power and applicable algorithms have introduced increased efficiencies and new capabilities in processing big data, enabling companies in nearly every industry to use data analytics [52]. Data analytical schemes include statistical modelling, data visualization, machine learning, and data mining which provide competitive insights when managing supply chains.

Many companies already use data analytics, especially in the downstream supply chain when the items reach the retailer, consumers, and the end of the item's life cycle [12]. Ref. [53] argue that while big data analytics have been used towards the end of the supply chain to gain customer insights, the use of data analytics, logistics and supply chain management (LCSM) in operations is less understood. LSCM is complex, involving a large amount of constantly changing factors that introduce the risk of wastage, inefficiencies, delays, increased fuel costs, inconsistent/unreliable actors, and ever-increasing consumer expectations [19]. Interoperable DRSs in LSCM would make data from LSCM records more easily accessible to stakeholders for analytics.

While data analytics could help reduce the negative effects of logistics and supply chain disruptions, an automated supply chain using analytics capabilities coupled with self-executing smart contracts and IoT would reduce the instances of disruptions themselves [54]. With minimum human intervention, a highly automated supply chain would make faster decisions and consider more information in the decision process than manual or hybrid semi-manual processes. The increased speeds and information processing abilities push the limits of flexibility and agility in SCM [55].

Analytics, IoT, and smart contracts could enable an autonomous, predictive, and prescriptive supply chain with decreased costs, increased efficiencies, increased visibility supporting fraud detection, and streamlined due diligence tasks [55]. This would improve the management of demand volatility, cost fluctuations, procurement, supply chain network design, inventory, and logistics [21].

However, the output of an analytics system is only as good as its input, and the accuracy of records is a potential issue. In the field of SCM, big data for predictive analytics are known to often contain errors [56,57]. Data quality, which depends on its completeness and accuracy is critical for SCM analytics and is required to increase the value-added from decision-making practices [58]. Without data quality, the reliability of the output is called into question [58]. In a recent survey of more than 3000 business executives, one in five executives identified issues with data quality as a primary barrier to adopting more advanced analytics strategies [59].

Additionally, poor data quality in records can have a direct, negative impact on business decisions [60,61], and has been linked to business losses [62]. Poor data quality has been estimated to cost a typical organization revenues of 8% to 12% and can constitute 40% to 60% of a service provider's expenses [63]. This translates to billions in losses per year [57].

Data quality is represented consistently in the Management Information Systems literature by four dimensions which are critical for analytics: completeness, timeliness, accuracy and consistency [57,62,64–68].

Completeness refers to a record having all the information captured [69], e.g., a billing address should have all items required by the system, including any variables not required for the task at hand as they may be critical variables when the record is used or verified later [57]. Incomplete or missing records, such as any form of missing data in analytics, can have significant impacts on data analysis and the accuracy and reliability of information derived from analytics. As a control measure, the ISO recommends that records should be created at the time of the event which it represents or soon after [2].

The use of verifiable credentials and DIDs could particularly help alleviate completeness issues as the information would be digitally exchanged. Furthermore, information could be automatically exchanged when programmed into an automated smart contract. With minimal human intervention, the information about the object would be automatically uploaded, reducing opportunities for human mistakes that lead to incomplete records.

Timeliness refers to the records being up to date, which, for example, is critical when processing records for supply chain inventories [57]. IoT would support continuous monitoring by analyzing a quintillion of IoT-generated bytes representing immediate inputs of events occurring in the supply chain [55]. For example, as objects with RFIDs travel through the supply chain, their movement and associated events would be tracked instantly as the RFIDs communicate with IoT nodes throughout the supply chain. It would also predict and identify risks by considering more data than is manually possible to process, creating more agility and responsiveness in complex, unstable environments [55].

Accuracy reflects the degree to which the data represent the "real" corresponding values [64]. In the countdown to Y2K, for example, accuracy was challenged as the year value was represented using only the last two digits of the year, which would soon no longer accurately reflect the year. In the 1990s, issues started to arise including someone receiving a $91,250 fine for a 100-year overdue video rental [70]. In addition to properly representing the real value, records in two systems must match in terms of content.

In SCM, record accuracy is an issue [58], and low levels of accuracy can lead to unreliable analytics outputs and challenges with data cleaning. However, the tamper-evident nature of a DRS and the consistent monitoring enabled through the use of IoT can help increase the reliability, thus securing the accuracy of data by automatically identifying any inputs that are inconsistent with the item's records. For example, the weight of an item should be the same when leaving the manufacturing facility as when recorded in the billing system, and when recorded at customs. By having an interoperable DRS, mismatched entries could be automatically corrected for improved data quality in analytics. Analytics that are integrated into self-executing smart contracts in a DRS could also identify an overproduction of goods for the number of raw materials a manufacturing facility receives, enabling the detection of fraudulent activities in markets that value authenticity or rare goods.

Consistency denotes the degree to which the format and data structure match in related records [57]. In [64]'s words, it is when the "representation of the data value is the same in all cases" (p. 153). Ref. [62] go further and divide consistency into intra-relation and inter-relation constraints. Intra-relation consistency is achieved when the values in a record fall within the range of possible values, while inter-relation is achieved when data in related records are presented with the same structure. For example, a date of enrolment for a new university program should fall within the possible range of years the program was available (e.g., 2019–2021) (intra-relational constraint), and the data should be recorded in the format that matches the format of other dates in the system (e.g., dd/mm/yyyy) (inter-relation constraint).

Heterogeneous data have always been one of the challenges of big data analytics [21]. The lack of data format harmonization in SCM reflects the consistency issue and remains an issue in the technological component of data analytics. Increasing interoperability using a DRSM would allow systems to communicate with one another to maintain completeness, timeliness, accuracy, and consistency.

3.5. Finances

Currently, the fragmented network of supply chains enables the existence of weak areas of governance across smaller and informal actors in the supply chain. This creates entry points for illicit sources of goods, finance, and logistical support for supply chain operations [24]. Illicit activity extends to tax evasion, price-fixing, smuggling, and fraudulent insurance claims—67% of which go undetected in the diamond industry for example [24,40].

Using the capabilities of the previously discussed technology layers, blockchain-based DRSs might promote fair payment, financial inclusion, and efficiency in the transaction processes by connecting stakeholders using smart contracts and mobile payment services. Additionally, a network of blockchain-based digital identities would formalize the supply chain actors—an important factor in reducing financial risk. Smaller players would, ideally, join multi-stakeholder initiatives rather than duplicating technology efforts. Using smart contracts, the increased automation and efficiency would free up capital previously used in siloed SCM records systems solutions.

The increased authenticity, reliability, integrity and usability of records introduced by DRSs would also support traceable supply chain finance (SCF) and trade credit insurance. SCF, a promising new financial product, is a set of technology-based processes for business and financing which allow financiers to fund organizations through their supply chain operations [33]. SCF enables actors to optimize working capital and generate additional operating cash while minimizing their financial exposure. It also allows for reduced inventories and faster payment processing.

Trade credit insurance is a common risk mitigation instrument and an often-required component of obtaining financing [71]. Trade credit insurance (also known as credit insurance or accounts receivable insurance) can be domestic or international and protects suppliers and their receivables from credit risks, including the non-payment of invoices.

In emerging markets, over 50% of micro, small and medium enterprise (MSME) trade financing requests are rejected by banks, and over 70% do not have alternative financing options [33]. This acts as a barrier to MSMEs, and as such, drives the market for illicit supply chain financing alternatives [24,33]. MSMEs create the majority of employment opportunities (70–90%) in emerging economies, up to 40% of the GDP in developing markets, and up to 60% of global total employment [33]. However, the financing gap for SMEs is estimated at US $4.7 trillion globally [33]. Innovative SCF solutions offer a powerful tool for SME buyers, suppliers, and financiers to overcome this funding gap [72].

A primary adoption barrier to SCF programs in global supply chains is the lack of trust and transparency [72] for which blockchain-based DRSs could provide a solution. Blockchain technology enables real-time, transparent, reliable, authentic, tamper-evident records (e.g., regarding proof of order, sale, and payment verification). SCF participants could also maintain an immutable set of records and contracts hosting agreed-upon prices [72]. Furthermore, using blockchain-based DRSs, records could be transmitted in real-time allowing stakeholders to maximize the benefits of SCF and easily take advantage of early payment discounts and credit arbitrage opportunities [72].

Smart contracts could alleviate some risks for the insurer, financer, and supplier as the self-executable code would protect suppliers from inappropriately withheld payments. However, if the funds are not available, the smart contracts would not be able to complete the transaction. Therefore, trade credit insurance would still be a very relevant actor in the supply chain. Data analytics and end-to-end transparency would benefit insurance providers by providing more accurate, reliable, near-to-real-time information on the actors and businesses and circumstances involved, enabling them to make more informed decisions.

3.6. Privacy and Confidentiality

To reduce fraudulent activity in SCM, an open DRS solution is based on the principle of maximum transparency for all stakeholders. However, commercial and regulatory requirements necessitate some level of privacy and confidentiality. Companies may not want to disclose the details of their operations to their competitors and privacy legislation, such as the European Union's General Data Protection Regulations has introduced strict privacy regulations that apply to personal data (i.e., small business owners, farmers, etc.) [24].

Regardless of the technology used, records and trade secrets can still be leaked from DRSs. For instance, in any system, buyers can leak the prices or contract parameters of a particular seller [18]. Technical solutions need to address such human-centric vulnerabilities as well as technology-specific vulnerabilities, as the way that data are stored in distributed systems is fundamentally different from how they is stored with other technologies [73]. Many blockchain projects are incorporating smart contracts to enable business process automation and zero-knowledge proofs to manage privacy [19]. Most companies working on privacy solutions are using encrypted transactions and data silos to keep information private while maintaining the needed transparency in the supply chain. Zcash, for example, has created a wallet that uses zero-knowledge proofs to maintain privacy during transactions [74].

The use of IoT needs to be considered in relation to privacy as well. While the use of IoT creates value by collecting massive amounts of data, big data collection has always posed privacy risks [75–77]. It is also challenging to manage the scattered but widely connected nature of an IoT network; any security breach could affect the entire network.

By using blockchain technology, DRSs could balance the necessary yet conflicting privacy, confidentiality, communication, and transparency needs. Blockchain technology provides a platform with assured transparency among a community of collaborating entities. It enables Proof of Existence (PoE) functionalities including time stamping, document integrity verification, and record ownership credentials to assert some information about a record without having to reveal all the information contained in the record. It can also further support privacy functions in multi-stakeholder agreements, allowing multiple parties to contribute their encrypted input to the computing function in a privacy-preserving mode.

Additionally, with the use of Verifiable Credentials in the context of Self-Sovereign Identity (SSI) systems, SSIs could introduce governance over one's own data, allowing users to decide what data they wish to disclose. The use of SSIs in DLT-based DRSs is a fundamentally different approach to privacy than Ann Cavoukian's Privacy by Design which still depends on data stewards, and the ethical processing of personal data. With SSIs, the ownership, control, and decision-making regarding the disclosure of records are shifted to the person that the data are about [78].

4. Business Implications of Improved Emerging Technology Layers

By using interoperable DRSs across the technology layers of SCM, reduced inefficiencies, reduced costs, better forecasting consumer needs, and fostering better business practices could be achieved.

4.1. Inefficiencies

Smart contracts can reduce inefficiencies by introducing automation and reducing opportunities for human error or fraud, using IoT-driven real-time information, and by streamlining regulatory, compliance, reporting, and due diligence tasks [26,79]. Complementing the technological efficiencies, the increased alignment in policy and guidelines can streamline regulatory compliance processes for businesses and governments [24].

4.2. Costs

Cost savings can be found as a result of reduced inefficiencies and streamlined processes enabled by smart contracts [24,80]. The integration of IoT can help introduce preventative measures with real-time tracking to reduce costly damages incurred as a result of mistakes or unforeseen problems in the supply chain. Smart contracts will additionally reduce the number of intermediaries in the supply chain [79,80].

Reliable records sharing in supply chains also introduces potential cost savings. While many businesses may want to keep advantageous information private, decentralized identifiers and VCs can enable the sharing of records without disclosing all data elements of transaction records. Businesses having access to reliable data otherwise previously not within their scope can reduce supply chain costs, the "bullwhip effect", and result in profitable advantages [81–83]. These cost savings can enable more investment in capital improvements as a result of freeing up capital previously used in siloed SCM operations [24].

4.3. Consumer needs

The increased transparency and traceability enabled by DRSs would satisfy consumer trends in wanting to know the provenance of products. The provenance-tracking capabilities would benefit industries competing with fake goods in markets where the authenticity of rare materials, organic and fair-trade features, contribute a significant competitive advantage [80].

Pharmaceuticals are one area that has struggled with the introduction of counterfeit products in the supply chain for some time. Counterfeit pharmaceuticals pose a risk to public safety and undermine the trust in regulators and manufacturers which has been particularly felt during the current COVID-19 pandemic [84]. COVID-19 has seen the opportunistic bulk purchasing and reselling of certain goods resulting in shortages (e.g., toilet paper and sanitizer), Interpol has identified a rise in fake medical products [85], the US Food and Drug Administration (FDA) has warned the public of potential counterfeit COVID-19 vaccines [86] which have already been identified in Russia and Ecuador [84]. A traceable supply chain that could prove item provenance, authenticity, and integrity would increase consumer confidence.

4.4. Better Business Practices

A holistic distributed solution will be enhanced by the multi-stakeholder cooperation involved in creating the standards of responsible business conduct (RBC), rules, protocols, and governance for the system [24].

5. Gaps

To achieve interoperability across DRSs, there are a few notable areas that particularly need support to make the transition. These areas include:

1. *The cooperation of stakeholders in an area that has traditionally conformed to the needs of larger stakeholders.* The World Economic Forum has built a multi-stakeholder community to

design a framework to support decisions involving inclusivity, interoperability, and integrity [4].

2. *The development of a governance model to ensure the credibility of records inputted into the blockchain.* A DRS only ensures the integrity of the records in the distributed ledger but does not prevent dishonest or inaccurate information from being inputted.
3. *The integration of stakeholders into existing DLT efforts rather than duplicating efforts.* This is particularly important for smaller stakeholders.
4. *Technology adoption by laggards.* For example, farmers or remote suppliers of raw materials have not adopted much technology in their processes. Addressing the reasons for this, whether related to access to technology or digital literacy will be important.
5. *Accurately and officially identifying actors and records in the supply chain.* Currently, there exist many unofficial actors that need to be integrated using standardized digital identifiers.
6. *The threat of quantum computing.* Quantum computing poses a real threat to the security of information stored in any network of interoperable supply chains that relies upon cryptography for security. Specifically, it poses a threat to public-key cryptographic algorithms which are a key component of the cryptographic architecture of blockchain. This poses a threat to the private keys which control a user's digital identity and associated credentials [19]. It should be noted that quantum computing poses a threat to all web-based systems, not just blockchain, and quantum-safe blockchains are under development [87,88].
7. *Blockchain technology limitations.* DLT and blockchain technology are not immune to the interoperability challenge facing SCM.
8. *Standardization is needed to make interoperability possible.* Standardization has already been recognized as a needed factor in the proliferation of blockchain [89], and efforts have been made in their development by the International Standards Organization (ISO), as well as industry groups including the Blockchain in Transportation Alliance (BITA), W3C, the Digital Container Shipping Association (DCSA), and the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT). Work in standardization that still needs attention includes:

    a. clarifying the unclear legal implications of smart contracts and creating universally agreeable implications [90];
    b. data harmonization by establishing standard data formats;
    c. standardizing protocols and technological components to support interoperability of all technologies;
    d. collaboratively establishing an overarching governance model for the distributed systems;
    e. creating a plan for managing false or inaccurate records entered in the immutable ledger and establishing configuration plans;
    f. identifying solutions for identifying and implementing solutions to compliance with international privacy, data localization and encryption laws;
    g. long-term technology plans to manage the relevancy, compatibility, and security of IoT equipment;
    h. strategies for addressing retention, disposition and long-term preservation of blockchain-based records.

There are also technology gaps amongst the technology layers which are broken down, next, by technology layer.

5.1. Technology-Based Gaps: Events

Weak areas in the events technology layer are centred around the limitations of DLT and blockchain technology, for which there are active research and industry efforts. Notable issues include the following.

1. *Consensus mechanisms.* Some consensus mechanisms, primarily proof of work, have performance challenges, mainly the block size and block frequency, which cause latency [91] This impedes increasing throughput, as increasing the block size to increase throughput causes propagation delays across the network. Additionally, there can be a lag in blockchain transactions, between the time a block is approved and made available to the entire network. Both of these issues cause a negative security risk, as long delays make the blockchain vulnerable to forks and double-spending attacks [91]. Chain splits are a potential disruptive problem facing a blockchain-based system (i.e., Ethereum and Ethereum Classic) [19]. If this happens, the smart contracts will be duplicated onto both chains and actors will have to monitor both for a period resulting in confusion about the reliability and authenticity of records and inefficiencies in managing events. Existing Layer 2 solutions include sidechains, state channels and plasma frameworks [92]. However, these do not address the underlying issue of consensus mechanisms. Furthermore, (1) side chains are responsible for their own security, (2) state channels move state-modifying operations (critical to SCM and the tracking of state changes) off-chain, and (3) the plasma framework periodically broadcasts their commitments to the root chain [92,93], which undermine the reliability of state-machine technology whereby only one state can exist at a time. To reduce the risk of chain splits and latency, more efficient consensus mechanisms need to be explored and adopted. Various consensus mechanisms already exist, such as proof of stake, delegated proof of stake, proof of elapsed time, proof of importance, proof of capacity, proof of authority, and consensus as a service (CaaS). Different tasks have different requirements for speed and security. A complex architecture of chains, their consensus mechanisms and their network capacity will need to be designed to increase the effectiveness of the entire network.
2. *Latency and throughput*. Some consensus mechanisms, primarily proof of work, have performance challenges, mainly the block size and block frequency, which cause latency [91]. This impedes increasing throughput, as increasing the block size to increase throughput causes propagation delays across the network. Additionally, there can be a lag in blockchain transactions, between the time a block is approved and made available to the entire network. Both of these issues cause a negative security risk, as the long delays make the blockchain vulnerable to forks and double-spending attacks [91].
3. *Overlap.* To help manage a large architecture with several overlapping processes, blockchains and networks, data-driven state machine technology should be incorporated. State machine technology is an abstract mathematical model of a process. The process can only exist in one state at a time and moving between states is called transitioning. This gives the governing bodies flexibility in system applications without having to create, test or deploy new code. A system is needed that supports multiple state machines and can be extended with new ones.
4. *Complexity.* Data-driven workflows should be developed to help manage the complexity of SCM. In data-driven workflows, workflows are represented using data, meaning users do not need to modify, test and support new code to add more workflows. They just add data. This is a unique feature in the decentralized platform marketplace.
5. *Blockchain resilience.* Blockchain resilience can also pose a challenge in the far future if it is decommissioned. Centralized systems can easily be constructed and deconstructed [19]. With blockchain, however, due to its decentralized nature, there is the possibility that it never completely shuts down [19]. This is especially true with large-scale blockchains made up of millions of nodes. A terminated blockchain is susceptible to an attack whereby a malicious user overpowers the remaining active nodes to replace the blocks or create a significant fork [19]. Therefore, a defunct blockchain ledger is not a reliable source of historical information needed for, i.e., auditing, data analysis, etc., and may pose future security and compliance risks.

5.2. Technology-Based Gaps: Digital Identities

Much work still needs to be carried out in the digital identity space, as outlined below.

1. *Verifiable credentials.* W3C VCs will need to be developed. SSIs are the only identity system to support VCs.
2. *Digital wallets.* To interact with a DRS, users need to hold a private key. Currently, existing digital wallets are not purpose-built wallets; they do not provide necessary advanced features because they do not have the context of how the user would interact with them. Usable wallets for SCM records systems need to be developed and should incorporate several technical components not used by other wallets including biometric identifiers for self-employed agents and contractors, cloud agents, QR code scanning, contextual user interface, credential rendering, blockchain public key, backup, device syncing, and personas—especially for logistics companies that offer several services throughout the supply chain. For enterprises, cloud services will need to be developed to provide the equivalent of digital wallets to meet organizational needs.
3. *Onboarding.* A secure onboarding system needs to be developed. It will require reliable sources of real-world identity verification to securely and reliably onboard actors into their digital identities and a system to evaluate the reliability of different sources and combinations of information sources [94]. Once real-world identities are authenticated, storing and mapping relationships will need to be developed between the proven identities and the digital identity [95].
4. *Quantum threat.* Quantum-resistant algorithms need to be considered for the cryptography used in the system to ensure the security of digital identities [19]. Hybrid quantum-resistant algorithms should be considered in the interim until quantum-resistant algorithms are ready so that ledger records are protected both from future and present threats.

5.3. Technology-Based Gaps: IoT

IoT objects are already heavily used in SCM and are very effective. However, there are still some gaps between the current state and the future state. Among the gaps which we have identified, a survey of the Biggest Opportunities and Challenges of IoT-Enabled Products and Services showed that 51.3% of IoT implementers identified costs as being their top concern, followed by data analytics (48.1%), safety (47.5%), and framework integration (43.8%) [32].

1. *Cost.* The costs reflect two components. The increased generation of records is costly to manage. IoT networks need to support many messages (communications costs), distributed device-generated data (storage costs), processing, and analysis of the data (server costs). In addition to the increased processing and storage requirements, there is also the cost of managing a vast distribution of what will eventually be outdated equipment (IoT devices).
2. *Analytics.* The IoT analytics concern is a result of the distributed and fractured nature of the records. The IoT network for the supply chain is made of large amounts of fragmented information. While this allows for the sale of specific valuable information, it adds challenges to collecting complete and accurate information [32]. In addition to being fragmented, much of the data are heterogeneous; another challenge for analytics [52]. This further supports the need for a supply chain enabled by DLTs with harmonized data formats. Additionally, redundancy is another challenge facing analytics, as the overlapping networks will result in temporal and spatial redundancies which can introduce inconsistencies and biases [52].
3. *Privacy and security issues.* Privacy and security issues in the IoT space commonly stem from the simplicity of the functions in IoT objects which are unable to support robust cryptographic algorithms and security functions [25]. The Modum.io AG pilot project, for instance, found notable issues and concluded that going forward, data

in IoT sensors need to be secured with cryptographic signatures or access control mechanisms [40].

4. *Framework integration.* The framework integration concern reflects the complex process of coordinating all the existing IoT objects due to their simple functions and coexistence of multiple protocols [32]. Existing IoT interfaces and protocols are diverse and inconsistent across, e.g., data model standards, hardware protocols, network protocols, sensors, and equipment connection standards, platform standards, and third-party service providers. A single blockchain or IoT platform cannot connect to the equipment of all manufacturers [32]. As a result, a complex architecture, with adequate bandwidths able to support the consistent flow of data between all of the networks without bottlenecks needs to be developed [52].
5. *Adoption.* While IoT objects are regarded as ubiquitous, there are still gaps in the supply chain, especially among smaller organizations. The implementation of a DRS-based supply chain may pose additional barriers for some remote producers of raw materials who do not have consistent connectivity. Adoption efforts are still needed in these areas.
6. *Managing fragmented data.* The fragmented nature of the information collected by IoT devices will be aggravated with overlapping interoperable networks. To prevent data redundancies, data formalized digital identities and data harmonization will need to be implemented into DRSs.
7. *Oracles.* Oracles reintroduce the concept of centralization and trusted third parties and are thus seen as a "problem" [35,96]. Decentralized alternative approaches still need to be identified and adopted.

5.4. Technology-Based Gaps: Analytics

Data analytics is an area with strong technological innovation. However, when applied to the supply chain, it is limited by the complexity of the supply chain. A significant challenge is that a lot of data are redundant and heterogeneous, creating biases and extensive data cleaning work in data analytics. As with IoT, going forward, data format harmonization needs to be implemented.

5.5. Technology-Based Gaps: Finances

Many of the financing capabilities of blockchain technology have been ironed out as financial transactions have been a primary focus in blockchain research and development. Challenges facing SCF center more around the complexity of implementing SCF in global supply chains including onboarding suppliers and aligning incentives [26,72]. However, the shared nature of the benefits of a holistic solution introduces the challenges of how to share the cost across the stakeholders equitably and convince stakeholders to invest in infrastructure to support it. This is made more complex by the fact that some stakeholders particularly benefit more than others from the system [24].

5.6. Technology-Based Gaps: Privacy and Confidentiality

Privacy gaps centre mostly on encryption, and are as follows.

1. *Cryptographic solutions.* To address privacy concerns, attention needs to be given to cryptographic solutions [19]. This includes zero-knowledge proofs (ZKPs), group signatures, multi-party computation, and homomorphic encryption. However, these are still in the early phases of implementation and have no real-world, large-scale applications as of yet.

A ZKP allows a party to assert some information about some data without having to reveal the data. Data structures that support ZKP for data need to be constructed, and algorithms to generate them need to be implemented. The data model, algorithms, and code would ideally be open-source so that they could be trusted to generate the correct ZKP results. Without ZKP, if multiple parties contribute their respective inputs to a single records system, they would have to reveal their inputs. With ZKP, the privacy of data is guaranteed while their commitments are audited [19].

Another cryptographic primitive to assist with the confidentiality of data in public/consortium blockchains is homomorphic encryption. The data could be constructed in such a way that they can be encrypted for use outside of the originating company, and one could use that encrypted data without having to first decrypt it. This is often used for anonymized access to medical data for analysis by third parties. Homomorphic encryption is designed in such a way that certain operations on the input translate into analogous operations on the output. Hence, one could apply those operations on the encrypted information which simply corresponds to the operations on the decrypted information.

2. *Group signatures.* A group signature scheme is also needed in the supply chain since many parties are often involved. Group signatures are a method for allowing members to sign automatically on behalf of the group. A related cryptographic primitive is called secure multi-party computation (MPC) that allows multiple parties to contribute their encrypted input to the computing function in a privacy-preserving mode. In other words, the respective inputs are never observed in unencrypted form outside of their origin and yet they can be used in computation to obtain the combined score.

Integrity assertion by a group of entities is another cryptographic primitive that can be used in this setting. There are several classes of signature protocols that provide enhanced capabilities for integrity in a variety of situations. For example, they could allow for digital signature integrity without revealing who the signing parties are. This could be used to ensure integrity on data made available on the public/consortium blockchains while keeping the originator of the data confidential. The approach could be combined with a threshold scheme whereby any k out of m parties could produce a valid signature.

3. *Explore alternatives.* Finally, architectures that store fewer data on the chain could be more secure as vulnerabilities could be discovered in the authentication and messaging protocols used in data transmission across the network [19].

6. Conclusions

Supply chains are highly complex and dynamic and, as a result, there are many ongoing efforts to improve SCM. The complexity, and siloed nature of SCM reduces the transparency, traceability and reliability of records, and thus any research or solutions are only as good as the records used to manage the business activities in the supply chain. Until records systems are connected by digital highways and are able to communicate authoritative records with each other, they will remain digital islands, limited to their own technological capabilities. The full potential of SCM solutions and operations cannot be reached without trustworthy records. Thus, interoperability, transparency, traceability, and integrity and authenticity of records need to be embedded in the future state.

This review article provides a survey of the current state of practice, a proposed future state, and a gap analysis. By summarizing the current state of existing literature, review papers enable readers to grasp the existing knowledge on a topic without having to search for, sort, and read all the published works in that field [7]. The focus of the literature reviewed in this review article is less theoretical and more practical with an emphasis on supply chain issues, blockchain capabilities and proposed capabilities, and potential gaps. We believe we have accurately captured the literature, presented it from the perspective of the six technology layers that we identified and additionally tied it to the International Standards Organization's definition and requirements for records.

Our proposed future state of SCM, being an interoperable global network of Decentralized Records Systems (DRS), will leverage several emerging technology layers (ID management, IoT, analytics, event management, finance, and privacy) to create a holistic solution. Using blockchain technology will further enable provenance, traceability, transparency, privacy, supply chain finance, trade credit insurance, and reliability of the information. However, without interoperability, the information is fragmented, and the full capabilities of the technology cannot be achieved. Interoperability across DRSs and ICTs would support end-to-end supply chain visibility, greater provenance, further deter fraud and financial discrepancies, increase efficiencies and responsiveness, simplify due diligence processes and reporting, reduce errors and costs, and improve analytics.

Our survey of the existing literature and future state were then used to conduct a gap analysis between the current state and "what ought to be". The gap analysis identifies several future research directions to overcome overarching and technical gaps which apply not only to our proposed future state, but to many fractional DLT-based SCM solutions. Major technological gaps that need to be addressed include the development of digital identities and verifiable credentials and creating a network architecture that manages network capacity and throughput. Key factors in fostering interoperability in standardization include the standardization of processes, protocols, transactions, and data formats. Importantly, collective efforts and cross-boundary (cross-industry, cross-border, etc.) efforts will be needed to create long-term solutions that can be accepted globally.

Limitations of this review article stem from any discrepancies between the actual state of practice and what has been published and presented to the public; any projects that have not been disclosed to the public were not included in our survey. However, several projects which were included still face significant gaps with regards to the current state of the technology before their proposed solution can be executed beyond pilot settings.

Author Contributions: Conceptualization, A.H. and A.M.; methodology, A.H.; validation, A.M.; formal analysis, A.H. and A.M.; investigation, A.H. and A.M.; resources, A.M.; data curation, A.H.; writing—original draft preparation, A.H.; writing—review and editing, A.H. and A.M.; visualization, A.H.; supervision, A.M.; project administration, A.M.; funding acquisition, A.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded, in part, through a generous contribution from Mavennet Inc., a Toronto-based blockchain development firm, and the National Research Council of Canada under the Industrial Research Assistance Program. The APC was funded by the Natural Sciences and Engineering Research Council of Canada (NSERC) under the Discovery Grant (RGPIN-2019-06150, PI: Atefeh Mashatan).

Acknowledgments: The authors would like to sincerely thank Victoria Lemieux, Guest Editor, for her guidance and valuable feedback, as well as anonymous reviewers for their insightful suggestions, which helped the authors to greatly improve the paper. Ryerson University is in the "Dish With One Spoon Territory". The Dish With One Spoon is a treaty between the Anishinaabe, Mississaugas and Haudenosaunee that bound them to share the territory and protect the land. Subsequent Indigenous Nations and peoples, Europeans and all newcomers, have been invited into this treaty in the spirit of peace, friendship and respect. We thank them for allowing us to conduct research on their land.

Conflicts of Interest: The authors declare that they have no conflicts of interest.

Appendix A

Appendix A provides a brief overview of the DLT-based SCM initiatives identified and tabled in Section 2.3.

1. BiTA works with a standards committee and board to set industry standards for blockchain technology. In the supply chain IoT space, they have set some standards for data and metadata regarding location components, i.e., with GPS and IoT units.
2. Everledger offers a fraud detection ledger for diamonds which can be verified by insurance companies, law enforcement, and buyers to verify the provenance of the diamond. The increased visibility could be used to detect and deter fraudulent insurance claims.
3. Modum's MODlink gives the entire supply chain a way to share trusted events by joining data silos without exposing private data and is connected to existing infrastructure without intrusion. Their MODsense is an automated way of collecting, assessing, and reporting conditions of sensitive goods through the supply chain while

tracking their location and reducing operational costs. Using analytics can grasp the root-cause of problems, reduce costs and limit risks.

4. Mojix provides supply chain subcontracting and has integrated many RFID and IoT technologies to provide real-time location tracking which increases traceability, monitors proper transportation of goods, and detects errors early.
5. OrgBook BC uses VON to verify that an organization is registered to conduct business in BC as a corporation.
6. Scantrust provides secure QR codes which act as digital identities in the supply chain once printed onto the packaging of goods and "activated". Their QR codes act as SCM tags and enable the collection of data and attributes of each product on a unit-level. The SCM tags are used for automated alerts for recalls, or "sell by" dates. Scantrust provides a Business Intelligence Dashboard, showing stakeholders end-to-end visibility into the supply chain. Google Analytics is also integrated to provide consumer information associated with the goods.
7. SKUChain tracks raw materials through the supply chain and has worked with the mining industry to track conflict minerals to the mines to provide a provable clean supply chain with traceable financial events.
8. SustainBlock uses encrypted transactions to store relevant information on the blockchain and track the provenance of raw materials originating from conflict and high-risk areas (e.g., conflict minerals to the retail store). They have carried out a proof-of-concept project with a mine in Rwanda in 2019 which traces conflict minerals and establishes data acceptance criteria including sovereignty, quality, and relevance of data in the supply chain.
9. Things Lab uses smart card tracking IDs to prevent the introduction of counterfeit items into the supply chain. However, they identify batch production which can still be susceptible to the introduction of counterfeit productions and double-spend problems within the batch.
10. TradeLens coordinates customs agencies, government planners, and financial service providers for large shipping concerns. TradeLens tracks every detail, even throughout the shipping portion of the supply chain. By tracking all the events, stakeholders can have more control over the shipment and the increased visibility of all minute events reduces the window to double-spend. It provides an audit trail for the entire shipping life cycle in the supply chain. Stakeholders can obtain access to key shipping data throughout the shipping process which can be used with AI to improve operational efficiencies. This includes timeline changes, impacted by vessel changes, weather, and harbour issues.
11. Treum's service provides transparency, traceability, and tradability through tokenization. The added transparency is centred on preventing double-spend and ensuring authenticity for organic foods and valuable trade products such as historic jerseys. The tokenization is a useful feature towards the end of the product life cycle for goods with resale potential which can be co-owned and traded, where the continued authenticity and origin of the product is essential.
12. Unisot provides real-time tracking throughout the supply chain. Their Digital Twin and Product DNA solutions create digital representations of supply chain items enabling stakeholders to track and trace them quickly and securely, from origin to disposal.
13. WaltonChain relies on RFID technology to integrate information from IoT devices in the supply chain to provide full traceability [32]. These enable automation of the supply chain reducing human interference and better reliability of the events in the supply chain. This, combined with the tamper-proof record of the data, reduces the opportunity for double-spend and the introduction of counterfeits into the supply chain. They allow for child chains to be created to monitor logistics, warehousing, retail circulation, and production, which store and upload their own data to the parent chain for cross-chain queries.

14. Zcash enables transparent transactions for wallets and exchanges which do not support private transactions. They use zero-knowledge proofs to maintain privacy in transactions in a public blockchain.
15. ZenGo has created a wallet that uses threshold signatures. They create two secret shares. When the shares are combined it takes the role of the private key, making a password-less wallet.

References

1. Huang, S.H.; Sheoran, S.K.; Keskar, H. Computer-assisted supply chain configuration based on supply chain operations reference (SCOR) model. *Comput. Ind. Eng.* **2005**, *48*, 377–394. [CrossRef]
2. International Standards Organization. Information and documentation-Records management-part 1: Concepts and principles. *Int. Organ. Stand.* **2016**, 1–20.
3. Blossey, G.; Eisenhardt, J.; Hahn, G. Blockchain Technology in Supply Chain Management: An Application Perspective. In Proceedings of the 52nd Hawaii International Conference on System Sciences, Maui, HI, USA, 8–11 January 2019. [CrossRef]
4. World Economic Forum. Annual Report (2019–2020). WEF. 2019. Available online: http://www3.weforum.org/docs/WEF_Annual_Report_2019_2020.pdf (accessed on 13 July 2021).
5. Concordia University. Review vs. Research Articles. Available online: https://www.concordia.ca/library/guides/exercise-science/review-vs-research.html (accessed on 13 July 2021).
6. Kim, S.; Ji, Y. Gap Analysis. In *The International Encyclopedia of Strategic Communication*; John Wiley & Sons: Hoboken, NJ, USA, 2018; pp. 1–6.
7. McMahan, P.; McFarland, D.A. Creative Destruction: The Structural Consequences of Scientific Curation. *Am. Sociol. Rev.* **2021**, *86*, 341–376. [CrossRef]
8. Mineraud, J.; Mazhelis, O.; Su, X.; Tarkoma, S. A gap analysis of Internet-of-Things platforms. *Comput. Commun.* **2016**, *89*, 5–16. [CrossRef]
9. Scott, J.M.; Davis, F.; Csuti, B.; Noss, R.; Butterfield, B.; Groves, C.; Wright, R.G. Gap analysis: A geographic approach to protection of biological diversity. *Wildl. Monogr.* **1993**, *123*, 3–41.
10. Brown, S.W.; Swartz, T.A. A gap analysis of professional service quality. *J. Mark.* **1989**, *53*, 92–98. [CrossRef]
11. Geodis. Supply Chain Worldwide Survey. *White Pap.* 2017, pp. 1–36. Available online: https://geodis.com/fr//sites/default/files/2019-03/170509_GEODIS_WHITE-PAPER.PDF (accessed on 13 July 2021).
12. Dubey, R.; Gunasekaran, A.; Childe, S.J. Big data analytics capability in supply chain agility. *Manag. Decis.* **2019**, *57*, 2092–2112. [CrossRef]
13. Vescent, H.; Caballero, J. Sensors, Identifiers & Digital Twins Tracking Identity on the Supply Chain. The Purple Tornado. 2020. Available online: https://medium.com/in-present-tense/introducing-sensors-identifiers-digital-twins-556a22e42bbe (accessed on 13 July 2021).
14. Griffis, S.E.; Closs, D.J. Managing the Complexity Paradigm. 2017. Available online: http://www.apics.org/docs/default-source/default-document-library/final-bth-msu-white-paper.pdf?sfvrsn=e80612df_8 (accessed on 13 July 2021).
15. Dalvit, C.; De Marchi, M.; Cassandro, M. Genetic traceability of livestock products: A review. *Meat Sci.* **2007**, *77*, 437–449. [CrossRef] [PubMed]
16. McKean, J.D. The importance of traceability for public health and consumer protection. *Rev. Sci. Tech.-Off. Int. Epizoot.* **2001**, *20*, 363–371. [CrossRef]
17. Aung, M.M.; Chang, Y.S. Traceability in a food supply chain: Safety and quality perspectives. *Food Control.* **2014**, *39*, 172–184. [CrossRef]
18. Feng, Q.; He, D.; Zeadally, S.; Khan, M.K.; Kumar, N. A survey on privacy protection in blockchain system. *J. Netw. Comput. Appl.* **2019**, *126*, 45–58. [CrossRef]
19. Lesavre, L.; Varin, P.; Mell, P.; Davidson, M.; Shook, J. A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems. *NIST Cybersecur. White Pap.* **2019**. [CrossRef]
20. Green, J.S.; Daniels, S. *Digital Governance: Leading and Thriving in a World of Fast-changing Technologies*; Routledge: London, UK, 2019.
21. Wang, G.; Gunasekaran, A.; Ngai, E.W.; Papadopoulos, T. Big data analytics in logistics and supply chain management: Certain investigations for research and applications. *Int. J. Prod. Econ.* **2016**, *176*, 98–110. [CrossRef]
22. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://nakamotoinstitute.org/bitcoin/ (accessed on 13 July 2021).
23. Mitrovic, N.; Narayanan, A.; Asif, M.T.; Rauf, A.; Dauwels, J.; Jaillet, P. On centralized and decentralized architectures for traffic applications. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 1988–1997. [CrossRef]
24. OECD. Is There a Role for Blockchain in Responsible Supply Chains? 2019. Available online: https://mneguidelines.oecd.org/Is-there-a-role-for-blockchain-in-responsible-supply-chains.pdf (accessed on 13 July 2021).
25. Ben-Daya, M.; Hassini, E.; Bahroun, Z. Internet of things and supply chain management: A literature review. *Int. J. Prod. Res.* **2019**, *57*, 4719–4742. [CrossRef]

26. Banerjee, A. Blockchain Technology: Supply Chain Insights from ERP. *Adv. Comput.* **2018**, *111*, 69–98. [CrossRef]
27. Chang, Y.; Iakovou, E.; Shi, W. Blockchain in global supply chains and cross border trade: A critical synthesis of the state-of-the-art, challenges and opportunities. *Int. J. Prod. Res.* **2019**, *58*, 1–18. [CrossRef]
28. Wood, G. Polkadot: Vision for a Heterogeneous Multi-Chain Framework. White Paper. Available online: https://polkadot.network/PolkaDotPaper.pdf (accessed on 13 July 2021).
29. Kwon, J.; Buchman, E. Cosmos Whitepaper: A Network of Distributed Ledgers. White Paper. Available online: https://cosmos.network/resources/whitepaper (accessed on 13 July 2021).
30. TradeLens. Trade Made Easy. Available online: https://www.tradelens.com/ (accessed on 13 July 2021).
31. Unisot. Unisot. Available online: https://unisot.com/ (accessed on 13 July 2021).
32. WaltonChain. WaltonChain White Paper V.2. 2019. Available online: https://www.waltonchain.org/en/Uploads/2019-04-25/5cc171763aebb.pdf (accessed on 13 July 2021).
33. International Finance Corporation. *Supply Chain Finance Knowledge Guide*; International Finance Corporation: Washington, DC, USA, 2019; Available online: https://www.ifc.org/wps/wcm/connect/254277bc-86bd-420e-b390-94a13b19ca36/SCF+Knowledge+Guide+FINAL.pdf?MOD=AJPERES&CVID=mYOre4A (accessed on 13 July 2021).
34. Osipkov, I.; Vasserman, E.Y.; Hopper, N.; Kim, Y. Combating Double-Spending Using Cooperative P2P Systems. In Proceedings of the 27th International Conference on Distributed Computing Systems (ICDCS'07), Toronto, ON, Canada, 25–27 June 2007. [CrossRef]
35. Caldarelli, G. Understanding the Blockchain Oracle Problem: A Call for Action. *Information* **2020**, *11*, 509. [CrossRef]
36. Hackius, N.; Petersen, M. Blockchain in Logistics and Supply Chain: Trick or Treat? In Proceedings of the Hamburg International Conference of Logistics, Hamburg, Germany, 12–13 October 2017; Voulme 23, p. 3.
37. Pfizer. COVID-19 Vaccine U.S. Distribution Fact Sheet. Pfizer. November 2020. Available online: https://www.pfizer.com/news/hot-topics/covid_19_vaccine_u_s_distribution_fact_sheet (accessed on 13 July 2021).
38. Mohanta, B.K.; Panda, S.S.; Jena, D. An overview of smart contract and use cases in blockchain technology. In Proceedings of the 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bengaluru, India, 10–12 July 2018; pp. 1–4.
39. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, W.; Chen, X.; Weng, J.; Imran, M. An overview on smart contracts: Challenges, advances and platforms. *Future Gener. Comput. Syst.* **2020**, *105*, 475–491. [CrossRef]
40. Bocek, T.; Rodrigues, B.B.; Strasser, T.; Stiller, B. Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management, Lisbon, Portugal, 8–12 May 2017; pp. 772–777. [CrossRef]
41. Sedgwick, K. Zengo is a Keyless yet Noncustodial Bitcoin Wallet. 2020. Available online: https://news.bitcoin.com/zengo-keyless-noncustodial-bitcoin-wallet/ (accessed on 13 July 2021).
42. Hong, N. A security framework for the internet of things based on public key infrastructure. *AMR* **2013**, *671*, 3223–3226. [CrossRef]
43. Reed, D.; Sporny, M.; Longley, D.; Allen, C.; Grant, R.; Sabadello, M.; Holt, J. Decentralized Identifiers (DIDs) V1.0. W3C. 2020. Available online: https://www.w3.org/TR/did-core/ (accessed on 13 July 2021).
44. Alzahrani, B. An Information-Centric Networking Based Registry for Decentralized Identifiers and Verifiable Credentials. *IEEE Access* **2020**, *8*, 137198–137208. [CrossRef]
45. Barclay, I.; Radha, S.; Preece, A.; Taylor, I.; Nabrzyski, J. Certifying Provenance of Scientific Datasets with Self-sovereign Identity and Verifiable Credentials. *arXiv* **2020**, arXiv:2004.02796.
46. Toth, K.C.; Anderson-Priddy, A. Self-Sovereign Digital Identity: A Paradigm Shift for Identity. *IEEE Secur. Priv.* **2019**, *17*, 17–27. [CrossRef]
47. Saveen, A.; Radmehr, M. Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger. *IJRET* **2016**, *5*, 1–10.
48. Ellis, S.; Santagate, J.; Morris, H.D. IoT-Enabled Analytic Applications Revolutionize Supply Chain Planning and Execution. *White Pap.* **2015**, 1–13.
49. Zhang, H.-Y. (Ed.) *Fault Detection, Supervision and Safety of Technical Processes 2006: A Proceedings Volume from the 6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*; Elsevier: Amsterdam, The Netherlands, 2007.
50. Provost, F.; Fawcett, T. *Data Science for Business: What you Need to Know about Data Mining and Data-Analytic Thinking*; OReilly Media: Sebastopol, CA, USA, 2013.
51. Chen, H.; Chiang, R.H.L.; Storey, V.C. Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Q.* **2012**, *36*, 1165–1188. [CrossRef]
52. Dai, H.N.; Wang, H.; Xu, G.; Wan, J.; Imran, M. Big Data Analytics for Manufacturing Internet of Things: Opportunities, Challenges and Enabling Technologies. *Enterp. Inf. Syst.* **2019**, 1–14. [CrossRef]
53. Srinivasan, R.; Swink, M. An investigation of visibility and flexibility as complements to supply chain analytics: An organizational information processing theory perspective. *Prod. Oper. Manag.* **2017**. [CrossRef]
54. Gunasekaran, A.; Yusuf, Y.Y.; Adeleye, E.O.; Papadopoulos, T. Agile manufacturing practices: The role of big data and business analytics with multiple case studies. *Int. J. Prod. Res.* **2017**, *56*, 385–397. [CrossRef]
55. Calatayud, A.; Mangan, J.; Christopher, M. The self-thinking supply chain. *Supply Chain. Manag.* **2019**, *24*, 22–38. [CrossRef]
56. Dey, D.; Kumar, S. Reassessing data quality for information products. *Manag. Sci.* **2010**, *56*, 2316–2322. [CrossRef]

57. Hazen, B.T.; Boone, C.A.; Ezell, J.D.; Jones-Farmer, L.A. Data quality for data science, predictive analytics, and big data in supply chain management: An introduction to the problem and suggestions for research and applications. *Int. J. Prod. Econ.* **2014**, *154*, 72–80. [CrossRef]
58. Hofmann, E.; Rutschmann, E. Big data analytics and demand forecasting in supply chains: A conceptual analysis. *Int. J. Logist. Manag.* **2018**, *29*, 739–766. [CrossRef]
59. LaValle, S.; Lesser, E.; Shockley, R.; Hopkins, M.S.; Kruschwitz, N. Big data, analytics and the path from insights to value. *MIT sloan Manag. Rev.* **2011**, *52*, 21–32.
60. Dyson, R.G.; Foster, M.J. The relationship of participation and effectiveness in strategic planning. *Strateg. Manag. J.* **1982**, *3*, 77–88. [CrossRef]
61. Warth, J.; Kaiser, G.; Kügler, M. The impact of data quality and analytical capabilities on planning performance: Insights from the automotive industry. In Proceedings of the 10th International Conference on Wirtschaftsinformatik, Zurich, Switzerland, 16–18 February 2011; pp. 322–331.
62. Batini, C.; Cappiello, C.; Francalanci, C.; Maurino, A. Methodologies for data quality assessment and improvement. *ACM Comput. Surv. (CSUR)* **2009**, *41*, 1–52. [CrossRef]
63. Redman, T.C. The impact of poor data quality on the typical enterprise. *Commun. ACM* **1998**, *41*, 79–82. [CrossRef]
64. Ballou, D.P.; Pazer, H.L. Modeling data and process quality in multi-input, multi-output information systems. *Manag. Sci.* **1985**, *31*, 150–162. [CrossRef]
65. Haug, A.; Arlbjørn, J.S.; Pedersen, A. A classification model of ERP system data quality. *Ind. Manag. Data Syst.* **2009**, *109*, 1053–1068. [CrossRef]
66. Blake, R.; Mangiameli, P. The effects and interactions of data quality and problem complexity on classification. *J. Data Inf. Qual.* **2011**, *2*, 1–28. [CrossRef]
67. Lee, Y.W.; Strong, D.M.; Kahn, B.K.; Wang, R.Y. AIMQ: A methodology for information quality assessment. *Inf. Manag.* **2002**, *40*, 133–146. [CrossRef]
68. Wang, R.Y.; Strong, D.M. Beyond accuracy: What data quality means to data consumers. *J. Manag. Inf. Syst.* **1996**, *12*, 5–33. [CrossRef]
69. Gomes, P.; Farinha, J.; Trigueiros, M.J. A data quality metamodel extension to CWM. In Proceedings of the Fourth Asia-Pacific Conference on Conceptual Modelling, Ballarat, Australia, 2007, 1 January 2007; Volume 67, pp. 17–26.
70. BBC. Was Y2K Bug a Boost? BBC: Science and Nature. 4 January 2020. Available online: news.bbc.co.uk/2/hi/science/nature/590932.stm (accessed on 13 July 2021).
71. Valverde, R.; Talla, M. Risk Reduction of the Supply Chain Through Pooling Losses in Case of Bankruptcy of Suppliers Using the Black-Scholes-Merton Pricing Model, Some Recent Advances in Mathematics and Statistics. *World Sci.* **2013**. [CrossRef]
72. Huertas, J.; Liu, H.; Robinson, S. Eximchain: Supply Chain Finance solutions on a secured public, permissioned blockchain hybrid. *White Pap.* **2018**, 1–13.
73. Ma, C.; Kong, X.; Lan, Q.; Zhou, Z. The privacy protection mechanism of Hyperledger Fabric and its application in supply chain finance. *Cybersecurity* **2019**, *2*, 1–9. [CrossRef]
74. Zcash. How it Works. Available online: https://z.cash/technology/ (accessed on 13 July 2021).
75. Ahmed, E.; Yaqoob, I.; Hashem, I.A.T.; Khan, I.; Ahmed, A.I.A.; Imran, M.; Vasilakos, A.V. The role of big data analytics in Internet of Things. *Comput. Netw.* **2017**, *129*, 459–471. [CrossRef]
76. Asplund, M.; Nadjm-Tehrani, S. Attitudes and perceptions of IoT security in critical societal services. *IEEE Access* **2016**, *4*, 2130–2138. [CrossRef]
77. Zheng, S.; Apthorpe, N.; Chetty, M.; Feamster, N. User perceptions of smart home IoT privacy. In Proceedings of the ACM on Human-Computer Interaction, New York, NY, USA, 12–14 September 2018; pp. 1–20.
78. Cavoukian, A. *Privacy by Design in Law, Policy and Practice*; Office of the Information and Privacy Commissioner of Ontario: Toronto, ON, Canada, 2011.
79. Parker, T. *Smart Contracts: The Ultimate Guide to Blockchain Smart Contracts-Learn. How to Use Smart Contracts for. Cryptocurrency Exchange!* CreateSpace Independent Publishing Platform: North Charleston, SC, USA, 2016.
80. Boschi, A.A.; Borina, R.; Raimundob, J.C.; Batocchioa, A. An exploration of blockchain technology in supply chain management. In Proceedings of the 22nd Cambridge International Manufacturing Symposium, Cambridge, MA, USA, 27–28 September 2018. [CrossRef]
81. Schinle, M.; Erler, C.; Stork, W. Distributed Ledger Technology for the systematic Investigation and Reduction of Information Asymmetry in Collaborative Networks. In Proceedings of the 53rd Hawaii International Conference on System Sciences, Grand Wailea, HI, USA, 7–10 January 2020. [CrossRef]
82. Cachon, G.; Fisher, M. Supply Chain Inventory Management and the Value of Shared Information. *Manag. Sci.* **2000**, *46*, 1032–1048. [CrossRef]
83. Fiala, P. Information sharing in supply chains. *Omega* **2005**, *33*, 419–423. [CrossRef]
84. Jarrett, S.; Wilmansyah, T.; Bramanti, Y.; Alitamsar, H.; Alamsyah, D.; Krishnamurthy, K.R.; Pagliusi, S. The role of manufacturers in the implementation of global traceability standards in the supply chain to combat vaccine counterfeiting and enhance safety monitoring. *Vaccine* **2020**, *38*, 8318–8325. [CrossRef]

85. Interpol. Global Operation Sees a Rise in Fake Medical Products Related to COVID-19. Interpol. 2020. Available online: https://www.interpol.int/News-and-Events/News/2020/Global-operation-sees-a-rise-in-fake-medical-products-related-to-COVID-19 (accessed on 13 July 2021).
86. US Food and Drug Administration. Beware of Fraudulent Coronavirus Tests, Vaccines and Treatments. Consumer Updates. 2020. Available online: https://www.fda.gov/consumers/consumer-updates/beware-fraudulent-coronavirus-tests-vaccines-and-treatments (accessed on 13 July 2021).
87. Fernández-Caramés, T.M.; Fraga-Lamas, P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access* **2020**, *8*, 21091–21116. [CrossRef]
88. Kiktenko, E.O.; Pozhar, N.O.; Anufriev, M.N.; Trushechkin, A.S.; Yunusov, R.R.; Kurochkin, Y.V.; Fedorov, A.K. Quantum-secured blockchain. *Quantum Sci. Technol.* **2018**, *3*, 035004. [CrossRef]
89. O'Donnell, D. Why Engage with Standards? 2013. Available online: https://www.continuumloop.com/why-engage-with-standards/ (accessed on 13 July 2021).
90. Engelenburg, S.V.; Janssen, M.; Klievink, B. A Blockchain Architecture for Reducing the Bullwhip Effect. In *International Symposium on Business Modeling and Software Design*; Springer: Cham, Switzerland, 2018; pp. 69–82. [CrossRef]
91. Vukolić, M. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In *International Workshop on Open Problems in Network Security*; Springer: Cham, Switzerland, 2015; pp. 112–125. [CrossRef]
92. Mosse, P. Ethereum's Layer 2 Scaling Solutions. 29 November 2018. Available online: https://medium.com/datawallet-blog/ethereums-layer-2-scaling-solutions-380b696fa469#:~{}:text=Layer%202%20solutions%20are%20protocols,you%20can%20attach%20cryptoeconomic%20systems (accessed on 13 July 2021).
93. Poon, J.; Buterin, V. Plasma: Scalable autonomous smart contracts. *White Pap.* 2017, pp. 1–47. Available online: https://www.plasma.io/plasma-deprecated.pdf (accessed on 13 July 2021).
94. Blue, J.; Condell, J.; Lunney, T. This is Me: A Bayesian Approach to Weighting Digital Identity Sources. In Proceedings of the 30th Irish Signals and Systems Conference, Maynooth, Ireland, 17–18 June 2019; pp. 1–6. [CrossRef]
95. Chen, Y.; Yang, R.; Lin, Y.; Liu, J. System and Method for Mapping Decentralized Identifiers to Real-World Entities. U.S. Patent Application No. 16/735,538, 25 February 2020.
96. Schaad, A.; Reski, T.; Winzenried, O. Integration of a Secure Physical Element as a Trusted Oracle in a Hyperledger Blockchain. *ICETE (2) July, 2019*; Offenburg, Germany, 2019; pp. 498–503. Available online: https://www.researchgate.net/publication/335167358_Integration_of_a_Secure_Physical_Element_as_a_Trusted_Oracle_in_a_Hyperledger_Blockchain (accessed on 13 July 2021).