


Article

# Security of Blockchain-Based Supply Chain Management Systems: Challenges and Opportunities

Sana Al-Farsi \*, Muhammad Mazhar Rathore  and Spiros Bakiras

Division of Information and Computing Technology, College of Science and Engineering,  
Hamad Bin Khalifa University, Doha P.O. Box 34110, Qatar; mrathore@hbku.edu.qa (M.M.R.);  
sbakiras@hbku.edu.qa (S.B.)

\* Correspondence: saalfarsi@hbku.edu.qa

**Abstract:** Blockchain is a revolutionary technology that is being used in many applications, including supply chain management. Although, the primary motive of using a blockchain for supply chain management is to reduce the overall production cost while providing the comprehensive security to the system. However, current blockchain-based supply-chain management (BC-SCM) systems still hold the possibility of cyber attacks. Therefore, the goal of this study is to investigate practical threats and vulnerabilities in the design of BC-SCM systems. As a starting point, we first establish key requirements for the reliability and security of supply chain management systems, i.e., transparency, privacy and traceability, and then discern a threat model that includes two distinctive but practical threats including computational (i.e., the ones that threaten the functionality of the application) and communication (i.e., the ones that threaten information exchange among interconnected services of the application). For investigation, we follow a unique approach based on the hypothesis that reliability is pre-requisite of security and identify the threats considering (i) design of smart contracts and associated supply chain management applications, (ii) underlying blockchain execution environment and (iii) trust between all interconnected supply management services. Moreover, we consider both academic and industry solutions to identify the threats. We identify several challenges that hinder to establish reliability and security of the BC-SCM systems. Importantly, we also highlight research gaps that can help to establish desired security of the BC-SCM. To the best of our knowledge, this paper is the first effort that identifies practical threats to blockchain-based supply chain management systems and provides their counter measures. Finally, this work establishes foundation for future investigation towards practical security of BC-SCM system.

**Keywords:** blockchain; supply chain; information security; privacy; transparency



**Citation:** Al-Farsi, S.; Rathore, M.M.; Bakiras, S. Security of Blockchain-Based Supply Chain Management Systems: Challenges and Opportunities. *Appl. Sci.* **2021**, *11*, 5585. <https://doi.org/10.3390/app11125585>

Academic Editor: Paula Fraga-Lamas

Received: 31 March 2021

Accepted: 18 May 2021

Published: 17 June 2021

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

Blockchain has established trust among distributed components of a system through introducing new currencies (e.g., Bitcoin), auto-enforced digital contracts (e.g., smart contract), and intelligent assets that can be monitored and controlled over the Internet [1–3]. In the area of blockchain, majority of the current research is focused on the development of cost-effective applications in various domains. Supply chain management is one of the domains where the records and chain-transaction data are stored and processed using blockchains, aimed at increasing trust, transparency, and efficiency, while reducing overall supply chain cost.

Based on the fact that blockchain ensures data integrity and secures data against tampering attacks by chaining data in a secure-hash way, many supply chain systems have been developed using blockchain and related technologies by academia and industries. In academia, most of the research has been focused on employing blockchain technology to ensure the protection of information exchanged among different business partners and customers. These academia systems lead us to successfully detection of various attacks

that are related to information leakage and tampering. However, since the deployment of current blockchain aims to protect communication among distributed components of a business, it fails to detect any threat that arises from any other layer of the architecture, e.g., application. In industry, most of the research has been focused on developing tools that use blockchain to support transparent exchange of information by automatically enforcing the transactions among parties. However, again these tools fail to detect any threat that targets business level agreements and other local threats.

There are several literature studies available, discussing current research in this domain. However, current surveys and reviews on blockchain-based supply chain systems have focused on data driven protection of supply chain and involved stakeholders, compliance of supply chain with various regulations, interoperability among cross-chain and cross-border supply chains, to name a few. This survey will help the interested reader to find a systematic way through the diverse literature on the security of blockchain-based supply chain topics out there already. This survey provides a systematic investigation of various security issues by defining classification of different attacks contextualising blockchain and then investigating various academic and industrial efforts to handle them. Importantly, we are interested in end-to-end protection of the supply chain processes that involves security of all the involved stakeholders, their business processes and corresponding assets. We have identified the gaps that need to be addressed by the corresponding stakeholders and entities involved in the supply chain process to ensure end-to-end security of the process.

Overall, the research so far has been focused to use blockchain in supply chain systems to handle different issues enabling trusted communication among interacting partners and stakeholders of the supply chain. However, with the introduction of the blockchain technology in the supply chain, new attacks and threats have emerged that needs to be considered, in particular the attacks that are related to the actual business and assets.

To this end, we discussed our survey methodology in Section 2. We explained our study starting from an overview of related technologies like supply chain management, blockchain and block mining, smart contracts, and blockchain-based supply chain systems in Section 3. Initially, we defined the threat model for BC-SCM systems in terms of security requirement, possible attacks, and sources of attacks, in Section 4. Based on our threat model, we classified attacks on BC-SCM systems into computational and communication ones, and we have investigated current academic and industrial efforts to handle them in Sections 5 and 6. Finally, in Section 7, we identified research gaps that may help to build blockchain-based supply chain systems that support more rigorous protection to the supply chain and their associated partners and stakeholders. At last, we conclude our article in Section 8.

## 2. Survey Methodology

We performed a survey in a very systematic way by identifying top research findings in the domain of blockchain-based supply chain management (BC-SCM). We extracted information and summarised the current literature according to the guidelines suggested by Kitchenham [4,5]. Our approach follows a defined sequence of steps using a systematic literature review (SLR) [6], started from downloading related research articles, reports, thesis, and industrial tools using keyword-based query-searching mentioned in Table 1. At the initial stage of the study, we found that industries played a major role in identifying the role of blockchain for supply chain management, while developing tools based on the blockchain technology. Therefore, we partitioned our survey into industrial efforts and academic efforts. Industrial efforts particularly focus on the development of blockchain-based tools for supply chain management. On the other hand, the academic efforts are the published research literature, focusing on the research aspects of the blockchain technology for supply chain processes.

**Table 1.** Search Keywords.

	supplychain
	finance OR banking
	agriculture OR food
	healthcare OR medicine
	compliance OR regulation
	(computation OR communication) AND threats
Blockchain AND	(security OR privacy) AND threats
	“automotive industry” OR “manufacturing industry”
	(“smart contracts” OR cryptocurrency OR transaction) AND threats
	“business control” OR “process control”
	“security analysis” OR verification

The security of communication and computation operations is the major concern of any blockchain system. On this account, research questions are defined based on the existing solutions to communication and computational attacks on supply chain systems to identify the research gaps and opportunities through a designed framework. Mainly, following research questions are investigated in this study.

- What is the blockchain technology and how it is used for a supply chain system?
- The use of smart contracts for a blockchain-based supply chain system?
- What is the security requirement for a supply chain system and what are major computation and communication attacks that compromises the security of a blockchain-based supply chain system?
- What efforts had been made by the industrial sector—in terms of tools development—to handle existing computation and communication attacks by introducing secure blockchain system?
- What research solutions had been achieved by the academia to cater computation and communication attacks on a blockchain-based supply chain system?
- What are the current research gaps and future potentials for the academia and the industry to focus on?
- What are the main aspects that must be considered while designing a blockchain-based supply chain system (recommendations)?

To widely cover the current literature, we considered studies published in five multidisciplinary electronic bibliographic database including IEEE, ACM, Springer, Elsevier, and ScienceDirect. Since the blockchain technology is recently become popular, it started to be used for supply chain management in last decade. Wherefore, we considered articles published from 2015–2020. Even though, we found more than 30,000 blockchain related studies, we selected top 150 studies that matches our search criteria in Table 1. Downloaded articles were critically examined based on the research questions and related abstracts, and half of the papers were excluded in this phase. During full-text screening and Snowball sampling, 20 more papers are eliminated. Backward and forward selection is performed on references of the remaining 55 papers, identifying 7 more potential papers. In addition to research articles and thesis, 29 web-reports and industrial tools are pointed out in this study. Figure 1 shows the number of studies considered from each year, from 2015 to 2020.

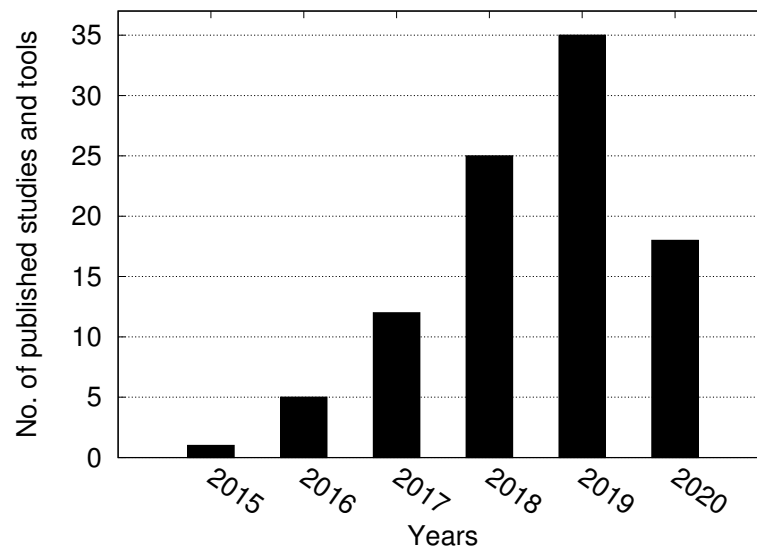


Figure 1. Statistics of the covered literature.

### 3. Blockchain for Supply Chain: Fundamentals

#### 3.1. Supply Chain Process Management

We can view a supply chain as an organized and systematic network between a company and its suppliers to manufacture and sell a particular product to the final customer, aimed at reducing costs and being competitive in the market. It consists of different processes, data and information flows, people, entities, and other resources. Simply, supply chain covers all the stages and entities involved in delivering a product from its original state to the final customer, starting from supplying and transforming raw materials into a manufactured product, moving the product in the market, and distributing them to the final customer. Overall, supply chain processes rotate in-between five entities including suppliers, manufacturer, distributors, Retailers, and consumers, as shown in Figure 2. Every entity in the supply chain delivers items to another entity against the agreed terms and payments. In modern supply-chain management systems, these agreements, payments, and deliveries are facilitated by blockchains.

Effective management is crucial to realize optimized supply chain processes, achieving reduced costs and a rapid production cycle. Supply chain management consists of wide range of functions, covering numerous areas. Several supply chain management models exist in the market, varying the number of functions offered. Supply Chain Council developed one of the widely used and more effective model, called Supply chain operations reference (SCOR) model [7], with the help of top-seventy manufacturing firms across the world. SCOR effectively guides managers to tackle, refine, and disseminate supply chain management practices using five primary stages, including plan, source, make, deliver, and return.

Planning focuses on the analysis of demand and corresponding supply options. It involves various operational strategies and decisions to improve supply chain process effectively, such as balancing resources, determining communication along the entire chain, determining suppliers, determining business rules related to inventory, transportation, and assets, etc. At this stage, it is ensured that the supply chain plan is aligned with the company's financial plan. Next, at 'source' stage of supply chain, matters related to procurement of raw materials and components are handled. Sources are assessed and selected, contracts are being negotiated between companies and suppliers, and deliveries are scheduled. In short, it involves the management of inventory, the supplier network, agreements, performance, payments, and scheduling of the entire process from the material reception and verification to its delivery. The third stage 'make' entails the management of production activities like, constructing, packaging, assembling, and releasing. It also

facilities the records of production network, assets and facilities, and transport. The 'deliver' stage cares about all the aspects of customer orders, warehousing, inventories, and delivery-transport. It manages orders collections from customers and invoicing them after product delivery. In addition, it also manages records of warranty and trial periods (if any), retail sites invoicing and payments, and import and export requirements of the manufactured product. Finally, the 'return' stage deals with the return aspects of the product, including return of containers, packages, defective product, inventory, assets, and transportation, and the related business rules and regulatory requirements. A BC-SCM system implements these stages (fully or partially) using a blockchain and smart contracts.

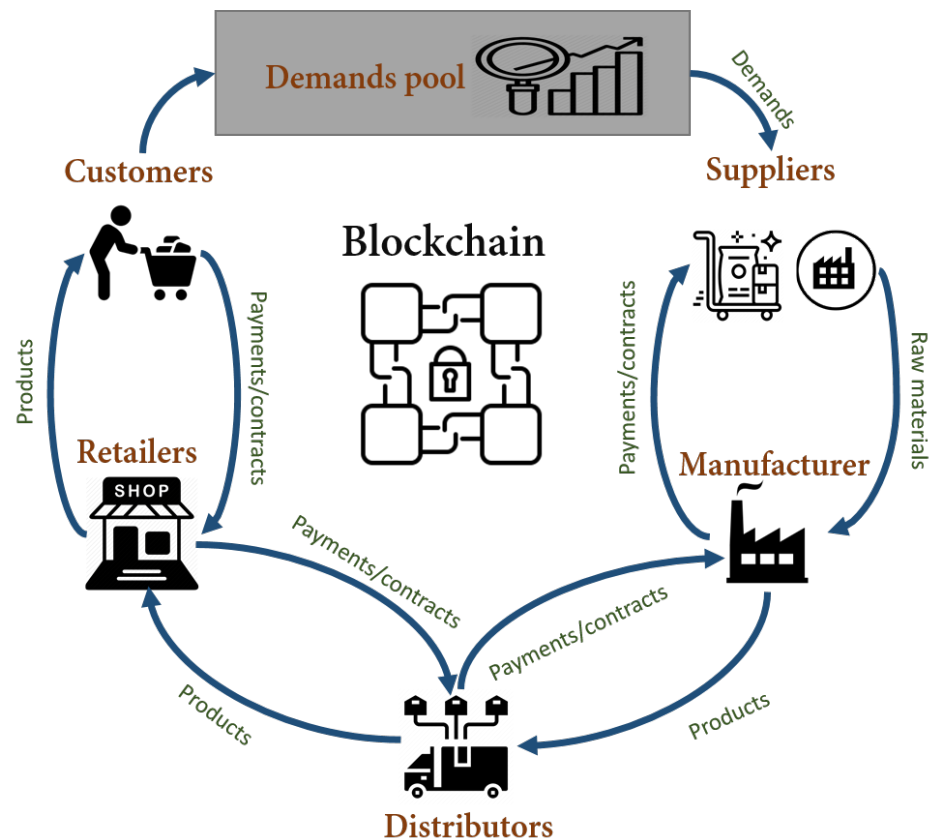


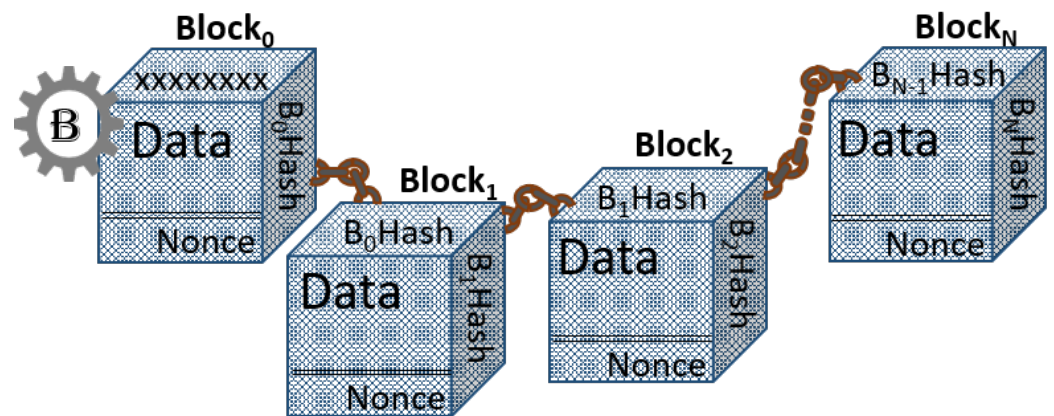
Figure 2. Supply chain process.

### 3.2. Blockchain

Blockchain is a distributed and decentralized database system that keeps records into numerous digital blocks by forming an unbreakable and immutable chain between them, as shown in Figure 3. Each block is uniquely identified by its hash-code, which is generated by a one-way cryptographic hash function using block-data. A cryptographic hash function assures large unpredictable change in the hash-code with a single bit alteration in the block-data. Each new block stores the hash-code of the previous block, along with its actual data, to form a chain. Summarising, a single block stores four types of information i.e., (1) a hash-code of the previous block, (2) the actual data records that may be transactions data like date and time, amount, quantity, and the participants' information (e.g., buyer and seller's digital signatures), (3) the nonce, and (4) the hash-code of the current block, produced by applying hash function on the hash-code of the previous block, the nonce, and the transaction data. Thousands of transactions of more than 1MB can be stored in a single block (<https://www.blockchain.com/charts/avg-block-size> accessed on 20 May 2021)). Number of blocks in a blockchain is called the height of the blockchain.

Thousands of computers work together as a part of the blockchain network. Each computer, called blockchain node, stores its own replica of the blockchain, thus, thousands

of identical copies of the blockchain exist. The replication of blockchain and the constructed chain by hash-codes between blocks make it difficult for the attacker to manipulate the data in any block. A manipulation in a single block constrains changing all the subsequent blocks in the chain, as well as, changing at least 51% copies of the blockchain on nodes, which is not practical in case of large blockchain or its network.



**Figure 3.** Blockchain overview.

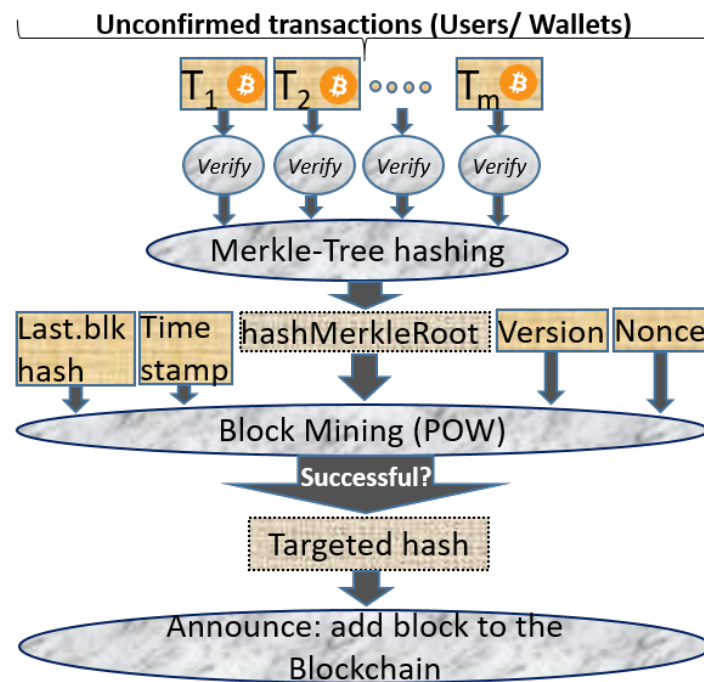
### 3.3. Block-Mining: How New Records Are Added to a Blockchain?

In a blockchain system, every user owns a public and private key pair, which serves for digital signature and verification of the transaction (or a record). When a transaction is carried out between two participants (or a record is generated), it is digitally signed by the generating party and broadcast to the blockchain network. It remains unconfirmed until it is added to the blockchain as a part of a block. Every node in the blockchain receives all the unconfirmed transactions from blockchain users (or wallets), verifies their digital signatures, and organizes them in a chronological order. Individually and independently, all the nodes form a temporary-block by choosing multiple transactions from the unconfirmed-transactions pool. It means, a temporary-block of any node 'A' at time 't' may differ a temporary-block of any other node 'B' at the same time. Hundreds and even thousands of transactions can be added into a block. The number of transactions in a block varies based on time and size of the block. A shorter block assures faster transactions but overall more mining efforts. The block time for Ethereum is 14–15 s, and for bitcoin, it is around 10 min.

Once a temporary-block is formed by a node, a single hash is computed against all the selected transactions in the temporary-block. Bitcoin system utilizes Merkle-Tree to generate this single hash against thousands of transactions in a block [8]. Next, the node starts block-mining, which is a very complex and time-taking process. It is a process to solve a complex mathematical puzzle in order to confirm block transactions and add a block to the blockchain. In Bitcoin system, Proof of Work (PoW) protocol is used as a mining tool, aimed at finding a hash value of the block-header, which meets a given criteria e.g., a hash value that starts with 10 zeros. The block-header consists of five basic fields including (1) the hash of the final-block of the existing blockchain (i.e., the previous-block hash), (2) the timestamp, (3) a transactions hash (Merkle-Tree root hash), (4) version, (5) a nonce. The mining process computes a hash of the block-header using changing values of the nonce until it finds a hash value meeting the given criteria (e.g., a hash with starting 10 zeros). In other words, a bitcoin mining process is to find a special nonce value on which the hash of the block-header meets the defined criteria.

Block-mining is a race where every node in the network is busy in constructing a temporary-block by selecting unconfirmed-transactions and mining it; Who wins the race of mining a block, his block is appended to the blockchain. Remember, nodes immediately stop block-mining process when they receive a claim of a successful mining from a node. Every node verify the successful mining, add the mined-block to the blockchain, reconstruct

their temporary-blocks by removing confirmed transactions (the ones, which are in the newly mined-block) and adding other unconfirmed transactions from the pool, and restart mining on new temporary-block. In a nutshell, once a node successfully mines a block, all the transactions in its block are confirmed and the blockchain is extended by one new block. In a bitcoin blockchain system, a node's block-mining process is depicted in Figure 4.



**Figure 4.** Blockchain mining-node's operation.

### 3.4. Smart Contract

Smart contract is a program that possibly work with the blockchain technology to execute a transaction automatically when a particular condition is fulfilled. Smart contract can be used as an agreement between two parties to automatically transfer funds (or execute any other terms of agreement) when particular conditions are met at both sides. For Example, in case of supply chain, there is an agreement between a customer and a supplier that when a product is received by the customer with a predefined characteristics and quality, the customer will immediately transfer funds to the suppliers account. This agreement can be programmed as a smart contract, which automatically transfers funds from the user to the supplier's blockchain wallet (like bank account), immediate after the product is received perfectly, meeting all requirements.

### 3.5. Blockchain for Supply Chain

Because of the wide range of functionalities of supply chain management, using the blockchain for a complete supply chain process is not practical. For example, while implementing the entire SCOR model-from its 'plan' step to 'return' step-using a blockchain, we need vast amount of processing and storage resources, interconnection between all involving parties, and technological advancement at each level of production and delivery. However, even with the partial implementation, the blockchain is a revolutionary technology that can bring an advancement in the supply chain management because of its safety, more transparency, traceability, and efficiency [9]. A typical blockchain-based supply chain system can be viewed as Figure 5. Most of the existing supply chain systems follow this approach.

BC-SCM not only reduces the supply chain operational cost, but also enhances the trust of customers, suppliers, dealers, and retailers by allowing them to track products (or

raw material) from origins to the reception. This can help them to verify the authenticity of the product or the purchased material and prevent product-fraud. For Example, the Diamond Trading Company (DTC) built a blockchain-based system “Tracr” to manage the supply chain of diamonds [10]. Walmart is trying to monitor the supply chain of lettuce and spinach [11] by storing its blockchain on IBM cloud. A Brazilian meat restaurant “Fogo de Chao” implement blockchain technology, which enabled suppliers, wholesalers, and diners to trace the beef served in the restaurants back to the farm where it was produced [12]. DLT Labs developed a blockchain system for shipping industry to track shipments and deliveries; the system allows automatic invoicing and avoid the billing disputes between parties [13]. Similarly, blockchain-based supply chain systems have been developed for other industries such as, pharmaceutical industry [14], agriculture and food industry [15], airline industry [16], manufacturing industry [17], construction industry [18], product recycling [19], and electronics industry [20].

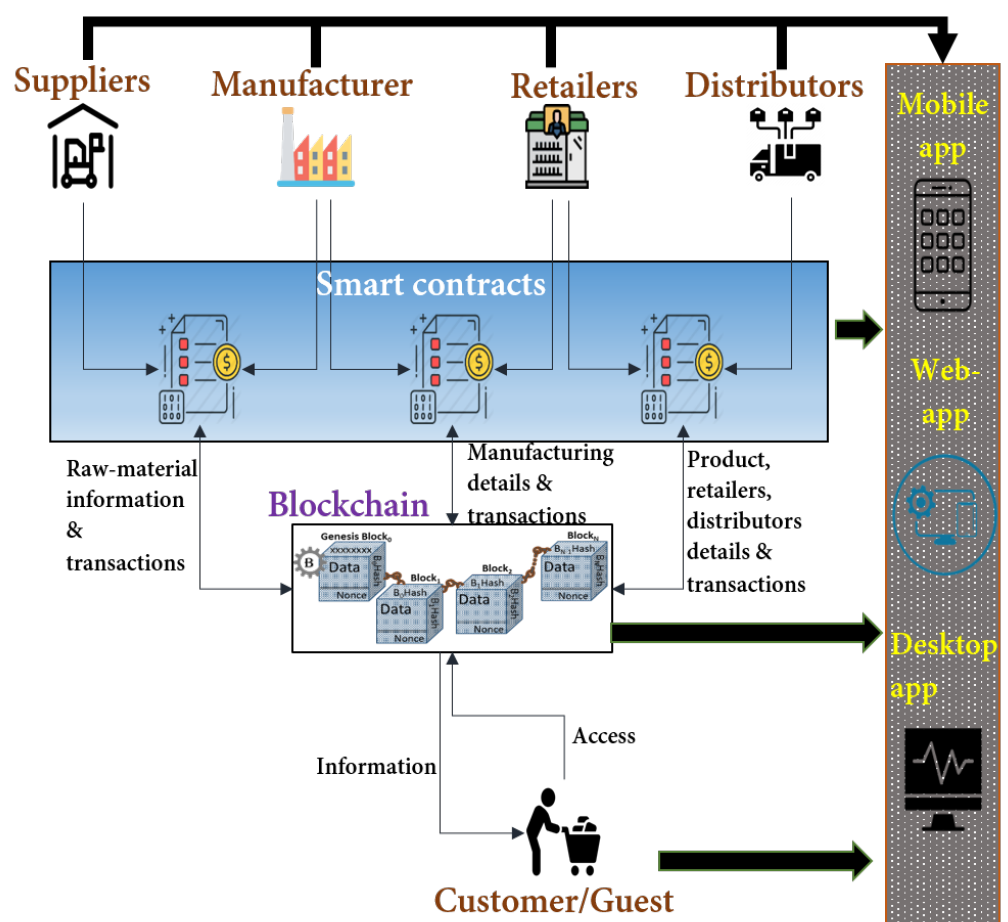


Figure 5. Blockchain-based supply chain management.

#### 4. Threat Model for a Blockchain-Based Supply Chain System

A typical supply chain application involves two types of interactions. The first one is the interaction within the internal processes or parties, e.g., finance, inventory, and warehouse. Whereas, the other one involves the external processes or parties such as supplier, vendors and banks. Being part of the same organization, the former interaction and associated processes are trusted ones, as they are usually fully digitized and automated. However, the latter interaction and associated processes are un-trusted as they usually require combination of automated and manual interaction.

Analogously, a BC-SCM is a typical supply chain application that requires an infrastructure to handle blockchain technology. The infrastructure includes smart contracts that usually ensure secure interaction among parties, and a distributed ledger that stores all



corresponding interactions. The focus of this survey is to analyse existing BC-SCM systems for possible attacks on its computational and communication processes and corresponding solutions.

#### 4.1. Computational Attack

In a supply chain domain, a *computational process* performs *business computations* that typically implement business processes in an application, and *interactive computations* that typically implement interactions in a smart contract. A computational process is two-dimensional, considering both its implementation and execution.

In a computational attack, adversary aims to compromise the functionality of the supply chain setting by various means. For instance, the adversary may compromise the functionality by modifying the smart contract and its execution, or by exploiting any vulnerability or bug in the contract or its execution engine.

#### 4.2. Communication Attack

The *communication process* is responsible for exchange of data among different parties (processes or people), involved in the supply chain. In a communication attack, the adversary aims to compromise the information that is exchanged among various connected services. For instance, the adversary may compromise the information either by tampering input values to smart contracts or other components, or by breaching integrity of the communication by selective forward and drop tactic, or by injecting false information based on mining of public contracts and the ledger.

#### 4.3. Sources of Attacks

Importantly, we investigate the attacks that mainly arise due to the weak design of smart contracts and applications, blockchain execution environment, and untrusted-environment among interconnected supply chain services.

*Design of smart contract and application* (DSC) is key source of various attacks. Current smart contracts are limited, only offering transaction related functionality, and they fail to handle any serious security requirement of the application. This is due to the fact that smart contracts were design without considering security and privacy of the applications interacting with them.

*Blockchain execution environment* (BEE) is an important source of various attacks because typical deployment of blockchain-based solutions involve public ledgers and contracts (i.e., they are visible to anyone), therefore, adversaries can easily determine their vulnerabilities and weaknesses and can exploit them to launch attacks.

*Trust among interconnected supply chain services* (TIS) is a crucial source of very critical attacks. Several sub-processes of the supply process are not digitized, therefore their trust cannot be established easily. Importantly, the trust of digitized and automated sub-processes is also threatened, mainly because of the supply services that are not context-aware. Importantly, the trust among services also critically depends on secure exchange of information through underlying communication channel.

The mapping between the above-mentioned attacks, security requirements of the supply chain management system, and potential causes of attacks is shown in Table 2.

**Table 2.** Mapping of Attacks to Requirements.

Attack Type	Attack Mechanism	Affected Requirements	Causes
Computational	Contract modification	Traceability, Privacy	DSC, BEE
	Execution modification	Traceability, Privacy	DSC, BEE, TIS
	Vulnerability exploit	Traceability, Transparency, Privacy	DSC, BEE
Communication	Tampered input values	Traceability, Transparency, Privacy	BEE, TIS
	Breach of data integrity	Traceability, Transparency, Privacy	BEE, TIS
	False information injection	Traceability, Transparency, Privacy	DSC, BEE, TIS

#### 4.4. Security Requirements for Supply Chain Systems

With recent advent of technologies like industrial IoT and 5G, modern supply chain management systems aim to digitally co-ordinate all sub-processes of supply chain from supplying products to delivering and/or resumption of the products. We considered the reliability of such systems as the pre-requisite of security. Accordingly, we scrutinize transparency, traceability, and privacy as the key requirements for the security of supply chain systems. *Transparency* guarantees a transparent co-ordination among all sub-processes, which helps in immediate identification of inconsistencies or conflicts between any of the two sub-processes, in order to ensure timely supply of the product on one hand and to save the cost (e.g., logistics) on the other hand. *Traceability* demands sufficient information recordings that can perfectly facilitate in tracing the product and interactions among entities, and performing auditing at later stages. Finally, preserving the *privacy* of sensitive organizational information is important. Privacy can be archived by protecting the co-ordination between processes and communication between involving parties from possible security threats.

In recent developments, blockchain has been used in supply chain in different ways to handle security and privacy issues [21–26]. Importantly, blockchain integrated supply chain solutions are good in providing security and privacy of data that does not allow to modify the data records or to misuse the data. Also, such solutions facilitate audit for security and privacy violations as it has full trail of interactions among communicating parties.

While such solutions are good at providing protection of data it does not help to detect any security threat (as discussed in Section 4) that arises from the computational and communication process. In detail, such solutions fail to detect any threat in real-time that occur when a computation or a communication goes wrong, such as the execution of a smart contract is compromised, or a communicating party gets compromised and shares undesired data, respectively.

In this survey, we investigated state-of-the-art blockchain-based supply chain management-proposals, considering three security requirements of transparency, traceability, and privacy. In addition, we analysed the existing solutions based on the thread model presented in Section 4, including the types and sources of attacks. We classify efforts of building a secure blockchain-based supply chain system into two categories as academic and industrial. The Academic efforts and the industrial efforts are individually discussed in the following sections.

### 5. Academic Efforts to Blockchain-Based Supply Chain Management: Current Research

In this section, we investigated existing blockchain-based solutions, by the academia, in the domain of supply chain management, particularly aimed at handling the communication attacks and computational attacks.

#### 5.1. Efforts against Communication Attacks

Most of the academic proposals for blockchain-based supply chain system focused on four operations, in order to handle communication attacks. These operations are (1) preserving the privacy of shared information among parties [21,27,28], (2) improving the governance [29,30], (3) achieving the interoperability among heterogeneous systems and infrastructures [31–35], and (4) securing the data sharing mechanism [36,37]. The academic efforts to realize these operations are examined using the security requirements and threat model, as discussed in Sections 4 and 4.4, and these efforts are summarised in Table 3.

**Table 3.** Handling Communication Attacks—Academic Efforts.

Papers	Application Areas	Target Operations	Key Contributions	Affected Requirements	Potential Attack Mechanisms
[21,27,28,38,39]	Finance, Logistics	Privacy of information	Traceable proof of ownership, Product authenticity, Audit-ability	Traceability Privacy	Breach of data integrity
[29,30,40,41]	Payment, Intellectual property, Healthcare, International policy	Governance	Directive compliance, Ownership rights, Privacy of genomic data, Policy analysis and design	Traceability, Transparency, Privacy	Breach of data integrity, Tampered input data
[22,42–46]	Cross blockchain systems, Supply chain resilience, Cross crypto-systems, Cross non-blockchain systems, Cross IoT and typical network systems	Interoperability among heterogeneous systems	Token based interaction, Privilege based access, Avoid intermediate disruptions, Functional interoperability, Data driven track and trace	Traceability, Transparency, Privacy	Breach of data integrity, Tampered input data, False information injection
[36,37,47–51]	Healthcare, Food, Agriculture, Smart cities	Secure data sharing	Storage scheme, Integration of RFID and blockchain, Reward based share, Decentralized file system	Traceability, Transparency, Privacy	Breach of data integrity, Tampered input data, False information injection

### 5.1.1. Preserving-Privacy

Some of the academic efforts focused on the assurance of privacy of the shared-data among different coordinating parties. These research efforts are made in the supply chain processes of finance and logistics. These efforts attempted to ensure traceability and privacy of the information exchanged through blockchain, by allowing traceable proof of ownership of the products, authenticity of products, and audit of the products at anytime. For instance, Ref. [27] enabled supply chain management with IoT-based solutions, integrating special tags (e.g., RFID, NFC, and QR-codes) with products to create Smart Tags (ST). These tags eventually helps to track products during their supply chain lifecycle. Being based on distributed ledger technology (DLT), the solution offers a decentralized, privacy-preserving, and verifiable management of Smart Tags during a product's supply chain lifecycle. Furthermore, Ethereum blockchain is used for interaction among various stakeholders while product exchange process. Since the consensus requires agreement on the product's information on the blockchain, all involved stakeholders and consumers can verify the authenticity of the product's information without revealing their identity. Although, the solution provides traceability of the product—the origin of the product and its journey across the supply chain—without manipulation, this works under the assumption that ST generator and other stakeholders within the supply chain are providing authentic data related to the products, which is not true in practice.

Furthermore, in a supply chain system by Feng et al., [21], a homomorphic encryption is used to ensure the information-privacy among different stakeholders for a transaction. However, this system assumed that a certain percentage of the participants in decentralized-mixing protocols are honest. Again, this assumption may not be practical, thus such systems cannot avoid some attacks like Sybil. Besides, in another effort [28], a real-world implementation of blockchain was demonstrated to ensure traceable proof of ownership while transferring goods in freight carriers. To preserve the privacy, a blockchain-based decentralized system lead to business networks, and company information was being disclosed through data triangulation. However, such approaches works, if the information is only exchanged among trusted stakeholders, which is not typical in the case of real-time transfer of goods, particularly when the transfer is across the border. Similarly, there are other systems [38,39] that mainly addressed the privacy concern in a supply chain system using the blockchain.

### 5.1.2. Improving Governance

Academia also made efforts to improve the governance of supply chain systems using blockchain in various interesting application areas including payment, intellectual property, healthcare, and international policy. In detail, few systems are developed to secure payment systems, compliant with the agreed policy and directive to achieve traceability. Alike, various other systems were developed to secure intellectual properties by establishing blockchain-based transparent and traceable ownership rights. Interestingly, one of the system investigated coordination mechanism among parties in a transparent and traceable way across the border to help decide analysis and design of the coordination policies. For instance, Gcoin blockchain [29] is used to enable drug supply chain transaction data immutable, consensus driven, and transparent. The solution also extends governance model of the drug supply chain to support surveillance net. The surveillance net is established by every stakeholder involved in the drug supply chain, e.g., manufacturer, retailer/wholesales, pharmacies/hospitals and patients. To support surveillance net, the government agencies set a risk threshold by identifying a transaction pattern through data mining. Later, if any transaction behavior of a drug stakeholder/company is not compliant with the threshold, the smart contract can raise an alarm for inspection. Based on the alarm, the potential illegal transaction can be judged invalid by the Gcoin, until the drug inspectors sent by the competent government authorities check the drugs and provide their digital signature to verify the transaction. Importantly, the result of each of the suspicious inspection cases is automatically fed back to revise the threshold. Though this work ensures traceability of the product information along its journey across the drug supply chain, however, it only works for the static (i.e., shallow) specification of the product, and it may not be directly applicable to trace dynamic properties of the product (e.g., performance, behavioral properties). The task of tracing dynamic properties of the products becomes challenging, if the product includes software (i.e., functional and non-functional specification of the product).

Also, Holland, Stjepandić, and Nigischer [30] introduced a blockchain-based digital rights management as a key governance technology for the successful transition to additive manufacturing methods and a key for its commercial implementation and the prevention of intellectual property theft. In fact, 3D printing technology is an emerging disruptive innovation, which involves spatially distributed development of printed components, e.g. for the rapid delivery of spare parts, creates a new challenge when differentiating between “original part”, “copy” or “counterfeit” becomes necessary. Therefore, the proposed approach adopts the characteristics of licensing models as we know them in the areas of software and digital media. Unfortunately, the project only supports the governance through traceability. It only works when all operations of stakeholders are occurring in a trusted environment, which is not a typical case in real-time technology-based operations. There are several other systems to improve government in different applications, such as [40,41].

### 5.1.3. Interoperability

To ensure interoperability among various systems and infrastructures in a secure way, there were some proposals that devised a token based access approach to support interoperability among blockchain-based systems, implementing different underlying hashing and encryption mechanisms. To support functional interoperability among various crypto-systems and non-blockchain-based systems, privilege based mechanism is proposed. While, to support interoperability among underlying heterogeneous infrastructures, data driven approaches were developed—to track and trace various devices—and identified associated with different infrastructures, e.g., IoT. John et al., [34] designed a protocol for cross-blockchain asset transfers through “claim-first transactions”. In principle, they concluded that it is not possible to verify on one blockchain,  $CA$ , that data,  $D$ , have been recorded on another blockchain,  $CB$ . They call it “cross-blockchain proof problem” whose formal proof requires (i) “the presence of a subset of the block lineage of  $CB$  on  $CA$ , and

(ii) the verification of the transaction consensus of *CB* by the transaction consensus of *CA*. Since, these are typical problems with “spend-first” transactions, where the recipient of a transfer of assets on one blockchain is unable to verify that the assets have been marked as spent on the originating blockchain. The work handles this problem by reversing this intuitive processing sequence and creates a claim transaction for the assets on the target chain. Such approaches supported interoperability across different blockchain systems, but they failed to support end-to-end interoperability of supply chain systems that involves stakeholders, companies, and products with fundamentally different policies, governance, and operations.

Recently, a blockchain-based privacy preserving payment mechanism [31] has been proposed for V2G networks, which enables data sharing among different V2G networks while securing sensitive user information. The proposed mechanism includes a registration and data maintenance process, based on a blockchain technique. The mechanism ensures the anonymity of user’s payment-data, while enabling payment-auditing by privileged users. The solution achieves interoperability by recording information for data exchange among different stakeholders, however, this fails to detect threats that arise from business process of the stakeholders—e.g., the attacks that requires injection of incorrect information at first place. Furthermore, a tokens-based mechanism [32] was introduced—called MID (MOSChain Identity)—that included name and quantity of a product. The name and the quantity is tracked and traced to support interoperability among departments (e.g., production factory, warehouse, distribution center, logistics and wholesale or retail stores, etc.), when the products are transferred among the departments. The solution works in a restrictive environment as it does not trace any process information of the involved departments, thus it failed to provide end-to-end interoperability of the products.

In addition, Koens and Poll [33] distinguished interoperability solutions (i.e., technical and non-technical) and classified their sub-categories based on key properties of solutions. Based on the approach, they have shown that it is possible to describe, analyze, and evaluate DL interoperability solutions with these properties. Furthermore, they have described that the zero-spend attack is applicable to all those interoperability solutions that include a DL with a probabilistic consensus algorithm. In fact, they concluded that as a consequence of this attack, it is critical for deciding on whether or not ledgers should inter-operate. A successful attack would lead to an invalid state between immutable ledgers. Since the solution ensure interoperability of various blockchain-based solution, it cannot provide interoperability among the involved stakeholders which run different business process for their interaction. Few other blockchain-based solutions [22,42–46] exists for interoperability among supply chain entities.

#### 5.1.4. Data Security

Finally, we investigate academia efforts for securing data among supply chain parties in application areas of healthcare, food, agriculture and smart cities. Various schemes have been developed for traceable and transparent storage of healthcare data. Several approaches enabled transparent tracing of food items by employing decentralized file systems to store local food clusters for efficient and timely detection of undesired items. Some other attempts have been made for a reward-based data share among various smart city entities in a privacy-preserving and transparent way. For instance, Wen et al., [36] developed a solution for the supply chain management that not only know how to collect the data but also ensures the un-leakage of data. The solution combines the monitoring and recording of IIoT devices, and stores real-time data in the network by smart contracts. Furthermore, the combination allows collaboration solutions between different stakeholders and entities involved in the supply chain. The solution guarantees a secure data exchange by setting access policies to the smart contract, and later, only those stakeholders and entities that satisfy the attributes of access policies can execute the smart contract and view the details of the transaction. The solution made sure the reliable exchange of data among various supply chain entities, and also protected the privacy of the chain. But, it is limited to

secure only those data properties that are bound with smart contracts. It failed to ensure end-to-end data security in a supply chain, because a typical chain involves people and business processes which are beyond the scope of smart contracts.

Also, for data security, a robust ultra-lightweight mutual authentication RFID protocol [37] is proposed that works together with a decentralized database to create a secure blockchain-enabled supply chain management system. The protocol has been proven to be secure from key disclosure, replay, man-in-the-middle, de-synchronization, and tracking attacks. Furthermore, a formal analysis has been performed using automated validation of internet security protocols—using Gong, Needham, and Yahalom logic—and applications tool to verify security properties of the protocol. The protocol is proven to be efficient with respect to storage, computational, and communication costs. Additionally, a further step is taken to ensure the robustness of the protocol by analyzing the probability of data collision written to the blockchain. Similar other data security solutions in a blockchain based supply chain system are [47–51].

### 5.2. Efforts against Computational Attacks

On the contrary to communication attacks, computational attacks find the vulnerabilities in the computational processes of the system. Existing BC-SCM systems established a defence against computational attacks by (1) assuring transaction and operations privacy and compliance [52–54] and (2) identifying unique ways for vulnerability detection in smart contracts and establishing trust on their execution environment [55–58]. State-of-the-art blockchain-based solutions from the academia, handling computational attacks, are recapped in Table 4.

**Table 4.** Handling Computational Attacks—Academic Efforts.

Paper	Application Areas	Target Operations	Key Contributions	Affected Requirements	Potential Attack Mechanisms
[52,54,59–61]	Healthcare prediction, Financial credit scoring, Smart buildings	Transaction privacy and compliance	Flow shop scheduling, Voucher based compliance, Decentralized coordination	Traceability, Privacy	Execution modification (rewriting attacks)
[53,55–58,62–66]	Real-state, Investors	Vulnerability detection in smart contracts	Fairness, Transfer amount vs required amount, Transaction disorder, Non-validated arguments, Exception handling, Overflow and Underflow	Traceability, Transparency, Privacy	Vulnerability exploit, Execution modification

#### 5.2.1. Security of Transactions and Operations

Since blockchain transactions actually implement a contract among various stakeholders, therefore, it is critically important to ensure that the encoded contracts are compliant with desired directives/policies and are privacy-aware and secure. To ensure traceability and privacy in logistics, an effort has been made in developing a flow-shop scheduling mechanism using blockchain [52]. Also, to ensure transaction compliance among cryptocurrencies, another solution is developed for a voucher based compliance mechanism [54]. Furthermore, to achieve traceability and privacy among real-estate agents, a decentralized coordination based security mechanisms have been implemented [59]. For instance, Cheng et al., [53] designed ‘Ekiden’, which is a system to address lack of blockchain inherited confidentiality and poor performance of smart contracts. To this end, the system combines blockchains with trusted execution environments (TEEs). Ekiden architecture separates consensus mechanism from smart contract execution, enabling efficient TEE-backed confidentiality-preserving smart contracts and high scalability. The system-prototype outperformed the Ethereum mainnet by 600× increased throughput and 400× reduced latency with 1000× lesser cost. Moreover, the system identifies and treats the pitfalls arising from the integration of TEEs and blockchains. Handling TEEs and blockchains separately guarantees stronger security, but their integration endangers new attacks. For example, in naive designs, privacy in TEE-backed contracts can be jeopardized by forgery

of blocks, a seemingly unrelated attack vector. The insights learned from Ekiden are of great importance in integrated and hybrid TEE-blockchain systems. Still, the Ekiden's preserve the limited end-to-end privacy to data across the supply chain journey, particularly when the journey include cross-chains.

In [52], a design model of smart contract for the supply chain with multiple logistics service providers was proposed. Authors tested the model to show that the problem can be presented as a multi-processor flexible flow shop scheduling problem. The model introduced a "virtual operation" that allowed to describe the execution of physical operations inside the start and completion of cyber information services. The constructed model has been tested in an experimental environment that constitutes an event-driven dynamic approach to task and service composition when designing the smart contract. The model also uses state control variables that enables operations status updates in the Blockchain that in turn, feeds automated information feedback, disruption detection, and control of contract execution. Consequently, the resulting feedback mechanism launches the re-scheduling procedure, comprehensively combining planning and adaptation decisions within a unified methodological framework of dynamic control theory. Even though, the model provides good prediction of the supply chain process, but it is not clear what level of granularity of the physical and cyber operations it supports, and what is the key to practically ensure model-based security of the supply chain system.

Zhang et al., [54] also introduced a similar model that enabled a smart contract to effectively prevent rewriting attacks. The model requires each node—that creates a new block—to register with the smart contract to get a voucher, in order to validate the subsequent block. Later, the model explains the flow of the algorithm that is implemented in the smart contract. The model is able to detect various inconsistencies in the algorithm implementation using 'Solidity'. But, it cannot detect a security issue that is raised due to vulnerabilities in the language or the execution environment.

### 5.2.2. Security to Smart Contracts and Their Execution Environment

Most critical attacks on smart home are exploiting the vulnerabilities in a smart contract and executing them in a compromised way. Recently, several tools have been developed to identify vulnerabilities in smart contract. These vulnerabilities include (but not limited to) inconsistent balance, re-entrance, transaction disorder, tampering block timestamp, failed exception handling, call stack depth, over- and underflow of numeric values, asynchronous send operation, no restricted write operation, and non-validated arguments. To identify such vulnerabilities, existing tools perform static analysis on source code of the smart contract, static analysis on the byte code of the smart contract, dynamic analysis of the contract execution, symbolic analysis of the contract code and execution, and verification based analysis of the the contract.

Since the execution of smart contracts enables mutually untrusted entities to interact without relying on trusted third parties. Therefore, it is required to write a contract that is free from any vulnerability. Securify [57] is one of the tools with a rigorous security-analyzer to identify security vulnerabilities in Ethereum based smart contracts. To this end, Securify is scalable, fully automated, and is able to detect the safe/un-safe behaviors of smart contracts on a given model/property. Securify's performs security analysis in two steps. First, it generates dependency graph from the contract, and symbolically analyzes the dependency graph to extract precise semantic information from the contract code. Then, based on the extract semantics, it checks compliance and violation patterns that capture sufficient conditions for proving if a property holds or not. Furthermore, to enable extensibility, all patterns are modelled in a domain-specific language. Securify has been publicly released and has analyzed more than 18K contracts submitted by its users, and is also regularly used to conduct security audits by experts. although, Securify helps to detect security vulnerabilities in smart contracts, but it fails to detect those vulnerabilities which are raised by business operations of the involved stakeholders and consumers.

Also, ZEUS framework is developed by Kalra et al., [55] to verify the correctness and validate the fairness of smart contracts. The framework perceives correctness as adherence to safe programming practices, while fairness is validated by finding whether a smart contract following the higher-level business logic. To this end, ZEUS leverages both abstract interpretation and symbolic model checking, along with the power of constrained horn clauses to efficiently verify the security of contracts. The prototype implementation of the framework was evaluated on almost 22.4 K smart contracts of Ethereum and Fabric blockchain platforms, identifying 94.6% of contracts as vulnerable. Such vulnerabilities contain cryptocurrency transactions of more than \$0.5 billion. Furthermore, the framework was proven correct with zero false-negative and very low false-positive rates, had better performance as compared to state-of-the-art. The major drawback of the framework is its limitation to detect only those vulnerabilities that involve integer expressions. It failed to identify any external vulnerabilities, like the ones due to the language or its execution environment.

## 6. Industrial Efforts to Blockchain-Based Supply Chain Management: Tools

In addition to academic research, industries also developed many blockchain-based tool in the domain of supply chain to overcome the possibilities of communication and computational attacks. In this section, we are discussing state-of-the-art tool developed by industries for supply chain management while saving the system from computation and communications attacks.

### 6.1. Efforts against Communication Attacks

In order to avoid communication attacks, the developed tools (1) establish product provenance and traceability to reduce fraud [67–70], (2) improved security of financial transactions while reducing their cost [71–76], and (3) provide security to information exchanged among cross-border parties and dispute resolution [77–80]. The investigation of these industrial tools—by considering the security requirements and threat model explained in Sections 4 and 4.4—are presented in Table 5.

**Table 5.** Handling Communication Attacks—Industrial Solutions.

Paper	Application Areas	Target Operations	Key Contributions	Affected Requirements	Potential Attack Mechanisms
[67–70]	Food business, Airbus	Provenance	Product traceability, Product provenance, Accessible trace	Traceability, Transparency, Privacy	Breach of data integrity, Tampered input data, False information injection
[71–76]	Cargo, Financial trading, Crypto flow	Efficient financial transactions, Seamless inter-operability, Settlement	Directive compliance, Transparent exchange, Secure trade platform, Transparent finance flow	Traceability, Transparency, Privacy	Breach of data integrity, Tampered input data, False information injection
[77–79]	Cross-border trade, Trade dispute	Inter-operability among cross-border parties	Secure interaction, Privilege based access, Dispute settlement	Traceability, Transparency, Privacy	Breach of data integrity, Tampered input data, False information injection

#### 6.1.1. Product Provenance and Traceability

In industries like food and mechanical spare parts, some of the efforts are focused on the establishment of the provenance of a product by recording all its journey-traces. The main purpose of these efforts is to ensure traceability of the product through blockchains by guaranteeing traceable proof of the movement of products. For instance, Everledger [68] is a platform that helps suppliers and retailers to establish evidence of the product-origin, compliance, and sustainability metrics for their diamond products to get trust of conscientious consumers. Consumers have full access to such information on any device. In principle, the Everledger platform is a network to establish stronger trust in diamond trade and supply chain. Based on the blockchain, the platform supports ISO27001-compliant standards-based mechanisms for authentication of services. This enables stakeholders involved in the supply chain process of diamond-trade to ingest and extract secure diamond data, including characteristics, images, videos, invoices, certificates, and other compliance



documentation. For suppliers, the platform supports retail buyers in seeking new sources of value, who can be rewarded for their investment in a sustainable and ethical business practices [81]. Furthermore, all of the supply chain data is streamline through an API that enables suppliers to choose the onboarding right-choices. Access control mechanism of the platform allows various involved stakeholders—i.e., suppliers and retailers—to determine different rights for their data on the platform. The platform efficiently manages shared inventory, securely shares visibility of the similar diamond stones with retailers, and trusts that availability is universally updated at the time of ownership-transfer.

For retailers, the platform builds a profile around compliance and sustainability that reflects their purchase criteria and protect their brand's reputation through traceable journey of their diamond across the supply chain. The platform also allows retailers to go beyond 4Cs, i.e., by adding compliance, country, and the cognisance of mining and polishing events as entirely new dimensions of value. The platform provides them greater transparency and visibility to their suppliers. Moreover, they can see overall inventory, sustainability metrics, and diamond-compliance at a glance. It also enables them to confidently assert claims—made by leveraging an immutable audit trail—to substantiate certificate claims with third parties. We know that because of the use of blockchain, the platform supports product provenance to reduce fraud detection. But, it works under the assumption that the authentication of the services mechanisms are ISO27001-compliant, which unfortunately does not provide any objective standards that are automatically machine checkable when something goes wrong. Hence, we can say, it is unable to detect frauds automatically arising from subjective compliance of the authentication mechanisms.

Besides, an airbus developed a blockchain-based system [69] to track goods that will eventually become a complement to (not a wholesale replacement of) suppliers' procurement software. Analogously, Air France also started to plan introducing the blockchain-based solutions to improve aircraft maintenance-operations. Also, an American flight control systems producer 'Moog' is working on a blockchain-based platform to track aircraft parts, created by 3-D printers. In another project, HMM [70] plans to improve their service and its quality by adopting high-end IT technologies, such as blockchain and IoT, in shipping and logistics. This will help them to become one of the pioneers in fully traceable and transparent shipping and logistics services. Although, all of the above-mentioned projects are initiatives and the results have to come, therefore, it is difficult to judge their effectiveness.

#### 6.1.2. Security of Financial Transactions

Some of industrial tools mainly emphasis on the reliability and governance of digital trading-system using blockchain, especially in cargo and financial trading businesses. These tools employed a secure and traceable payment system, which is compliant with the directives to achieve traceability. For a secure financial trading, parties can anonymously compete for fair financial trade through establishing blockchain-based transparent and trancelable interactions among each other. For instance, OriginTrail [73] protocol was developed, which brought a trusted data sharing environment to supply chains by utilizing blockchain technology. The goal of OriginTrail is to establish a foundation for the next generation of business supply chain applications. In principle, OriginTrail ensures data integrity and validation in inter-organizational environments of supply chain, based on globally recognized standards and powerful graph data structures. The solution stack of the OriginTrail consists of the four layers, including application layer, ODN layer, ODN data layer, and blockchain layer. The *application layer* provides seamless integration for a broad ecosystem of supply chain management tools. Decentralized applications running on top of OriginTrail increases efficiency and integrity in supply chain management, insurance, banking, and other industries. Next, the *ODN (OriginTrail decentralized network) layer* supports scalability with its own off-blockchain network. A decentralized network of nodes enables key blockchain-like capabilities that are particularly relevant for supply chains focused on data governance and accessibility. Whereas, the *ODN data layer* provides

a highly performance and decentralized graph-database that connects data sets across supply chains. The layer establishes interoperability by supporting global standards for data exchange, while sensitive data is protected using a zero-knowledge privacy sublayer. Interoperability is established by building upon globally recognized GS1 standards for master data (descriptive attributes for products), transaction data (related to business relations), and visibility data (related to tracing and tracking) in addition to IoT and compliance data. In principle, data from different IT systems is transformed in a unified way, so the protocol can take full advantage of the relational nature of supply chain data. Once the data is aligned throughout the supply chain, consensus mechanism and the verification of data can take place. Furthermore, the privacy sublayer in ODN provides a zero-knowledge way for validating sensitive data elements in successive events in the supply chain. It supports data encryption for sensitive data with specific publicly verifiable properties, which provides very powerful way to unlock great value from information that is deemed unshareable. On this account, the OriginTrail protocol is able to validate a whole supply chain in terms of quantity, based on the encrypted data shared between stakeholders involved in one supply chain. Finally, the *blockchain layer* stores data that cannot be tampered. To this end, each data set is immutably fingerprinted on the blockchain with cryptographic hashes. Furthermore, by virtualizing the blockchain layer, OriginTrail can be used with different blockchains. This ensures flexibility and longevity of the protocol.

Despite, OriginTrail network is a special purpose network to ensure data security and privacy, it only supports security and privacy of data at network layer. It cannot be directly applied to establish end-to-end security and privacy of data along its journey across the supply chain. This limitation is because of the involvement of several other layers like application layer, which is software specific and requires different techniques to protect data against security and privacy breaches.

Daimler AG and Landesbank Baden-Württemberg (LBBW) [71] have jointly developed a blockchain-based platform to execute a financial transaction. The platform has been successfully tested for capital markets in parallel with the process that is required by regulatory authorities. Through LBBW, Daimler launched a €100 million 1 year corporate Schuldschein which is lead by Kreissparkasse Esslingen-Nürtingen, Ludwigsburg and Ostalb and LBBW. The platform together with the IT subsidiaries TSS (Daimler) and Targens (LBBW), successfully performed the entire transaction, i.e., from the origination, distribution, allocation, and execution of the Schuldschein loan agreement to the confirmation of repayment and interest payments. In another project Dianrong (one of China's top peer-to-peer lending platforms) [72] has employed blockchain-based system to its loans assessment system. The project aimed at helping small and medium suppliers with unsteady cash flows, breaching the last mile of creditworthiness to obtain financing. The proof of concept was developed and demonstrated last year, when Dianrong set up 'Chained Finance' with FnConn. Chained Finance originated US\$6.5 million in loans for small and medium suppliers in a successful pilot. In another interesting project, Slock [75] (who is the smart contract lock run on the Ethereum blockchain) together with RWE (energy giant) started a project that aimed at revolutionising the way the electric cars are charged. They developed a blockchain-based wallet that enabled cars to "talk" to autonomous electric charging stations which use smart contracts to allow users to rent the station, put up a deposit, charge their car, then get their deposit back. In spite of successful projects with real-time case studies, the lack of documentation and evidence made it difficult to analyze these projects in terms of their effectiveness, scalability, and security.

### 6.1.3. Interoperability and Secure Information Exchanged

To ensure interoperability among various cross-border systems and infrastructures in a secure way, industry experts devised block-chain based solutions to seamlessly interoperate digital trade among various cross-border parties. Such solutions enable traceable interactions among parties to establish confidence and trust among cross-border business partners. Since the cross-border communication requires dispute handling, therefore, some experts

emphasised on the developing of solutions that automatically resolve digital dispute that arises from cross-border companies through recording all interactions among parties in a blockchain. One of such replicable solutions is developed by IBM Blockchain [80] that transforms dispute resolution between multiple parties of supply chain. In IBM solution, the blockchain network serves as a single source of ground truth that is visible to only permissioned parties. The agreements and business rules are automatically executed by smart contracts. In principle, stakeholders send processed data to the blockchain directly from their recording-systems, and grant visibility to selected/permitted participants. By not granting visibility to anyone else, the privacy is preserved in a multi-participant environment. This also avoids errors that come from manual data entry processes. Next, business logic of the solution identifies discrepancies between data elements and documents to determine the root cause of any dispute. For example, in a supply chain process, a dispute can occur due to a measurement-unit error, a delivery location error, or the quantity delivered? Considering an example of the settlement of roaming charged by a telecom sector, everyone needs to agree on consumed data, text and voice, and rates to be charged. Here, all comparisons are performed on a near real-time basis as new data becomes available. As a result, disputes are identified and handled as they occur, dramatically reducing dispute resolution cycle time. IBM's platform supports automated dispute resolution rules synthesize the discrepancy data to reach consensus. The consensus decision, along with the applied rules, is made visible to all required participants. Consequently, final consensus decisions are then sent back to the system of record. All data, discrepancies and resulting decisions are stored within the blockchain distributed ledger to create a comprehensive and immutable audit history. The main problem of the IBM's platform is its inability to resolve disputes where cross-chains and cross-border interactions are allowed. Also, it cannot handle those disputes that are raised due to the processes which are not programmed using smart contracts.

Like IBM, Google also launched an exciting platform [77] for verifiable data audit using blockchain. Every time, the platform adds an entry to a special digital ledger, once there is any interaction with data. That entry records the fact that a particular piece of data has been used, and also the corresponding reason, e.g., "the blood test data was checked against the NHS national algorithm to detect possible acute kidney injury". The ledger and its entries share some of the properties of blockchain, like the idea behind Bitcoin and other projects. Like a blockchain, the ledger is append-only, so once a record of data use is added, it can't later be erased. Also, the ledger make it possible for third parties to verify the tampered entries.

The platform differs blockchain in couple of ways. Firstly, the blockchain is decentralised, whose ledger verification is determined by consensus amongst the participants. To prevent abuse, most blockchains require participants to repeatedly carry out complex calculations, with huge associated costs (according to some statistics, the total energy usage of blockchain participants could be as much as the power consumption of Cyprus). Unlike blockchain, verifiable data audit does not follow blockchain, and avoids the waste of energy-resources. Because, when it comes to the health service, the platform already has trusted institutions like hospitals and national bodies who can be relied on to verify the integrity of ledgers. Secondly, the developed platform is more efficient as it replaces the chain concept with a tree-like structure. However, overall the functionality of verifiable data audit is much similar to the blockchain. But, the operational effect is different because every time the platform adds an entry to the ledger, it generates a value known as a "cryptographic hash", which summarises not only the latest entry, but all of the previous values in the ledger too. This effect makes it effectively impossible for someone to go back and quietly alter one of the entries, since that will not only change the hash value of that entry but also that of the whole tree.

Industrial efforts have been demonstrated successfully, however, their outcomes are yet to be evaluated against the actual impact and their practical effectiveness.

## 6.2. Efforts against Computational Attacks

Again, the computational attacks exploit the vulnerabilities in computational processes of the system. In a supply chain domain, industries address these vulnerabilities by establishing compliance of supply chain operations and crypto-currencies transactions [82–85] and identifying vulnerabilities in smart contracts and in their underlying execution environment (e.g., EVM) [86–91]. We investigated these industrial efforts in detail in coming subsections, based on the security requirement and threat model of the blockchain based supply chain systems. The investigation summary is summed up in Table 6.

**Table 6.** Handling Computational Attacks—Industrial Solutions.

Paper	Application Areas	Target Operations	Key Contributions	Affected Requirements	Potential Attack Mechanisms
[82–85]	Regulators, Finance, Security agencies, IoT	Transaction compliance	Data compliance, Regulation compliance, Monitoring information exchange	Traceability, Privacy	Execution modification (rewriting attacks)
[86–91]	Enterprise business network	Vulnerability detection	Transfer amount vs. req. amount, Transaction debugging, Control flow graph, Non-validated arguments, Exception handling, Overflow and Underflow	Traceability, Transparency, Privacy	Vulnerability exploit, Execution modification

### 6.2.1. Security to Transactions and Operations

In fact, industries are interested in developing solutions to support more practical business models. In this regard, the main effort of industries is to secure the crypto-currency transactions and operations by establishing the compliance of transactions among different stakeholders. For instance, IBM's IoT [85] platform supports compliance of IoT enabled supply chain processes in their specific operations and interactions. Supply chain is supported through tracking of objects, as they traverse the export/import supply chain while enforcing shipping and line of credit contracts, and expediting incremental payments. The warranty of products and their parts is maintained through an indelible history of parts and end-assembly through supply chain management, potentially including critical events that affect their life or scheduled maintenance. This information can be shared with supply chain stakeholders, OEM, and regulators in a secure way. Decentralized edge computing implements secure computing of workloads, such as analytics, on edge devices owned by 3rd parties. Micro-payments are used to pay for services. Inter-connectivity among devices enable distributed devices to request and pay for services through distributed role management and micro-payments through micro-services. Regulatory compliance is established by tracking equipment or process history in an indelible record and enabling easy sharing of this information with regulatory agencies or insurers. Although, the platform only supports compliance of data shared among various stakeholders and their devices, it is limited to support compliance of business processes that may involve cross-chains and cross-border regulations.

IBM's reported [84] that several regulation-initiatives have been started around the globe to promote blockchain technology to lower costs while increasing transparency. The U.S. Securities and Exchange Commission (SEC) formed a Distributed Ledger Technology Working Group to build expertise, identify emerging risk areas, and coordinate efforts among the SEC's divisions and offices. The group consists of over seventy members that assist in coordination with federal, state, and local law enforcement and regulatory partners, and liaising with industry. Similarly, The Bank of England, working with a consulting firm, has developed a multi-node scalable blockchain platform that contains several "smart contracts" to illustrate the applications of the technology. The European Securities and Markets Authority has recently published the results of its 2016 market consultation exercise, and in the U.S., the Financial Industry Regulatory Authority is in a similar market exercise. Also, the Hong Kong Monetary Authority launched its "Fintech Supervisory Sandbox" that allows banks to conduct pilot trials in a controlled production

environment, without the need to achieve full compliance. A few banks are in discussions for projects in areas such as blockchain and artificial intelligence.

#### 6.2.2. Security to Smart Contracts and Their Execution Environment

In addition to providing security to crypto-currency transactions and operations, industries also developed tools to identify vulnerabilities in smart contracts and their underlying virtual execution environment. These vulnerabilities include (but not limited to) short address stack, delegate call, blockchain ingestion, wallet theft, double-spending, cryptojacking, default visibilities, and transaction ordering dependence. In order to identify such vulnerabilities, the developed tools [86–91] perform static analysis on source code and byte code of smart contracts, dynamic analysis of the contract execution, symbolic analysis of the contract code and execution, and verification-based analysis of smart contracts.

One of the popular tool that supports identification of security vulnerabilities is SlithIR [91]. Slither translates smart contracts developed in Solidity to an intermediate representation ‘SlithIR’ to enable high-precision analysis via a simple API. The translation supports taint and value tracking to enable detection of complex patterns. The intermediate language includes extra details about the program when it is parsed. For example, a compiler creates a parse tree of a written-program, represents its functionality. The compiler enriches this tree with information, such as taint information, source location, and other items that could have impacted an item from control flow (e.g., resources). Furthermore, languages such as Solidity supports inheritance property, which enables functions and methods to be defined outside the scope of a given contract. An IR linearizes these methods, allowing additional transformations and processing of the contract’s source code. By translating Solidity into an IR, Slither normalizes many of these quirks to better analyze the contract. For Example, contract’s grammar defines an array-push as a function call to the array, and representation of this semantic would be indistinguishable from a normal function call. Slither, in contrast, treats array pushes as a specific operation, allowing further analysis of the accesses to arrays and their impact to the security of a program. Furthermore, the operators in SlithIR have a hierarchy, which enable anyone to track all the operators that write to a variable, making it trivial to write precise taint analysis. Slither also supports non-trivial variable tracking by default as identifiable by IR. This builds richer representations of contracts that allow deeper analysis of potential security vulnerabilities. For Instance, investigating a question like “can a user control a variable” is central to uncovering more complex vulnerabilities from a static position. Slither propagates information from function parameters to program state in an iterative way, which captures the control flow information across potentially multiple transactions. Based on the propagation, Slither enriches information and statically provide a stronger assurance to contracts for identifying existence of standard vulnerabilities that are reachable under certain suspicious conditions [91].

Ethereum graph debugger (EGD) [88] is a graphical debugger for identifying security vulnerabilities in the smart contract-based transactions and their execution environment. In contrast to typical debuggers, EGD debugger shows the whole program control flow graph and the actual execution of the transaction highlighted in red, which helps developer to see the whole execution flow and jump anywhere in a quick and graphical way. There are several key features of the debugger, e.g.,

- Control flow graph: the CFG can be built without debugging a transaction.
- Disassembler: just disassembled opcodes can be seen, from runtime and constructor.
- Source mapping: snippet of code related to the selected instruction is highlighted in the editor left panel.
- Debug transaction: a transaction can be debugged using the contract’s CFG and the execution trace.
- Storage viewer: Storage layout and values can be retrieved (including dynamic arrays and mappings).

- Supports contracts calls: All contracts involved in the transaction can be debugged (going to the caller/called tab to see the contract-specific trace).
- EVM state in transaction: it is shown below the editor when selecting an opcode present in the execution trace of the provided transaction hash.
- and When building the CFG a basic dynamic execution is made to calculate jumps and to remove most of orphan blocks (this will be improved in the future, probably with SymExec).

The debugger is very helpful to understand the flow of the transaction but unfortunately it is only usable for development and production environment. It cannot be used in a meaningful way for automatic detection of consistencies in the transactions in real-time contracts.

Another tool MythX [89] was developed as a security analyzer that facilitates development teams to avoid costly errors and make Ethereum a more secure and trustworthy platform. The tool detects various costly vulnerabilities in the contracts, including assertion and property checking, byte-code safety, authorization control, control flow, ERC standards, and Ethereum best practices. The tool employed different analysis to detect vulnerabilities, such as static analysis, dynamic analysis, and symbolic analysis. However, it can only evaluate security of Ethereum specific contracts with the assumption that all involved stakeholders are securely interacting with the contract, which is not the case in real-environment.

## 7. Research Gaps and Future Opportunities

Based on the security requirements of supply chain system as sketched in Table 2, and analysis of academic and industrial efforts to prevent communication and computational attacks, we have identified following gaps (opportunities) that need to be considered to better support end-to-end protection of blockchain-based supply chain business against communication and computational attacks.

### 7.1. Protection against Communication Attacks

We have identified the following opportunities to improve protection against communication attacks where the main focus of the blockchain-based systems is to ensure protection of communicated information, while the communication attacks on such systems are focused on developing mechanisms to compromise information and identity in different ways.

#### 7.1.1. Lack of Transparency and Privacy

Current blockchain-based solutions provide a full trace of interactions (i.e., data exchange) among various stakeholders involved in the blockchain. Yet, they fail to provide adequate transparency to its interacting stakeholders and customers, mainly because the blockchain based solutions consider all of the interacting components (i.e., implementation of computing/business process) as “blockbox” with very little information about their actual operations such as implementations of business/computing processes and APIs. Also, the only information the blockchain contains about stakeholders is the smart contract that is transaction specific. Thus, the blockchain-based solutions typically provide limited protection to supply chain systems. Resultantly, without the information of stakeholder’s entire supply chain business process implementation and based on the full trace of supply interactions, such solutions fail to identify concrete information about “why” a certain incident/compromise took place. Furthermore, getting full trace of supply interactions actually depends on the system design: some recent systems adopt the so called on chain and off-chain transactions to keep the maximum amount of tracing data. Due to the lack of transparency, partners and customers become more concerned about their data privacy and finally, may lose their trust in system operations.

### 7.1.2. Lack of Awareness

BC-SCM systems deliver information security by storing the information exchanged among different interacting stakeholders in an encrypted chain of blocks (i.e., distributed ledger). The chain is tamper-proof and able to detect any kind of modification of data. Also, such solutions are good at detecting what information has been compromised. However, since they are not aware of the information semantics (i.e., business process implementation that generated the information), they failed to determine potential impact of the compromised information. For instance, in case of a security incident, current solutions could not exactly identify what is the incident. In this case, they have very limited resolution information, resulting in failure to mitigate the impact of the incident on one hand; on the other hand, they are not able to initiate a relevant recovery strategy. Since blockchain-based solutions demand high credibility of the involved stakeholders, it becomes challenging for stakeholders to establish trust in the business if no victim is identified when something goes wrong. More recently, there have been some efforts [92,93] to develop semantic aware blockchain and smart contracts that partially consider the meta-data (i.e., process level information) to analyze the system security.

### 7.1.3. Lack of Context

Blockchain-based solutions have no information about the actual supply chain process—except transaction details and related information of business parts—through which the information has been generated or exchanged. Therefore, they are unable to understand the actual context of the compromise, which is very critical in detecting modern day multi-stage attacks with cascading effects. To support automated decision making in the supply chain, knowing context of undesired incidents is a key; without a context, it will not be possible to automatically mitigate impact of such threats and recover from such incidents.

### 7.1.4. Lack of Understanding

We know, BC-SCM solutions are employed to record communication (i.e., data exchange) among different stakeholders of a supply chain system. Due to lack of information about communication process (i.e., communication/computing protocol), BC-SCM solutions may not be able to comprehend intentions of the attacker or adversary. Therefore, they could not succeed to provide cognitive and intelligent protection against known as well as unknown attacks. In principle, any computing process/communication protocol may have different implementations, which implies that even though the implementations are producing the same output they may be vulnerable to different attacks because they have been implemented in different ways (i.e., using different libraries). Therefore, it is important to understand process/implementation level details in order to make systems self-aware as well as to identify attacker's intentions.

## 7.2. Protection against Computational Attacks

There are gaps in self-awareness, business process integration, and support for business evolution that need to be filled to improve the protection against computational attacks. The BC-SCM systems must ensure operational compliance with certain policies and directives, while identifying vulnerabilities and their exploitation in various computational parts of the system, e.g., smart contracts and virtual machines.

### 7.2.1. Lack of Self-Awareness

The blockchain-based supply chain systems typically have no information about the actual process—the process could be cyber or physical component/interface in Industry 4.0—through which the data has been generated or exchanged. These systems do not understand what they are trying to do with a certain input data. Therefore, we can say that they are not self-aware. Hence, due to the lack of business process information of the involved stakeholders, such systems could not detect advanced and complex attacks, arising due to either insiders or external adversaries with the knowledge of parts or

processes or sub-processes. Furthermore, without self-awareness, the main purpose of supply chain automation cannot be achieved, because of its requirement of high-degree of trust among stakeholders.

#### 7.2.2. Lack of Business Process Integration

Contemporary blockchain solutions in supply chain enforce protection of the information as per implementation of the smart contract, which mainly consists of rules for transactions and their compliance. However, the contracts only implement rules that are related to the transactions, and they have no information about the actual business process level agreements for the involved stakeholders. Therefore, such solutions may not detect threats that cause or impact on the involved stakeholders business, which is mostly the case in modern attacks as the goal of attackers is to damage the actual business assets or resources. Hence, due to the lack of integration of actual business process agreements of the stakeholders, such solutions cannot protect the business resources. This also hinders transparency of the supply chain business, because it is hard to identify which asset/resource of the involved stakeholders has been compromised.

#### 7.2.3. Lack of Support for Business Evolution

Typical BC-SCM solutions implement various agreements among involved parties/stakeholders in smart contracts, which hard codes agreements as rules. In practice, businesses keep evolving due to several reasons (e.g., changing business policies) and also their underlying processes and agreements also evolve. On the other hand, due to recent governance developments, various involved stakeholders, products, producers, and consumers also need to comply with various general directives. These directives can be GDPR [94] or domain specific directives, such as unfair trading in the agriculture and food supply chain [95,96]. Hard coded nature of such process agreements make these solutions incapable of integrating evolved business processes and changing business requirements as well as their compliance against emerging directives. Therefore, such solutions become infeasible on one hand and introduce inconsistencies between actual business process agreements and their corresponding implementation in smart contract on the other hand.

#### 7.3. Recommendations

Based on the identified research gaps as above, it is desired to equip current blockchain-based solutions with the information of actual business processes (i.e., computational components) and communication infrastructure (i.e., communication components) that enables various stakeholders to interact using blockchain-based supply chain environment. In the following, we discuss various ways in which business process level information of interacting stakeholders can be helpful to protect end-to-end operations of BC-SCM systems.

Firstly, information of the business process of interacting stakeholders strengthens blockchain enabled protection of supply chain management systems by making sure that interaction (including smart contracts) among stakeholders is not only compliant with the rules encoded in smart contracts but also compliant with their corresponding business processes. This will ensure that the interactions are deeply transparent and being compliant with their business processes. This also helps in detecting those threats that have cascading effects to their interacting business.

Secondly, such information will help developing self-aware and cognitive protection system for supply chain stakeholders by providing practical business context of the interactions (e.g., smart contract based), protecting information against critical infrastructure-targeting attacks as well as variant of known attacks. Furthermore, the information may also be used to ensure that smart contract-based interactions among stakeholders are consistent with business process of the stakeholders. Further, it is also possible to detect potential errors/inconsistencies in the stakeholders business processes that provide end-to-end protection of the information.



Thirdly, business process-level information also support evolving business policies/agreements without changing actual implementation of the blockchain based interactions. This is critically important because the business process is continuously evolving due to the changing business requirements or their compliant with emerging directives and policies, e.g., GDPR.

Fourthly, the business process information could also help in understanding the actual cause of a threat or attack. The system will not only be aware of the interactions (e.g., which are typically interface for transactions only) but also aware of the end-to-end details of the corresponding business process. In fact, current blockchain based systems only records interactions (e.g., data) which can only help to see any compromise to the information but fails to detect compliance/integrity of the actual contents of the information.

Fifthly, such information may be adequate not only to recover compromised operations but may also be helpful to automatically mitigate impact of the identified threats/attacks, due to the system's ability to identify exact asset/component that has been compromised. Thus, the information will help in detecting incidents as well as their impacts.

Finally, with such information, blockchain based systems would be more transparent with known potential reasons of a threat/attack incident. Since current interactions—including transaction rules—among stakeholders are based on smart contract, and they have limited information about the actual business process of the stakeholders, thus they are like blackboxes. Therefore, with the transparent business process to partners, this information can establish more trust among interacting stakeholders.

Consequently, business process information of supply chain stakeholders will strengthen protection that is provided by BC-SCM systems through providing end-to-end details of the interactions. This will not only detect attack-incidents but can also help in (i) understanding and reducing actual impact of the incidents, (ii) providing context-aware audit of the incidents that may identify compromised information, and ensure authenticity of the information contents, and (iii) improving confidence of stakeholders due to the end-to-end transparency of the interactions that is not only limited to transparency of transactions in smart contracts but includes transparency of actual business process of the interacting stakeholders. Finally, such information could help in handling vulnerabilities in business processes that will enable stakeholders to improve their business needs/targets.

## 8. Conclusions

In this paper, initially, we established key security requirements and threat model for blockchain-based supply chain management systems. Based on the identified threat model, the attacks are categorised as communicational and computational. We thoroughly investigated existing BC-SCM systems, handling such attacks systems Furthermore, We figured out several research gaps in existing systems and identified key opportunities in the domain of BC-SCM to make existing systems more effective, flexible and rigorous. Finally, we provided some recommendations to keep business process information and underlying communication infrastructure as a part of the BC-SCM system. We argued that the system with following recommendations can provide adequate information for rigorous protection of critical assets and information against known as well as unseen attacks. Moreover, such information also enables solutions to automatically enforce various policies and directives on one hand and to detect any error or bug in the system (i.e., detected as an inconsistency between business process and its underlying implementation) on the other hand. Furthermore, such information makes the solutions more cognitive as it will enable them to understand what they are doing, determine exact causes of the threat, and automatically mitigate the impact of the threat. Importantly, the recommended systems will provide partners and citizens actual cause of the threat achieving the real transparency of the protection of their business assets and critical information.

**Author Contributions:** Conceptualization, S.A.-F., M.M.R. and S.B.; methodology, S.A.-F.; investigation, S.A.F.; writing—original draft preparation, S.A.-F.; writing—review and editing, S.A.-F. and M.M.R.; supervision, S.B. All authors have read and agreed to the published version of the manuscript.

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

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

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

## References

1. Wright, A.; De Filippi, P. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *SSRN Electron. J.* **2015**. [CrossRef]
2. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 839–858.
3. Pilkington, M. Blockchain Technology: Principles and Applications. In *Research Handbook on Digital Transformations*; Ollerros, F.X., Zhegu, M., Eds.; Research Handbooks in Business and Management; Edward Elgar Publishing: Cheltenham, UK, 2016; Chapter 11, pp. 225–253. [CrossRef]
4. Kitchenham, B.; Brereton, O.P.; Budgen, D.; Turner, M.; Bailey, J.; Linkman, S. Systematic literature reviews in software engineering—A systematic literature review. *Inf. Softw. Technol.* **2009**, *51*, 7–15. [CrossRef]
5. Keele, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Technical Report; Elsevier: Durham, UK, 2007.
6. Okoli, C.; Schabram, K. A guide to conducting a systematic literature review of information systems research. *SSRN Electron. J.* **2010**. [CrossRef]
7. Huan, S.H.; Sheoran, S.K.; Wang, G. A review and analysis of supply chain operations reference (SCOR) model. *Supply Chain. Manag. Int. J.* **2004**. [CrossRef]
8. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*; Technical Report; Satoshi Nakamoto Institute: Austin, TX, USA, 2019.
9. Kshetri, N. 1 Blockchain's roles in meeting key supply chain management objectives. *Int. J. Inf. Manag.* **2018**, *39*, 80–89. [CrossRef]
10. Gstettner, S. How Blockchain Will Redefine Supply Chain Management. Available online: <https://knowledge.wharton.upenn.edu/article/blockchain-supply-chain-management/> (accessed on 31 March 2021).
11. Corkery, M.; Popper, N. From farm to blockchain: Walmart tracks its lettuce. *The New York Times*, 24 September 2018.
12. Bandoim, L. Can Blockchain And Chip Technology Improve Beef Sourcing Transparency? *Forbes*, 30 April 2019.
13. Vitasek, K. Walmart Canada And DLT Labs Launch World's Largest Industrial Blockchain Application. *Forbes*, 31 January 2020.
14. Mackey, T.K.; Nayyar, G. A review of existing and emerging digital technologies to combat the global trade in fake medicines. *Expert Opin. Drug Saf.* **2017**, *16*, 587–602. [CrossRef] [PubMed]
15. Lu, Q.; Xu, X. Adaptable blockchain-based systems: A case study for product traceability. *IEEE Softw.* **2017**, *34*, 21–27. [CrossRef]
16. Mansfield-Devine, S. Beyond Bitcoin: Using blockchain technology to provide assurance in the commercial world. *Comput. Fraud. Secur.* **2017**, *2017*, 14–18. [CrossRef]
17. Korpela, K.; Hallikas, J.; Dahlberg, T. Digital supply chain transformation toward blockchain integration. In Proceedings of the 50th Hawaii International Conference on System Sciences, Hilton Waikoloa Village, HI, USA, 4–7 January 2017. [CrossRef]
18. Wang, J.; Wu, P.; Wang, X.; Shou, W. The outlook of blockchain technology for construction engineering management. *Front. Eng. Manag.* **2017**, 67–75. [CrossRef]
19. Saberi, S.; Kouhizadeh, M.; Sarkis, J. Blockchain technology: A panacea or pariah for resources conservation and recycling? *Resour. Conserv. Recycl.* **2018**, *130*, 80–81. [CrossRef]
20. Lee, J.H.; Pilkington, M. How the blockchain revolution will reshape the consumer electronics industry [future directions]. *IEEE Consum. Electron. Mag.* **2017**, *6*, 19–23. [CrossRef]
21. 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]
22. Min, H. Blockchain technology for enhancing supply chain resilience. *Bus. Horiz.* **2019**, *62*, 35–45. [CrossRef]
23. Joshi, A.P.; Meng Han, Y.W. A survey on security and privacy issues of blockchain technology. *Math. Found. Comput.* **2018**, *1*, 121. [CrossRef]
24. Hackius, N.; Petersen, M. Blockchain in logistics and supply chain: Trick or treat? In *Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg International Conference of Logistics (HICL)*; Kersten, W., Blecker, T., Ringle, C.M., Eds.; epubli GmbH: Berlin, Germany, 2017; Volume 30, pp. 3–18. [CrossRef]
25. Al-Jaroodi, J.; Mohamed, N. Blockchain in Industries: A Survey. *IEEE Access* **2019**, *7*, 36500–36515. [CrossRef]

26. Xie, J.; Tang, H.; Huang, T.; Yu, F.R.; Xie, R.; Liu, J.; Liu, Y. A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2794–2830. [[CrossRef](#)]
27. Benčić, F.M.; Skočir, P.; Žarko, I.P. DL-Tags: DLT and Smart Tags for Decentralized, Privacy-Preserving, and Verifiable Supply Chain Management. *IEEE Access* **2019**, *7*, 46198–46209. [[CrossRef](#)]
28. Hackius, N.; Reimers, S.; Kersten, W. The Privacy Barrier for Blockchain in Logistics: First Lessons from the Port of Hamburg. In *Logistics Management*; Bierwirth, C., Kirschstein, T., Sackmann, D., Eds.; Springer: Cham, Switzerland, 2019; pp. 45–61.
29. Tseng, J.H.; Liao, Y.C.; Chong, B.; Liao, S.W. Governance on the Drug Supply Chain via Gcoin Blockchain. *Int. J. Environ. Res. Public Health* **2018**, *15*, 1055. [[CrossRef](#)]
30. Holland, M.; Stjepandić, J.; Nigischer, C. Intellectual Property Protection of 3D Print Supply Chain with Blockchain Technology. In Proceedings of the 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Stuttgart, Germany, 17–20 June 2018; pp. 1–8. [[CrossRef](#)]
31. Gao, F.; Zhu, L.; Shen, M.; Sharif, K.; Wan, Z.; Ren, K. A Blockchain-Based Privacy-Preserving Payment Mechanism for Vehicle-to-Grid Networks. *IEEE Netw.* **2018**, *32*, 184–192. [[CrossRef](#)]
32. Jabbar, S.; Lloyd, H.; Hammoudeh, M.; Adebisi, B.; Raza, U. Blockchain-enabled supply chain: Analysis, challenges, and future directions. *Multimed. Syst.* **2020**. [[CrossRef](#)]
33. Koens, T.; Poll, E. Assessing interoperability solutions for distributed ledgers. *Pervasive Mob. Comput.* **2019**, *59*, 101079. [[CrossRef](#)]
34. Johnson, S.; Robinson, P.; Brainard, J. Sidechains and interoperability. *arXiv* **2019**, arXiv:cs.CR/1903.04077.
35. Deng, L.; Chen, H.; Zeng, J.; Zhang, L.J. Research on Cross-Chain Technology Based on Sidechain and Hash-Locking. In *Edge Computing—EDGE 2018*; Liu, S., Tekinerdogan, B., Aoyama, M., Zhang, L.J., Eds.; Springer: Cham, Switzerland, 2018; pp. 144–151.
36. Wen, Q.; Gao, Y.; Chen, Z.; Wu, D. A Blockchain-based Data Sharing Scheme in The Supply Chain by IIoT. In Proceedings of the 2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS), Taipei, Taiwan, 6–9 May 2019; pp. 695–700. [[CrossRef](#)]
37. Sidorov, M.; Ong, M.T.; Sridharan, R.V.; Nakamura, J.; Ohmura, R.; Khor, J.H. Ultralightweight Mutual Authentication RFID Protocol for Blockchain Enabled Supply Chains. *IEEE Access* **2019**, *7*, 7273–7285. [[CrossRef](#)]
38. 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*, 5. [[CrossRef](#)]
39. Maouchi, M.E.; Ersoy, O.; Erkin, Z. DECOUPLES: A Decentralized, Unlinkable and Privacy-Preserving Traceability System for the Supply Chain. In Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, Limassol, Cyprus, 8–12 April 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 364–373. [[CrossRef](#)]
40. Smit, K.; Mansouri, J.; Said, S.; Meerten, J.; Leewis, S. Decision Rights and Governance within the Blockchain Domain: A literature analysis. In Proceedings of the Pacific Asia Conference on Information Systems, Dubai, United Arab Emirates, 22–24 June 2020.
41. Allen, D.; Berg, C.; Davidson, S.; Novak, M.; Potts, J. International policy coordination for blockchain supply chains. *Asia Pac. Policy Stud.* **2019**, *6*. [[CrossRef](#)]
42. Schulte, S.; Sigwart, M.; Frauenthaler, P.; Borkowski, M. Towards Blockchain Interoperability. In *Business Process Management: Blockchain and Central and Eastern Europe Forum*; Di Ciccio, C., Gabryelczyk, R., García-Bañuelos, L., Hernaus, T., Hull, R., Indihar Štemberger, M., Kő, A., Staples, M., Eds.; Springer: Cham, Switzerland, 2019; pp. 3–10.
43. Pillai, B.; Biswas, K.; Muthukumarasamy, V. Blockchain Interoperable Digital Objects. In *Blockchain—ICBC 2019*; Joshi, J., Nepal, S., Zhang, Q., Zhang, L.J., Eds.; Springer: Cham, Switzerland, 2019; pp. 80–94.
44. Lima, C. Developing Open and Interoperable DLTBlockchain Standards [Standards]. *Computer* **2018**, *51*, 106–111. [[CrossRef](#)]
45. Astill, J.; Dara, R.A.; Campbell, M.; Farber, J.M.; Fraser, E.D.; Sharif, S.; Yada, R.Y. Transparency in food supply chains: A review of enabling technology solutions. *Trends Food Sci. Technol.* **2019**, *91*, 240–247. [[CrossRef](#)]
46. Jayaraman, R.; Salah, K.; King, N. Improving Opportunities in Healthcare Supply Chain Processes via the Internet of Things and Blockchain Technology. *Int. J. Healthc. Inf. Syst. Inform. (IJHISI)* **2019**, *14*, 49–65. [[CrossRef](#)]
47. Chen, Y.; Ding, S.; Xu, Z.; Zheng, H.; Yang, S. Blockchain-Based Medical Records Secure Storage and Medical Service Framework. *J. Med. Syst.* **2018**, *43*, 5. [[CrossRef](#)]
48. Mondal, S.; Wijewardena, K.P.; Karuppuswami, S.; Kriti, N.; Kumar, D.; Chahal, P. Blockchain Inspired RFID-Based Information Architecture for Food Supply Chain. *IEEE Internet Things J.* **2019**, *6*, 5803–5813. [[CrossRef](#)]
49. Makhdoom, I.; Zhou, I.; Abolhasan, M.; Lipman, J.; Ni, W. PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Comput. Secur.* **2020**, *88*, 101653. [[CrossRef](#)]
50. Salah, K.; Nizamuddin, N.; Jayaraman, R.; Omar, M. Blockchain-Based Soybean Traceability in Agricultural Supply Chain. *IEEE Access* **2019**, *7*, 73295–73305. [[CrossRef](#)]
51. Zhu, L.; Wu, Y.; Gai, K.; Choo, K.K.R. Controllable and trustworthy blockchain-based cloud data management. *Future Gener. Comput. Syst.* **2019**, *91*, 527–535. [[CrossRef](#)]
52. Dolgui, A.; Ivanov, D.; Potryashev, S.; Sokolov, B.; Ivanova, M.; Werner, F. Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain. *Int. J. Prod. Res.* **2020**, *58*, 2184–2199. [[CrossRef](#)]
53. Cheng, R.; Zhang, F.; Kos, J.; He, W.; Hynes, N.; Johnson, N.; Juels, A.; Miller, A.; Song, D. Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy (EuroSP), Stockholm, Sweden, 17–19 June 2019; pp. 185–200. [[CrossRef](#)]

54. Zhang, S.; Lee, J.H. Smart Contract-Based Miner Registration and Block Validation. In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, Auckland, New Zealand, 9–12 July 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 691–693. [CrossRef]
55. Kalra, S.; Goel, S.; Dhawan, M.; Sharma, S. ZEUS: Analyzing Safety of Smart Contracts. In Proceedings of the Network and Distributed Systems Security (NDSS) Symposium 2018, San Diego, CA, USA, 18–21 February 2018. [CrossRef]
56. Albert, E.; Gordillo, P.; Livshits, B.; Rubio, A.; Sergey, I. EthIR: A Framework for High-Level Analysis of Ethereum Bytecode. In Proceedings of the 16th International Symposium, ATVA 2018, Los Angeles, CA, USA, 7–10 October 2018; pp. 513–520. [CrossRef]
57. Tsankov, P.; Dan, A.; Drachler-Cohen, D.; Gervais, A.; Bünzli, F.; Vechev, M. Securify: Practical Security Analysis of Smart Contracts. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 67–82. [CrossRef]
58. Chen, T.; Li, X.; Luo, X.; Zhang, X. Under-optimized smart contracts devour your money. In Proceedings of the 2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER), Klagenfurt, Austria, 20–24 February 2017; pp. 442–446. [CrossRef]
59. Karamitsos, I.; Papadaki, M.; Barghuthi, N. Design of the Blockchain Smart Contract: A Use Case for Real Estate. *J. Inf. Secur.* **2018**, *9*, 177–190. [CrossRef]
60. Baza, M.; Nabil, M.; Ismail, M.; Mahmoud, M.; Serpedin, E.; Ashiqur Rahman, M. Blockchain-Based Charging Coordination Mechanism for Smart Grid Energy Storage Units. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 504–509. [CrossRef]
61. Falazi, G.; Hahn, M.; Breitenbücher, U.; Leymann, F.; Yussupov, V. Process-Based Composition of Permissioned and Permissionless Blockchain Smart Contracts. In Proceedings of the 2019 IEEE 23rd International Enterprise Distributed Object Computing Conference (EDOC), Paris, France, 28–31 October 2019; pp. 77–87. [CrossRef]
62. Feist, J.; Grieco, G.; Groce, A. Slither: A Static Analysis Framework for Smart Contracts. In Proceedings of the 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), Montreal, QC, Canada, 27 May 2019; pp. 8–15. [CrossRef]
63. Wang, H.; Li, Y.; Lin, S.; Ma, L.; Liu, Y. VULTRON: Catching Vulnerable Smart Contracts Once and for All. In Proceedings of the 2019 IEEE/ACM 41st International Conference on Software Engineering: New Ideas and Emerging Results (ICSE-NIER), Montreal, QC, Canada, 25–31 May 2019; pp. 1–4. [CrossRef]
64. Mezquita, Y.; Valdeolmillos, D.; González-Briones, A.; Prieto, J.; Corchado, J.M. Legal Aspects and Emerging Risks in the Use of Smart Contracts Based on Blockchain. In *Knowledge Management in Organizations*; Uden, L., Ting, I.H., Corchado, J.M., Eds.; Springer: Cham, Switzerland, 2019; pp. 525–535.
65. Luu, L.; Chu, D.H.; Olickel, H.; Saxena, P.; Hobor, A. Making Smart Contracts Smarter. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; Association for Computing Machinery: New York, NY, USA, 2016; pp. 254–269. [CrossRef]
66. Coblenz, M.; Sunshine, J.; Aldrich, J.; Myers, B.A. Smarter Smart Contract Development Tools. In Proceedings of the 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), Montreal, QC, Canada, 27 May 2019; pp. 48–51. [CrossRef]
67. Russo, C. Walmart Is Getting Suppliers to Put Food on the Blockchain. Available online: <https://www.bloomberg.com/news/articles/2018-04-23/walmart-is-getting-suppliers-to-put-food-on-blockchain-to-track> (accessed on 18 March 2021).
68. A Blockchain Platform for Transparency and Traceability. Available online: <https://www.everledger.io/industry-solutions/diamonds/> (accessed on 18 March 2021).
69. Alper, T. Airbus, Rolls-Royce Seeking Blockchain Air Parts Traceability Solution. Available online: <https://cryptonews.com/news/airbus-rolls-royce-seeking-blockchain-air-parts-traceability-1700.htm> (accessed on 18 March 2021).
70. HMM Completes Assessment on Blockchain Technology Adopted in Shipping & Logistics. Available online: [https://www.hmm21.com/cms/company/engn/introduce/prcenter/news/1203283\\_18539.jsp](https://www.hmm21.com/cms/company/engn/introduce/prcenter/news/1203283_18539.jsp) (accessed on 18 March 2021).
71. Sackmann, H. Daimler and LBBW Successfully Utilize Blockchain Technology for Launch of Corporate Schuldschein. Available online: <https://media.daimler.com/marsMediaSite/ko/en/22744703> (accessed on 18 March 2021).
72. Soo, Z. Blockchain Sharpens Dianrong’s Edge in P2P Lending to Small Businesses. Available online: <https://www.scmp.com/tech/leaders-founders/article/2102840/blockchain-sharpens-dianrongs-edge-p2p-lending-small> (accessed on 18 March 2021).
73. Lelicanin, V. OriginTrail Decentralized Network Overview. Available online: <https://github.com/OriginTrail/ot-node> (accessed on 18 March 2021).
74. Vornic, A. Blockchain Against Hunger: Harnessing Technology in Support of Syrian Refugees. Available online: <https://www.wfp.org/news/news-release/blockchain-against-hunger-harnessing-technology-support-syrian-refugees> (accessed on 18 March 2021).
75. Allison, I. RWE and Slock.it—Electric Cars Using Ethereum Wallets Can Recharge by Induction at Traffic Lights. Available online: <https://www.ibtimes.co.uk/rwe-slock-it-electric-cars-using-ethereum-wallets-can-recharge-by-induction-traffic-lights-1545220> (accessed on 18 March 2021).
76. World’s First Blockchain Coffee Project. Available online: <https://medium.com/@MoyeeCoffeeIRL> (accessed on 18 March 2021).
77. Suleyman, M.; Laurie, B. Trust, Confidence and Verifiable Data Audit. Available online: <https://deepmind.com/blog/trust-confidence-verifiable-data-audit> (accessed on 18 March 2021).

78. Rajamanickam, V. FedEx Plans to Create Common Logistics Standards in Association with BiTA. Available online: <https://www.freightwaves.com/news/fedex-bita-blockchain-logistics-plans> (accessed on 18 March 2021).
79. Ream, J.; Chu, Y.; Schatsky, D. Upgrading Blockchains: Smart Contract Use CASES in industry—Deloitte Insights. Available online: <https://www2.deloitte.com/insights/us/en/focus/signals-for-strategists/using-blockchain-for-smart-contracts.html> (accessed on 18 March 2021).
80. Dickinson, A. Blockchain for Invoice Reconciliation and Dispute Resolution. Available online: <https://www.ibm.com/blogs/blockchain/2020/11/blockchain-for-invoice-reconciliation-and-dispute-resolution/> (accessed on 18 March 2021).
81. Gutierrez, C.; Khizhniak, A. A Close Look at Everledger—How Blockchain Secures Luxury Goods. Available online: <https://www.altoros.com/blog/a-close-look-at-everledger-how-blockchain-secures-luxury-goods/> (accessed on 18 March 2021).
82. Biggart, G.; Bear, K. Unblocking the Blockchain. Available online: <https://www.ibm.com/thought-leadership/institute-business-value/report/unblocking> (accessed on 18 March 2021).
83. Blockchain for KYC: Game-Changing RegTech Innovation. Available online: <https://www.ibm.com/blogs/regtech/blockchain-kyc-game-changing-regtech-innovation/> (accessed on 18 March 2021).
84. AAIS: Enabling Regulatory Compliance and Increased Data Access Using Blockchain. Available online: [https://mediacenter.ibm.com/media/AAISA+Enabling+regulatory+compliance+and+increased+data+access+using+Blockchain/0\\_njb950bk](https://mediacenter.ibm.com/media/AAISA+Enabling+regulatory+compliance+and+increased+data+access+using+Blockchain/0_njb950bk) (accessed on 18 March 2021).
85. Trusting the Transaction of Things: IoT and Blockchain Intersect. Available online: <https://www.ibm.com/downloads/cas/E6LEKG31> (accessed on 18 March 2021).
86. Revere, R.; Antunes, J.P. Solgraph. Available online: <https://github.com/raineorshine/solgraph> (accessed on 18 March 2021).
87. Swende, M.H. EVM Lab Utilities. Available online: <https://github.com/ethereum/evmlab> (accessed on 18 March 2021).
88. Garcia, F. Ethereum-Graph-Debugger. Available online: <https://github.com/fergarrui/ethereum-graph-debugger> (accessed on 18 March 2021).
89. MythX Tools. Available online: <https://mythx.io> (accessed on 18 March 2021).
90. Mythril. Available online: <https://github.com/ConsenSys/mythril> (accessed on 18 March 2021).
91. Josselin, F. Slither, the Solidity Source Analyzer. Available online: <https://github.com/crytic/slither> (accessed on 18 March 2021).
92. Baqa, H.; Truong, N.B.; Crespi, N.; Lee, G.M.; Le Gall, F. Semantic smart contracts for blockchain-based services in the Internet of Things. In Proceedings of the 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 26–28 September 2019; pp. 1–5. [CrossRef]
93. Ruta, M.; Scioscia, F.; Ieva, S.; Capurso, G.; Sciascio, E.D. Semantic Blockchain to Improve Scalability in the Internet of Things. *Open J. Internet Things* **2017**, *3*, 46–61.
94. General Data Protection Regulation. Available online: <https://gdpr-info.eu> (accessed on 18 March 2021).
95. Tajani, A.; Ciamba, G. Unfair Trading Practices in B2B Relationships in the Agricultural and Food Supply Chain. Available online: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32019L0633> (accessed on 18 March 2021).
96. The Directive on Unfair Trading Practices in the Agricultural and Food Supply Chain. Available online: [https://ec.europa.eu/info/sites/info/files/food-farming-fisheries/key\\_policies/documents/brochure-utp-directive\\_en.pdf](https://ec.europa.eu/info/sites/info/files/food-farming-fisheries/key_policies/documents/brochure-utp-directive_en.pdf) (accessed on 18 March 2021).

Reproduced with permission of copyright owner. Further reproduction prohibited without permission.