

Review

Agriculture-Food Supply Chain Management Based on Blockchain and IoT: A Narrative on Enterprise Blockchain Interoperability

Showkat Ahmad Bhat ^{1,*}, Nen-Fu Huang ², Ishfaq Bashir Sofi ³ and Muhammad Sultan ⁴ 

¹ ICE, Department of Electrical Engineering and Computer Science, National Tsing Hua University, Hsinchu 30013, Taiwan

² Department of Computer Science, National Tsing Hua University, Hsinchu 30013, Taiwan; nenfuhuang@cs.nthu.edu.tw

³ Gina Cody School of Computer Science and Engineering, Concordia University, Montreal, QC H3G 1M8, Canada; ishfaqbashir09@gmail.com

⁴ Department of Agricultural Engineering, Bahauddin Zakariya University, Multan 60800, Pakistan; muhammadsultan@bzu.edu.pk

* Correspondence: s108064891@m108.nthu.edu.tw

Abstract: Modern-day agriculture supply chains have evolved from sovereign and autonomous local stakeholders to a worldwide interconnected system of multiple participants linked by complicated interactions, impacting the production, processing, transportation, and delivery of food to end consumers. Regular instances of fraudulent acts reveal a lack of openness in agriculture supply chains, raising worries about financial losses, eroding customer trust, and lowering corporate brand value. To develop an efficient and reliable trading environment, several fundamental modifications in the present supply chain architecture are required. There is broad consensus that blockchain can improve transparency in agriculture-food supply chains (agri-food SCs). Consumers now demand safe, sustainable, and equitable food production processes, and businesses are using blockchains and the internet of things to meet these needs. For enhanced responsiveness in agri-food SCs, new concepts have evolved that combine blockchains with various Industry 5.0 technologies (e.g., blockchain technology, big data, internet of things (IoT), radio frequency identification (RFID), near field communication (NFC), etc.). It is critical to cut through the hype and examine the technology's limits, which might stymie its acceptance, implementation, and scalability in agri-food supply chains. This study presents Agri-SCM-BIoT (Agriculture Supply Chain Management using Blockchain and Internet of things) architecture to address the storage and scalability optimization, interoperability, security and privacy issues security, and privacy of personal data along with storage concerns with present single-chain agriculture supply chain systems. We also discussed the classification of security threats with IoT infrastructure and possible available blockchain-based defense mechanisms. Finally, we discussed the features of the proposed supply chain architecture, followed by a conclusion and future work.

Keywords: precision agriculture; supply chain; blockchain; internet of things; traceability; smart contracts



Citation: Bhat, S.A.; Huang, N.-F.; Sofi, I.B.; Sultan, M. Agriculture-Food Supply Chain Management Based on Blockchain and IoT: A Narrative on Enterprise Blockchain Interoperability. *Agriculture* **2022**, *12*, 40. <https://doi.org/10.3390/agriculture12010040>

Academic Editors: Michele Mattetti and Luigi Alberti

Received: 25 October 2021

Accepted: 28 December 2021

Published: 30 December 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

Agriculture is one of the significant fields in the world, affecting all human existence. Agriculture production is substantial for a nation's economy along with the security, nutrition, and health of its populace. Agriculture practice involves a lot of choices and vulnerabilities such as weather remains changing from season to season, the market price of agriculture products keeps fluctuating, degrading soil quality, not sustainable crops, weeds and pests harm produce, and global climate change. In the agriculture supply chain, big data analytics might be employed to analyze the food quality, storage conditions, weather patterns in a particular geographic area, soil quality such as pH and nutrients, marketing

and trade management, and the existence of food hazards by relating biotic or abiotic data with development and probabilistic existence of pathogens, pests, and toxicants. It can also be used for determining the behavior of customers and inventory management. Thus, it offers a prospect to utilize the data by abiding by the scientific methods and making efficient decisions at right time. To utilize agricultural big data a holistic approach involving several relevant technologies and data of various related sectors is required. Researchers, legislators, farmers, and other stakeholders can utilize agricultural big data for research, policymaking, decision making, crop management, and business management [1]. Figure 1 represents the characteristics of blockchain, IoT, artificial intelligence (AI), and big data for the agricultural sector. To keep up with such uncertainties farmers need to change their practicing approaches.

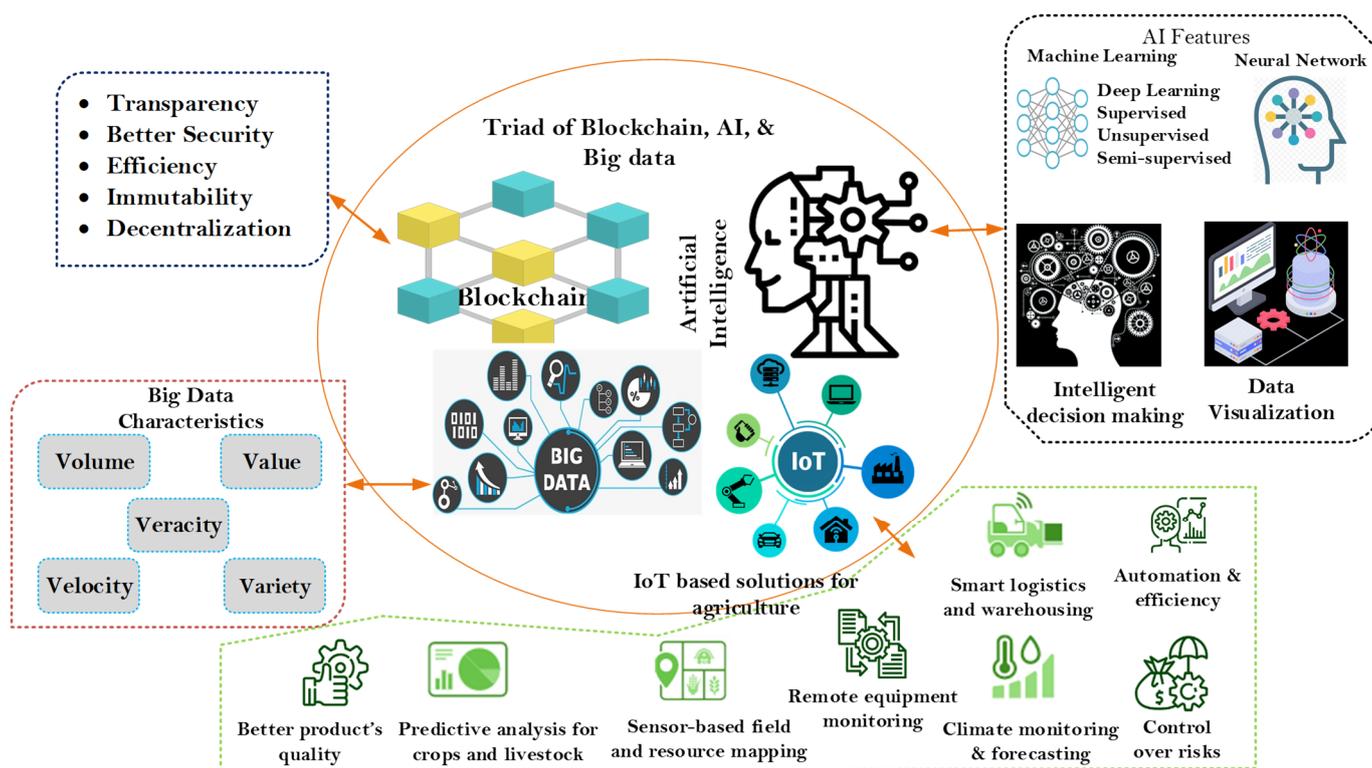


Figure 1. Characteristics of blockchain, AI, IoT, and big data for smart farming.

Farmers, processing factories, distributors, retailers, and consumers are all part of the complicated food supply chain involving many stakeholders. All food processing enterprises and supply chains must now provide safe food as a crucial and legally defined need. CAC/GL 60–2006 lays forth the basics of food traceability [2]: as acceptable to the targets of the food testing and enforcement scheme, the traceability/product tracking solution must be able to distinguish at any given stage of the food supply chain (from the production process to retailing) from where the food came (one step back) and where the food went (one step forward) from where the food came (one step back) and where the food went (one step forward). National and international regulations support the implementation of these concepts (see, for example, European Union (EU) Regulation (EC) No. 178/2002 and national methods assessed by Charlebois et al. [3]). Because all actors know who their suppliers are and where their product is sold, this pragmatic one up/one down system connects all tied supply chain participants. However, because many food items have complicated multistep vertical and horizontal branching supply networks, relying on the one up/one down strategy makes the supply chain susceptible (e.g., multiple ingredient products). Furthermore, with commodity items that are blended (e.g., milk from several farms in a dairy) or dissected and mixed across the supply chain, one up/one down

traceability can be easily lost (e.g., animals for meat production). With this level of intricacy, verifying the provenance and quality requirements of individual items becomes nearly difficult. Furthermore, the food sector continues to rely heavily on paper records, and the present food traceability systems are not integrated nor linked across all participants in the supply chain. This isolation creates a negative information imbalance among all supply chain stakeholders, a lack of transparency across numerous supply chain processes, and the potential for fraud to be promoted or concealed. Although several technologies for product traceability have previously been employed, such as bar codes, RFID tags, and Electronic Data Interchange (EDI), Bosnia and Gebresenbet [4] stated that more technical applications for food supply chain traceability are needed.

Moreover, existing IoT-based tracking and provenance systems for agri-supply chains are layered on top of centralized structures, leaving an opportunity for unresolved issues and key concerns such as data integrity, manipulation, and single points of failure. In reality, obtaining verified and confidential data in a supply chain is difficult because it necessitates a high degree of confidence between cooperating parties, and trust necessitates the development of a specific quantity of verified and communicated information [5]. Although scholars and practitioners believe that somehow a third party is required in the chain to ensure information quality and security, the incentive for supply chain stakeholders to increase transparency in the agri-supply chain varies [6]. In this way, blockchain may operate as a decentralized certificate authority, verifying transactions, and delivering tamper-proof cryptographic information to any point in the chain upon demand.

Globally known food companies have begun to collaborate to accelerate the implementation of distributed ledger technology in agri-food supply chains, and early prototype models are emerging. Novel design concepts for such a system have been offered in the literature. Globally known food companies have begun to collaborate to accelerate the implementation of distributed ledger technology in agri-food supply chains, and early prototype models are emerging. Novel design concepts for such a system have been offered in the literature. In this context, researchers have begun to implement blockchain-enabled supply chain product traceability models [7–12], however, preliminary findings are only accessible for latency, network traffic, and CPU load. Tian [13] has recently expanded the initial application to real-time food monitoring based on HACCP (Hazard Analysis and Critical Control Points), however widespread adoption of blockchain technology in the food processing sector and supply chain is difficult and may face several problems [9]. On the other hand, by far most of the existing logistic information systems in Agri-Food supply chains like Costco, Walmart, Cargill, Albert Heijn, etc., just store, track orders, and supplies, without giving characteristics such as transparency, auditability, and traceability. These characteristics in an agri-food supply chain will certainly improve the food quality and safety, thus are in demand from consumers. Therefore, numerous R&D communities both in industries and academia have engaged their efforts in developing efficient food chain traceability systems based on emerging technologies like the IoT and blockchain technologies, to facilitate remote monitoring at every stage all along the supply chain, from farm to fork. The above-mentioned companies have recently started experiments with blockchain for their supply chains.

The contributions of this paper can be summarized as: (i) we performed a comprehensive study of the state-of-art of IoT and blockchain technologies in agri-food supply chain and highlighted the prospective applications of these technologies, (ii) we identified and provided a comprehensive discussion on different research challenges of agriculture supply chain alongside the IoT security problems and existing defense mechanisms, (iii) we also presented the application of IoT and blockchain in different domains of agriculture sector such as food composition, quality, safety monitoring, food supply traceability, and farm and food waste management, (iv) we have also given the special consideration to security and implementation challenges of these technologies and smart contracts in blockchain-based agriculture sector, and (v) finally, we introduced a new blockchain-based Agri-SCM-IoT architecture to solve storage, security, and some other challenges in the agriculture supply

chain along with the necessity of interoperability among blockchain platforms to solve scalability and growing blockchain ledger size. Though there are several reviews [14–18] that focus on IoT and blockchain-based food supply chain management, to the best of our knowledge, no work has discussed the interoperability between different blockchain platforms and the ever-increasing nature of ledger size affecting the scalability of the single-chain based supply chain systems. This work presents a systematic literature review of blockchain, IoT, and AI technologies in agri-supply chain applications contributing to the existing literature of these three technologies by identifying the singularity of individual technological usage and accumulating a thorough understanding of the relationship among these technologies. Moreover, we exhibit the potential research directions to conduct comparative examinations of these technologies in agri-supply chain management and investigate interactive factors reported in the existing literature. This paper covers both technical and applicative characteristics in such a way that our intuitions can be applied for cross-blockchain agri-supply chain scenarios.

2. Related Work

To effectively manage the supply chain, and thus the human behaviors it includes, all stakeholders must agree on the information to be recorded on the blockchain, from raw materials to finished goods. The fundamental objective is to choose the information that is useful to all areas of the supply chain, with a particular focus on customer needs and applicable standards blockchain may be utilized as a marketing technique along with operating as a traceability system. Blockchains may be used to improve a company's image and reputation [19], promote loyalty among existing consumers [20], and bring new clients since they are entirely transparent [21] and participants can manage the items in them. In reality, organizations may simply set themselves apart from rivals by stressing product flow transparency and monitoring across the supply chain. Furthermore, quickly identifying a source of food contamination can boost a company's brand image [22] and mitigate the negative impact of media criticism. With the globalization of business, supply chains are growing more complicated, making it more difficult to track things across their intricate webs. In reality, stakeholder relationships are frequently complicated. As a result, suppliers can be divided into tiers, with a first-tier supplier supplying the organization directly with metal cans, for example, and a second-tier supplier supplying the raw materials needed to manufacture the cans [23]. Organizations sometimes have several suppliers at various levels involved in a single product; also, suppliers are frequently non-exclusive to a single firm. Aung and Chang [24], as well as Golan [25], have identified three key goals for traceability to enhance product-supply chain administration, product differentiation strategies, and quality assurance, and improved detection of non-compliant items. Compliance with applicable legislation and standards is another factor in ensuring traceability.

Majority of existing blockchain solutions for traceability management have been established based on single chain architecture such as the Fish supply chain [26] to decrease the transaction cost and enhance the transaction capacity and make system auditable and provide certifications to the product, Wine supply chain [27] to improve the performance, revenue, accountability, and security, and implement the more secure and secure global transactions, Agri-food supply chain [28] to enable quality and certified virtual identity especially for "bio" and DOCG products, Agri-food supply chain system [29] to share the authentic data in production, processing, distribution, retailer, etc. across the supply chain, Fruit supply chain based on public immutable distributed ledger based on decreased variance of mining rewards, Pork supply chain [30] to enhance consumer trust by protecting the brand and security through transparency, large enterprises supply chain food tracking project [31] to integrate the existing systems with the blockchain used by various stakeholders, fresh food [32] supply chain to attach the product origin data along with sensor data throughout the supply chain with product to enable data, and product transfer transparent from farm to fork. Furthermore, the AgriOpenData [28] blockchain integrated solution is a cutting-edge digital technology that ensures transparent, secure, and public transparency

throughout the whole agriculture supply chain and in the processing of agricultural goods. This is especially true for “bio” and DOCG (Designation of Origin Controlled and Guaranteed) items, which may have their quality and virtual identity certified (viz., provenance, ownership, seeding, treatments, crop, Internet of Things analysis, processing, storage, and delivery). This digitized history of organically cultivated products ensures end-consumer legitimacy and improves the agri-food industry’s quality. The variation of mining incentives, and thus the necessity for mining pools, maybe significantly minimized using some particular FruitChain protocols [33]. For example, in a FruitChain with 1000 fruits per block and each fruit taking 80 bytes, allocating memory for 1000 fruits every block occupies around 8% of a 1 MN block. A solitary miner may now get their initial rewards 1000 times quicker (in a day or several rather than a few years).

Furthermore, DNA samples from an animal may be used to determine its breed, but additional data such as country of origin, toxicity exposure, and uncontrolled medicine, among other critical factors, can be acquired. To ensure the animal’s identity and lifetime, this data may be compared to the blockchain record. Dey et al. [12] developed a Food-SQRBlock (Food Safety Quick Response Block) supply chain architecture using blockchain and QR codes. They have also proposed large-scale cloud integration of the developed system to demonstrate the framework’s practicality and scalability, as well as an experimental assessment to back it up. Tian et al. [13] proposed a theoretical real-time food traceability system using HACCP, blockchain, and IoT. The authors have claimed to achieve transparency, reliability, and security with the proposed model but have not provided any experimental implementation and evaluation of the system. Leng et al. [9] introduced a double chain-based agriculture supply chain architecture using a public blockchain. They also study the storage mode, resource rent-seeking, and consensus algorithms but have not evaluated the speed and competence of consensus algorithms by considering the case for a huge number of nodes and resources on the platform. Moreover, the access management for the user needs to be further investigated. Surasak et al. [10] presented an IoT-based blockchain traceability system particularly designed for Thai agriculture products. Blockchain has been used for creating a distributed ledger to increase data integrity and transparency and a structured query language (SQL) database has been used to make the platform user-friendly. There is a need to further research on the integration of blockchain with the proposed system to enhance the security, transparency, and integrity of the system. Dakshayini et al. [34] suggested a blockchain, big data, and cloud-integrated crop supervision system trying to realize effective demand-based decision support and to achieve a simple, auditable, and secure supply chain. The authors have also proposed a crop-trading platform to sell the agri-products at different stages. However, they have not implemented the IoT-based Blockchain architecture to gather the real data from the field parameters and then model the big data-based decision support system. They have just used the available data set and implemented a deep learning model to predict the demand.

3. Blockchain-Based Smart Contracts in Agri-Supply Chain Management

Agri-food supply chain system comprises multiple levels of transactions, each level with different terms and conditions [35]. Different systems with diverse characteristics and functions have collaborated in a supply chain, including food processing, transportation, storage, and distributors. All these levels maintain a record of all the products from processing to packaging, transportation to storage, and distribution, which are very long and complex processes. Smart contracts can assist in simplifying the whole process and enhance transparency throughout the supply chain. Integrating blockchain-based smart contracts with IoT devices enables tracking of the location of goods, allows tracking of inventory, and the change of ownership rights across the supply chain. This helps companies to prepare well for any disruption or incidents. Besides this, smart contracts enable companies and customers to determine the quality of the food products by tracing back all the information. The characteristics of smart contracts [36] enable their use in diverse applications or domains. Several of such characteristics are acquired from the core blockchain technology.

Table 1. shows the categorization of the key characteristics of smart contract characteristics. Figure 2. represents the typical structure of blockchain smart contract system having various functional blocks like user management and service management modules manages the user accounts, services, and smart contracts, business network module agent, API's are used to provide an interface for external components, and virtual blockchain platform (such as Ethereum virtual machine) is used to deploy, implement, and supervise the smart contract state machine, etc., in the contract run time once all parties have signed the contract. The smart contract terms and conditions of the smart contract are enforced dynamically depending on the real-time data from various distributed sources and the business transactions are secured by blockchain and distributed ledger technologies.

Table 1. Characteristics of Blockchain-based Smart Contracts.

Features	Description
Elimination of centralized authority	Since blockchain operates in decentralized mode with every node in the network, a smart contract allows autonomous execution according to predefined provisions. Thus decentralization of the system maintains ceaseless service availability by eliminating the single point of failure, reduces data usage and latency, and ensures accountability.
Forge Resistance	Smart contracts preserve the integrity of the distributed ledger and computational logic is verified with digital signatures. The smart contracts once implemented cannot be changed even by their owner.
Transparency	The transaction data and smart contract logic can be accessed by authenticated users all the time.
Self-execution	A business transaction between the entities within the network executes once predefined conditions and the flow of events defined in smart contracts are met without any inference of a centralized third party.
Accuracy	Since the conditions are programmed to be immutable and verified several times before deployment on the blockchain nodes, the execution is automatic and guarantees accuracy without any error on the execution. This feature removes the biased operation and maintains trust between the entities through transparent execution.
Event-Driven Program	Some smart contracts are executed based on the event logs generated within the context of a transaction predefined in its code. These transaction events are atomic i.e., either happen completely or not at all.

In an IoT-based supply chain, smart contracts with blockchain technology can be utilized to enhance the security measures [37], to expedite data management, besides enabling the communication of diverse nodes or devices in an interoperable way. In smart contract-based security management [38], smart contracts can be used instead of digital certificates by including a list of several forms of identifiers or characteristics linked with the public key of the contract owner. Additionally, this list can only be modified only by its owner, and additional security is guaranteed by smart contract residing in the blockchain. Thus, by implementing smart contracts in blockchain eliminates the use of certification authorities. A blockchain-based smart contract simplifies the identity management of the users by providing a GUI (Graphical User Interface) [39] to each user having very little collision probability. It also facilitates the traditional and novel security schemes by storing additional primitives including TLS (Transport Layer Security) [40] public keys. By keeping public keys in the blockchain, clients do not need to count on pre-trusted certification authorities. Furthermore, due to the transparent and distributed characteristics of blockchain, this method is more robust against malicious authorities, in comparison to the DNS-based Authentication of naming entities (DANE) protocol [41], depending on the domain name system (DNS). Smart contracts and blockchain can expedite and develop data management in several ways including access control, information, functionality scoping (i.e., same contract can be deployed by multiple users and each contract gets its address and execute independently), proof of ownership, data authentication, and non-

repudiation. Several platforms are emerging for smart contracts each having different associated characteristics that suit diverse applications.

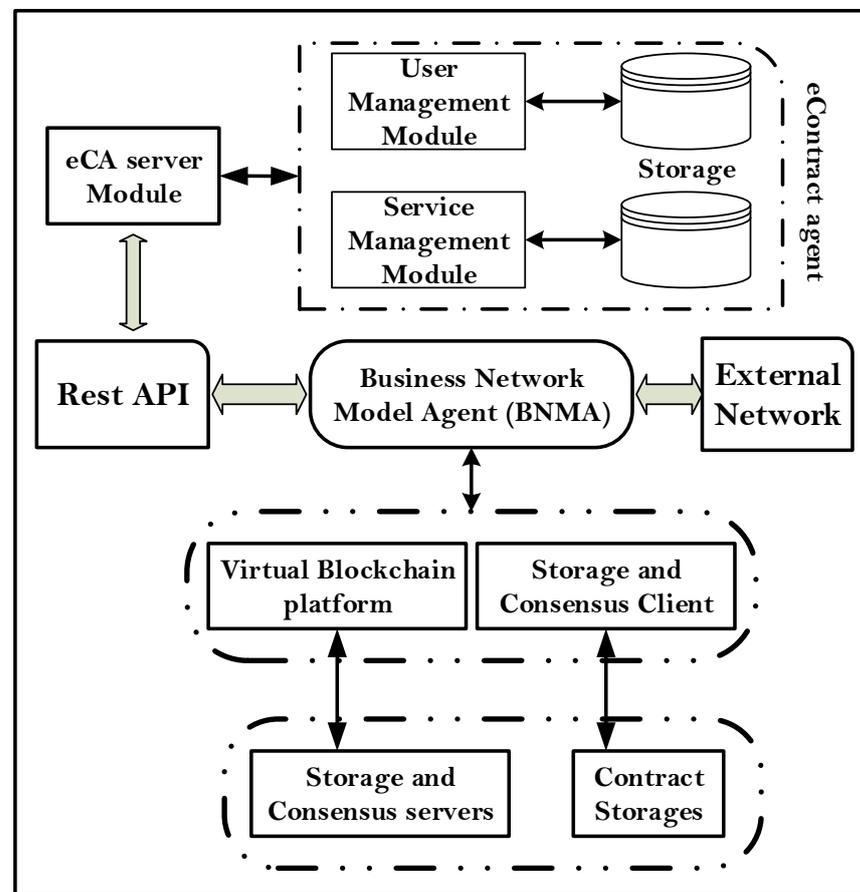


Figure 2. Typical structure of a smart contract system.

The associated workflows and cross-enterprise value procedures in a smart supply chain case can be thought of as an internet-connected intelligent production network or supply chain, in which products and services are developed and delivered downwards, data and finance move upstream, and smart contracts implement automated transaction protocols in both directions. As a result, blockchain technology, when combined with smart contract solutions, has the potential to promote entrepreneurial collaborative projects in logistics networks even throughout international borders, while also complementing existing foundation technology in the direction of smart supply chain solutions. Unlike conventional business processes, which are based on trusted centralized third-party service providers with their standards and architectures controlled by large players, blockchain technology allows these processes to be conducted in a distributed manner, lowering entry barriers, and encouraging process innovation. This supports entrepreneurial activity by deploying extra confidence inside firm networks and supply chains [42].

Furthermore, blockchains are often open and transparent, allowing all supply chain players to view, update, and check data, while modifying or deleting blockchain secured data is practically hard, resulting in increased transparency of all supply chain activities. As a result, supply chain providers may publicly advertise their availability to the whole market, as well as the capacity they have, enhancing their market position and increasing their independence from transportation brokers. This is an option for smaller suppliers and SME participants in a supply chain to combine their production outputs to fulfill large orders, allowing them to sell products directly to retailers or ultimate clients rather than through intermediaries. Wu et al. [43] created a smart contract for logistics, demonstrating

how contract digitalization can complement or replace highly centralized fourth-party logistics providers, reducing the layers of intermediaries or businessmen within supply chains by directly connecting suppliers, processors, retailers, distributors, and logistics companies. All of these ideas are valid and adaptable to smart supply chains beyond restrictions. Due to the openness and transparency of blockchain-based supply chains, cross-enterprise business processes may be improved and optimized. To oversee and improve operations management and supply chain activities, Nyhuis and Wiendahl [44] introduced logistic operation curve theory and throughput-oriented lot sizing. However, empirical findings show that these theoretical notions do not operate effectively in practice, necessitating a revision of the underlying theoretical models [45]. Smart contracts may be used to start transactions amongst supply chain units to coordinate and optimize the whole supply chain. This applies to time-related issues such as throughput, cycle, and lead time, as well as cash flows along the supply chain. So, based on the findings, the most promising use of blockchain technology and smart contracts in the agriculture supply chain network is reorganization of the agriculture product trading market by implementing cross-blockchain (cross-enterprise) asset and data transfer.

4. Application of Integrating Blockchain and IoT with Agri-Supply Chain

To establish an efficient and reliable supply chain management system, the industry needs to employ cutting-edge technologies like blockchain, IoT, and AI. A data-driven smart agriculture supply chain with AI, IoT, and blockchain is the most promising approach to solve different existing problems. If we could generate a huge quantity of data from the supply chain and use that data to drive the decision processes. It can help to solve several problems related to food quality, safety, foodborne, data sharing across the supply chain, etc., globally. Some of the potential applications of blockchain, AI, and IoT in supply chain management are discussed.

4.1. Food Composition, Quality, and Safety Monitoring

Recently consumers are increasingly being made aware of the composition and quality of food products [46] through different awareness programs regarding healthy lifestyles and technological advancements in food science. Furthermore, due to new food regulations around the world companies need to label food products in detail alongside quality monitoring. Labeling guidelines [24] perform a pivotal part in finding out which scientific tests are suitable for a specific issue. Consumers around the globe are progressively requesting a guarantee that the origin and ingredients of their food follow the data on the label. This is the reason shoppers, producers, and administrative bodies have perceived the authenticity of food items as significant quality standards. Thus different IoT sensors based on UV-Visible-near infrared spectroscopy [47], DNA-PCR methods [48], stable isotope measurement (IRMS) [49], mass spectrometry [50], separation techniques [51], and big data are making a rapid advance in food products quality, composition, and assessment fields. Thus, the advancements in the development of distributed ledger technology along with IoT, big data, and micro-fabrication, and miniaturization of spectroscopic devices. Largely, UV-Visible-near infrared spectroscopy-based IoT, in association with blockchain and big data analysis provides an indispensable and vigorous variety and authenticity management mechanism for the smart agriculture area.

4.2. Food Safety across Supply Chain

For all stakeholders around the world, food safety has developed as a global priority from farm to fork. There have been many foodborne outbreaks [52] based on fresh agriculture products in the recent past. That results in the dumping of a huge quantity of agri-produce to protect public health. It is estimated that the food requirement around the globe is anticipated to surge by fifty percent from 2020 to 2050, present practices of protecting the health of the masses by foodborne outbursts could be infeasible choices for the future. Every day an enormous amount of data is generated in the food industry and

recognizing methods to abstract the vital material from diverse sources would assist in bacterial risk evaluation [53], outbreak deterrence, classification of trends utilizing pathogen supervision [54], which empowers food safety conclusions and supports decision making. Concurrent supervision of agri-food products throughout repository and distribution [55], RFID tag, GPS, and QR code like digital labeling that is not difficult to synchronize with the cloud, and improved traceability due to blockchain are a few out of numerous benefits that ICT can add to the prospectus food safety. The potential of blockchain and the internet of things to boost food reconnaissance frameworks are encouraging and performing synergistically by integrating AI-based big data evaluation like a prompt response towards food safety outbursts [56,57]. It is expected that the internet of things would be beneficial to carry out a comprehensive methodology in food handling in which key drivers like environmental change, human conduct, and economy might be joined to visualize food safety hazards and blockchain will enhance the privacy and security of data.

4.3. Food Product Traceability

The traceability of food products has consistently been one of the main concerns of the customers. It is well-defined as the capability of a system to monitor and track the movement of agricultural food products across the supply chain from the producer to the final distribution stages [7,58]. Recently, with fast economic growth and the improved standard of living, people have started to pay more attention to the quality and nutritious values of the food. However, various food safety crises are always there. Customers from asymmetric information environments do not have access to the food supply chain information, which results in high health risks. Tracking has emerged as an essential service in the agri-food supply chain [13] to guarantee food safety to customers. The incompetence of the food monitoring organizations to isolate the source of adulteration in outbreaks break the community trust in the supply chain considerably. For instance, amid the Spinach flare-up [59] of 2006, it took fourteen days to identify the adulterant substance, and abundant resources were utilized. A different case incorporates the romaine lettuce episode [60] of 2018 during which all the lettuce was taken down the racks without awareness of the beginning of contamination. All available lettuce in markets was dumped due to a lack of proper back-tracing mechanism by the food governing organizations. The deficient record-keeping methods usage result in the inability of back-tracing of food products. This causes degradation of purchaser trusts and results in a critical setback for food producers. To solve this problem, blockchain innovation can be employed. Blockchain implementation will empower fast and exact back-tracing, decreasing expenses from food losses, and saving valuable living souls [61]. Blockchain distributed ledger technology [62] could be used in the food chain to store valuable information digitally such as food production data, ingredients, origin, shipment and storage data, expiry, etc. This will facilitate the prompt identification of foodborne outbreaks and the authenticity of the food.

In recent years, various solutions utilizing several technologies such as IoT, RFID, AI, etc. have been proposed to advance agricultural food product traceability [7,8,10,12,13,17,29,62–64]. Figure 3 below shows an outline of how the product and data flow in an IoT-based blockchain supply chain system. The traceability system contains all the information about food production, processing, and transportation as well as storage conditions. The consumer should be provided access to all the information about each step precisely and even about every single ingredient of the final product.

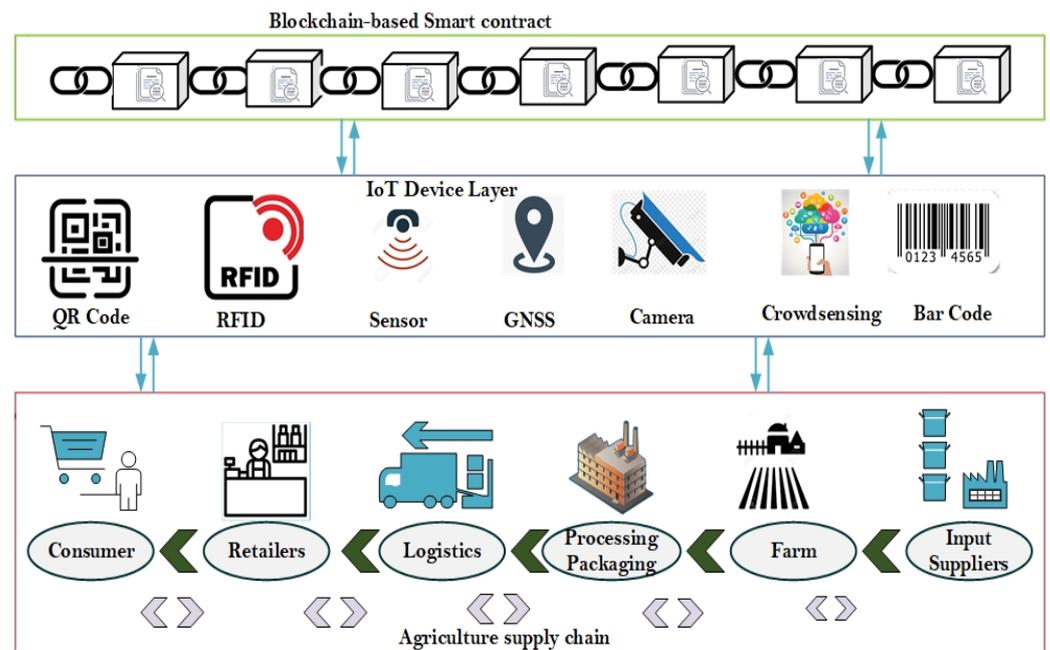


Figure 3. Blockchain-based smart agri-supply chain.

4.4. Tackle Food Waste

There are different stages such as harvesting, post-harvest management, and repository, processing, distribution to markets and retailers, and consumption in the food supply chain through that food traverses from farm production to arrive at the consumer [65]. Food loss occurs at stages of post-harvesting (i.e., during post-harvest handling, storage, preparation, and distribution) and processed stage (i.e., at the retailer operations or behavior of consumers). Food waste also consists of losses during the pre-harvest session due to pests and diseases, or other issues like losses in fields due to extreme weather conditions, not harvested due to price drops, etc. [66]. Food loss and waste at any stage of the supply chain create numerous challenges and waste opportunities for growers, consumers, and communities as a whole. Loss in produce causes financial losses to farmers, shortages, and higher bills for customers. This financial burden is particularly grave for people on the food insecurity edge, where a trivial swing in price can substantially impact livelihood.

Technology-based like blockchain, IoT, and big data solutions are being employed to manage food waste, perhaps the most pervasive issues confronting the food sector [67]. Addressing this persistent problem has turned into an industry critical that is being undertaken using different cutting-edge technologies to increase shelf-life, dynamic price adjustment depending on sell-by-dates, and monitor automatically food waste at restaurants, retail stores, pre-harvest and post-harvest losses, etc. In the food processing industries, blockchain-based supply chains are offering better transparency into food productions. IoT device network sends real-time data that can be utilized to optimize production processes and enhance quality, making it simple to satisfy the consumer needs, tackle the logistic issues, and withhold government regulations. Blockchain and IoT devices along with big data can provide food companies [67] with effective technological solutions to resolve challenging issues.

4.5. Inventory Management

Inventory management is described as the process of overseeing the movement of goods from the production plant to warehouses and from these facilities to retail outlets [68]. It is an important part of supply chain management. It is worth noting that demand forecasting and inventory management are inextricably linked. If the provider fails to satisfy the needs of the customers, the company's time and money are wasted, and the

customers are dissatisfied. Alternatively, if supply exceeds demand, vital resources are depleted for no additional profit since there are no possibilities to sell the excess inventory. High inventory levels, according to several well-known business gurus, are one of the key concerns that restrict firms' profitability [69]. Furthermore, as borrowing rates rise, inventory storage expenses rise as well. By precisely calculating supply volume in advance and devising dynamic operating plans, ML [70] approaches help to avoid such risks. Labor management, inventory system automation, vehicle deployment strategy optimization, and supply chain decision-making agility may all benefit from machine learning and data analytics methodologies. Proper forecasting of demand is critical for supply chain planning and management [71]. While demand patterns for basic things like food are somewhat steady, demand uncertainty in leisure products like apparel and technology may be significant. Supply chain managers may use demand forecasting to plan productive business operations, optimize inventory levels, assess possible hazards, handle demand exceptions, and develop mitigation solutions. Inefficient demand forecasting tactics, on the other hand, can lead to inaccurate projections, which can result in considerable financial losses for businesses and wastage of food products.

5. Cyber Security Challenges in a BIoT-Based Supply Chain Network

Supply chain networks are unnecessarily complex due to the involvement of multiple persons, business enterprises, governments, and maybe even nations. Supply chains confront several challenges, including (1) establishing trust amongst numerous parties involved; (2) cyberattacks; (3) cargo theft; and (4) counterfeiting, among others. However, in this section, we are going to discuss only the cyberattacks in IoT-based supply chains systems. Food and drinks are the most commonly stolen products, but medications and gadgets are expensive. The amount of security vulnerabilities that a supply chain confronts is directly related to the complexity of that supply network, i.e., as the supply chain becomes more complex, it becomes more vulnerable to various types of security threats. These hazards can disrupt supply chain operations in a variety of ways such as fraudulent replacement and tamper with items that can lower their utility and make them unpleasant for the end-user, the supply chain's businesses, particularly third-party service providers, may not all have the same security requirements, and because information technology (IT) systems now control substantial portions of the supply chain, cybersecurity is one of the most pressing concerns. The chain is vulnerable to a single point of failure due to its heavy reliance on a networked IT system. Access to one of the systems can lead to access to other portions of the system that are not as secure.

The future implication of IoT is apparent from its current applications in every field. It is growing continuously due to the evolution of hardware technologies including enhancing bandwidth utilization by addressing underutilization of frequency spectrum, improving energy efficiency, and extending computation and storage features. The cyber-physical systems and wireless sensor networks have developed as integral elements for the broader term IoT. As a result, the security issues associated with these technologies such as WSN, M2M continue to increase. Consequently, with the application of ICT and IoT in the agriculture industry, the potential risks of security attacks on the smart agriculture infrastructure [72] are increasing. Thus, the food sector is attracting more security attacks on its infrastructure and production facilities. Preventing such attacks needs a multi-disciplinary approach [73] that covers both hardware and software by policies and security mechanisms for preventing cyber-attacks or mitigating their impact on its occurrence. Thus, it is essential to identify potential security threats [64] and find solutions to prevent these threats.

The security problems of an IoT network can be classified into three levels: (1) at the application layer, (2) at the network layer, and (3) at the perception layer. At the application layer, we require studying three security concerns, i.e., user data privacy, encrypted data analysis, and secure computing. Thus, when IoT devices are connected with the network, identity authenticity and data integrity are required. Without any authentication scheme, malicious devices can get access to the network. The IoT devices can access the IoT network

application layer using cellular networks which adopt standard communication protocols. Those standard protocols are having advanced security. Two types of threats are faced in the perception layer: (a) many terminals have open insecure ports and numerous vulnerabilities that let unauthorized devices access. There are always security risks where hackers can exploit these weaknesses to launch different attacks and (b) terminals connected with short-range ISM band communication protocols such as ZigBee, WiFi, and Bluetooth having weak security mechanisms, thus are vulnerable to security attacks. Moreover, several of these terminals are having weak login and password mechanisms. These terminals also lack encryption algorithms between devices and the network.

In this section, we are going to discuss major cyber security threats, security requirements, and some available solutions. The different types of security attacks to which the IoT-based agriculture supply chain is vulnerable are discussed in Table 2. Blockchain technology finds its applications in nearly all areas of IoT, including the IoT-based smart agriculture supply chain [46,74,75]. The convergence of blockchain with IoT is to preserve privacy. Some of the relevant blockchain-based solutions that can be optimized for agri-supply chain applications available in the literature are presented in Table 3. Apart from the solutions presented in Table 3, there are several other methods present in the literature, which needs to be optimized for IoT-based smart agriculture application requirements.

Table 2. Security Vulnerabilities in IoT-based Smart Agri-Food Supply Chain Platforms.

Security Attacks	Description
RF jamming attack	Attackers can use different distributed low-power jammers to disrupt the GNSS and other cellular network frequencies to block smart farming equipment from working accurately.
Malware injection attack	An attacker can steal information; damage the normal working of the agriculture system, etc. by injecting malware into a connected device. Any farm infected with the malware is likely to infect other farms on the same network. It can have a devastating effect on a system.
Denial of service attacks	An attacker floods a system with an enormous number of service requests from a large number of the host machines, which the system is not able to withstand and crushes. It does not directly benefit the attacker but denies the services to the authentic users.
BOTNET	If an attacker succeeds to get control of a device on a farm, he can control all the devices on that farm and turn it into BOTNET. The attacker can then employ the infected devices to corrupt many other devices in the network.
Side-channel attack	Rather than exploiting the weakness in the system, this attack exploits the data about the implementation of the system and the sequence of data being transmitted by it.
Replay attack	The attacker can collect a copy of the transmitted data packet between two entities and try to deceive an authorized user by retransmission.
Man-in-the-middle attack	An attacker tries to modify or delete the content of the message during transmission between two entities and then sends it to the destination.
Stolen verifier attack	An attacker snips authentication data such as OTP from the server is present or past verification sessions. Then uses the verification data to access the server. If it succeeds, the attacker imitates an authorized user for the next session.
Brute force attack	An attacker uses all possible passwords to get access to the system until the correct password is matched. The attacker also tries to guess the key created from a known key derivation function which is called exhaustive key search.
Privileged-insider attack	An authorized user attempts to gain unauthorized access to other services or resources to modify or delete important information.
Masquerade attack	An attacker aims to impersonate as a legitimate entity or node to log into the system at agriculture sensor layers.
Tracing attack	An attacker collects a large amount of privacy data at the sensor layer from IoT devices to relate with a definite real identity.
Known key attack	Based on the previous compromised keys, an attacker tries to create new session keys.
Resilience against sensing device capture attack	An adversary may truly hold on to the sensing device and obtain the information he wants from the seized device to establish a connection with other devices in the network. Device capturing results in huge damage to the system.

Table 2. *Cont.*

Security Attacks	Description
Rogue device deployment attack	An attack can install illegal sensing devices in the IoT network environments. An adversary can even replicate the existing compromised sensing device to extract sensitive data and use replicated nodes to communicate with other genuine nodes of the network.
Sybil attack	In this type of attack, an attacker creates several pseudonym identities that are misinterpreted as multiple entities. This results in numerous requests accepted from the same identity and leads to a 51% attack.
Wormhole attack	An attacker deceits two nodes far away from each other into interacting with each other through a wormhole tunnel, employing an in-band and out-band communication channel, which can bypass across network traffic. Therefore, misleading the entities into the sense that they are close to one another.
Black-hole attack	An adversary node tries to modify routing-related data to create a scenario in which data transfer between the nodes is not permitted, as a result forming a black hole in the network. All the data gets stuck in the system and the flow of data between nodes is captured.
Selective forwarding	In this type of attack, the corrupted node did not forward the data to the next node and also stops routing data in some specific situations.
Enervation attack	An adversary tries to deplete the energy resources of the nodes by making them perform some unnecessary processes.

Table 3. Blockchain-based solutions for the cyber security threats of IoT-based Agrifood Supply Chain In-frastructure.

Work	Year	Description (2017–2020)
Jiang et al. [76]	2018	Suggested a thin-client authentication scheme (PTAS) for IoT applications. It is used to solve the problems of single-point failure in blockchain-based PKI. This security mechanism is robust against Sybil attacks, eclipse attacks, and 51% attacks.
Shen et al. [77]	2019	Provided a privacy-preserving mechanism (SVM) for IoT use cases. The scheme uses a public-key cryptosystem (Paillier), an additive homomorphic cryptosystem. This method is strong towards the known ciphertext model and known background model attacks.
Ma et al. [78]	2019	This solution presents a key management architecture based on blockchain technology (BDKMA), for IoT use cases. For actuating the hierarchical access control, the architecture employs security access managers for functioning blockchain.
Novo et al. [79]	2018	Presented a blockchain-based distributed access control archetype, where policies of access are controlled by a blockchain platform. The proposed scheme uses smart contracts and fog nodes to provide the advantages of transparency, mobility, accessibility, lightweight, and scalability.
Ding et al. [80]	2019	The authors came up with a blockchain-based layered architecture of a reputation and trust mechanism for IoT applications. This archetype is proposed to validate the transactions at three key layers of the system based on the reputation of the minor generating the node.
Zhou et al. [81]	2018	Presented a TSMPC protocol to extend Shamir's (t, n)-secret sharing (SSS) applied among a leader server and normal n servers. Ethereum blockchain is used to evaluate protocol performance, which establishes that it can only store transactions of 61 Mb size at most.
Hammi et al. [82]	2018	Proposed a decentralized system known as bubbles of trust to guarantee the robust authentication and identification of devices connected to the network. The proposed system divides the network into different virtual zones (bubbles) to uphold integrity and availability.
Derhab et al. [83]	2019	Presented a hybrid software-defined networking architecture combining two security modules namely blockchain-based integrity checking system and intrusion detection system.
Sharma et al. [84]	2017	Presented an integration of SDN and blockchain to enhance the scalability of IoT-based applications. Therefore, the authors suggested a secure SDN architecture called DistBlockNet.
Chae et al. [85]	2018	The authors proposed a lightweight smart farm authentication scheme to manage the farm securely. It employs session and public keys to make it simple and increase the throughput, diminishes encryption/decryption time, and decreases registration time to make it capable of implementing on resource constraint IoT devices. This method can be integrated with blockchain and adapted for smart farming applications.
Patel et al. [86]	2018	To overcome security issues, the authors proposed a blockchain-based lightweight architecture to optimize the energy consumption of the IoT sensor devices and provide secure communication among devices in the smart farm environments.

6. Implementation Challenges

Even though blockchain-based internet of things use cases have been investigated, but the impact of ever-growing blockchain ledger size [87] has not been considered in these studies. Blockchain-based agri-food supply chains are a complex network [61] of inputs and outputs from farm to the fork and the generation of an enormous quantity of data from the implementation of a huge number of IoT devices at each stage [88]. The data produced from the IoT devices are sent to the blockchain as transactions [89]. As blockchain nodes are append-only data storages by definition. This implies that the node's storage space requirements will constantly rise in direct correlation with the number of transactions executed per second [90].

Thus, the size of blockchain grows in proportion to the number of nodes that run concurrently, each node will want its own written copy of the blockchain ledger, and if you are operating at a large scale (hundreds and perhaps even multitudes of nodes), data storage space requirements might become a problem [91]. Due to two factors, the storage needs for blockchain networks will increase, (i) as the number of users expands, the number of transactions for each second increases, and (ii) every transaction expands the volume of the blockchain ledger, and since it is append-only, memory usage is continuously increasing. When we evaluate this with mutable systems, wherein data gets replaced, we could see how, as time passes, we begin to experience the ever-increasing ledger size in blockchain-based storage systems. There still are techniques to reduce the size of blockchain ledgers [92], but there is rising apprehension that the size of these ledgers may exceed the capacity of available storage considering the increasing number of IoT-based sensors in agriculture equipment, smart logistics, agri-stores, food processing companies, etc. Simply put, we want a system that allows us to expand our storage capacity without compromising performance or necessitating migrations that would result in downtime. Apart from the ever-increasing ledger size, as blockchain technology becomes more widely adopted, every industry and institution is transitioning from centralized data storage to decentralized distributed ledger networks. With each passing day, the use of blockchain and decentralized ledger systems grows. As a result, each sector or organization chooses the blockchain technology that best meets their storage, security and privacy, latency, and other needs. Thus, we need a system where any supply chain entity with any distributed technology can join the supply chain while maintaining interoperability with the particular supply chain. The new architecture of the agri-supply chain also needs to solve interoperability [93], scalability, security, and privacy of personal data along with storage concerns with present single-chain networks.

Interoperability may be improved by using common standards, this idea must be implemented since it will ensure that your networks are future-proof from the start. Furthermore, it would promote a strong ecosystem while avoiding any vendor lock-in issues. In the foreseeable future, it will all come down to interoperability [94]. As a result, adopting common standards to represent your blockchain strategy is a wonderful idea. This is something to consider for blockchain installation companies. Although most platforms are silos, the technology looks to be moving toward a paradigm that can support a network of networks. You must follow a set of common blockchain implementation standards to ensure that your solution does not fall behind. Furthermore, the initial step would be to create a solution registry. In addition, all blockchain implementation companies should make their data models and regulations public. When possible, use APIs with permissioned output, and base your blockchain strategy on industry standards. For example, the Decentralized Identity Foundation [95] publishes a set of rules for identifying digital assets, persons, and organizations across multiple platforms. A variety of collaborative initiatives, such as the Enterprise Ethereum Alliance's Burrow and Hyperledger [96], support these principles. Figure 4 shows the classification of all other primary challenges such as granularity, conflicting interests, stakeholder management, etc. faced by the agriculture-supply chain traceability.

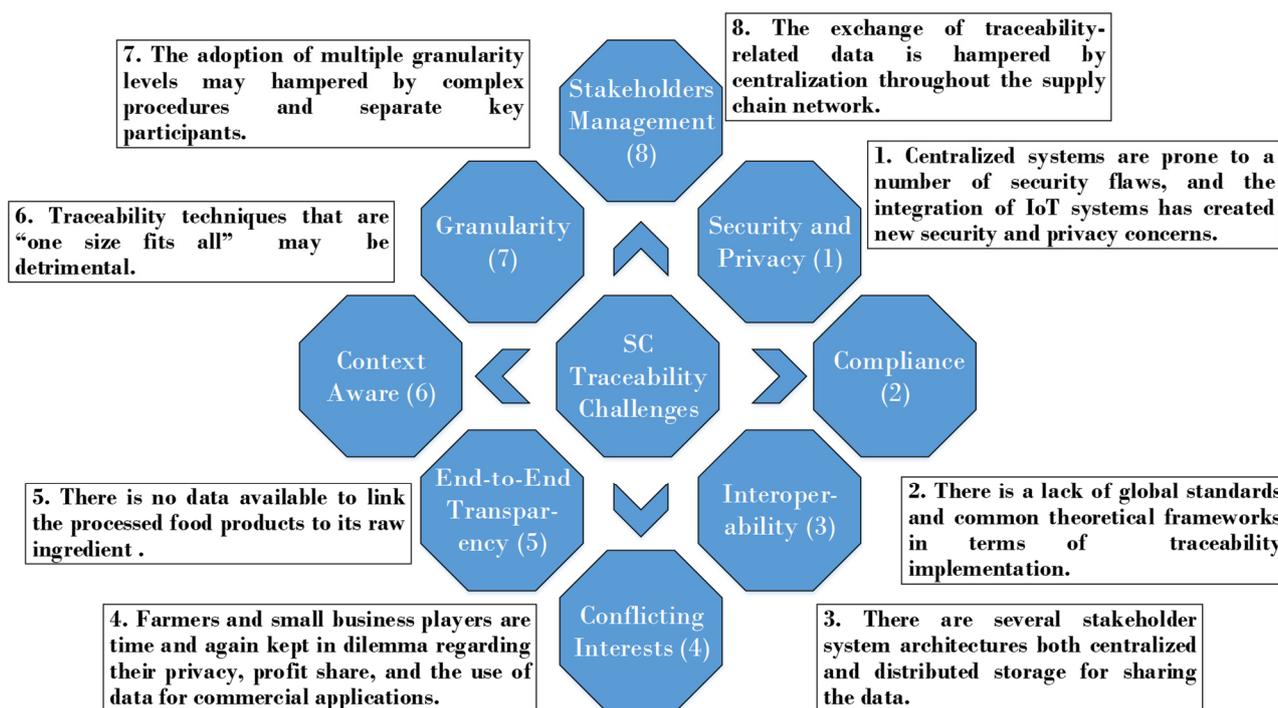


Figure 4. Supply chain (SC) traceability challenges.

7. New Agri-SCM-BIoT Architecture

New technologies that allow Industry 5.0, such as digital twins, collaborative robots, 5G and beyond, ML, IoT, edge computing, and others, when combined with human intelligence and innovation, can assist businesses in fulfilling demand and producing individualized and customized goods at a quicker rate. This enables SCM to integrate mass customization, a major idea in Industry 5.0, into their production processes [97]. Unmanned aerial vehicles are being employed in the supply chain to deliver the food packets, check and track the stocks, scan bar codes, and upload this data to warehouse systems [98,99]. Agri-food supply chains characterize a complicated system of inputs and outputs that connect agriculture farm products to consumers. Supply chains comprise several stakeholders such as financial institutes, agriculture practices, food processing industries, distributors, food retailers, and consumers. Apart from the main principle stakeholders, there are other parties like agrochemical industries, machinery and equipment manufacturers and dealers, waste processors, and feedstock supplies. As blockchain technology is submerging every sector and every organization is shifting from conventional centralized data storage to decentralized distributed ledger networks. Blockchain and decentralized ledge systems are exploding with each passing day. Thus, every industry or organization is selecting the blockchain technology that best suits its storage, security and privacy, latency, etc., requirements. Likewise, different agri-supply chain stakeholders should be able to select any distributed ledger technology while maintaining interoperability with a particular supply chain network. Therefore, interconnecting these stakeholders with different ledger technology with a particular supply chain is becoming a necessity. Storage, scalability, security, and privacy of personal data issues with the current single-chain networks also need to be addressed along with interoperability. To transfer assets in cross-blockchain systems and to solve the storage and scalability challenges of existing blockchain-based systems, we have introduced a new Agri-SCM-BIoT architecture (see Figure 4) for the agriculture supply chain.

The Agri-SCM-BIoT system uses multiple blockchains to meet the requirements of the agriculture supply chain business. The local area blockchain, as represented in Figure 4, consists of a confederation of logically distinct blockchains implemented across multiple

segments of the agri-supply chain network. In which the IoT gateways and edge computing nodes [100] function as blockchain member nodes. Consequently, each local area blockchain segment can have its blockchain ledger, policies of access control, and engagement terms. Different IoT agriculture business verticals can be represented in each edge-level blockchain organization. For instance, the multiple-tiered architecture of blockchain in the agri-supply chain can be used to reduce the security attack surface and prevent potential security risks [101] in the supply chain by keeping highly sensitive information like banking information away from the potential security risk nodes. The different blockchain verticals are used to store data of that particular segment like processing enterprise data is stored in processing enterprise blockchain vertical but other entities in the network are provided with access to trace back transaction data and other information at any time. This reduces the large memory requirement at participating nodes; the data turn out to be considerably more manageable and improves the latency of the system. In this scenario, the IoT devices are not required to take part in the consensus process [102], however, issue data transactions to local area blockchains. The IoT-based agri- robots, drones [103], and machines with mobility needs can utilize cellular data networks to send transactions to their particular blockchain segments.

The local area blockchain deployments are private blockchains, where resource exhaustive consensus algorithms [100] such as PoW and PoS are not required. Any new node from outside gains accesses by getting permission from its current participating nodes. Consensus algorithms in permissioned blockchains produce complex network overhead with the increase in the node count. Consequently, puts a constraint on the number of member nodes, and requires to be adopted in localized networks. Furthermore, several design factors need to be considered towards guaranteeing the integrity of local area blockchain data contents. Since private-permissioned blockchains do not accomplish a similar degree of decentralization and irreversibility as open permissionless blockchains, it gets important to have the option to demonstrate the data of local area blockchains are unmodified. As proof of edge-level trustworthiness, it is imperative to either utilize the core-level blockchains to intermittently store a hash of some of the latest added blocks in each edge-level blockchain or utilize an independently separate public blockchain as a store for hashes of all local area blockchains. Some specific local blockchain nodes function as gateways between local area blockchain and core blockchains. These gateways are very significant for developing the inter-blockchain asset transfer in the agri-supply chain. The core blockchain segment is implemented between edge and cloud storage as shown in Figure 5 but it functions as a distributed fabric for controlling the core chain itself along with inter-chain communication among multiple local blockchains and controls access of new requesting nodes.

Core-blockchain can be deployed as a public blockchain employing consensus algorithms like PoW and PoS for ensuring secure data transactions between blockchain verticals and users. Real-time communication among the local and core blockchain in place of an authenticating medium and access control, following which inter-blockchain communications [104] can take place. Inter-blockchain and cross-blockchain communication [105] are being investigated by academicians and industries at the protocol level. Transaction fees can be implemented within the local area blockchain to secure the local blockchain segments from flooding attacks effectively in case any IoT device or devices are compromised.

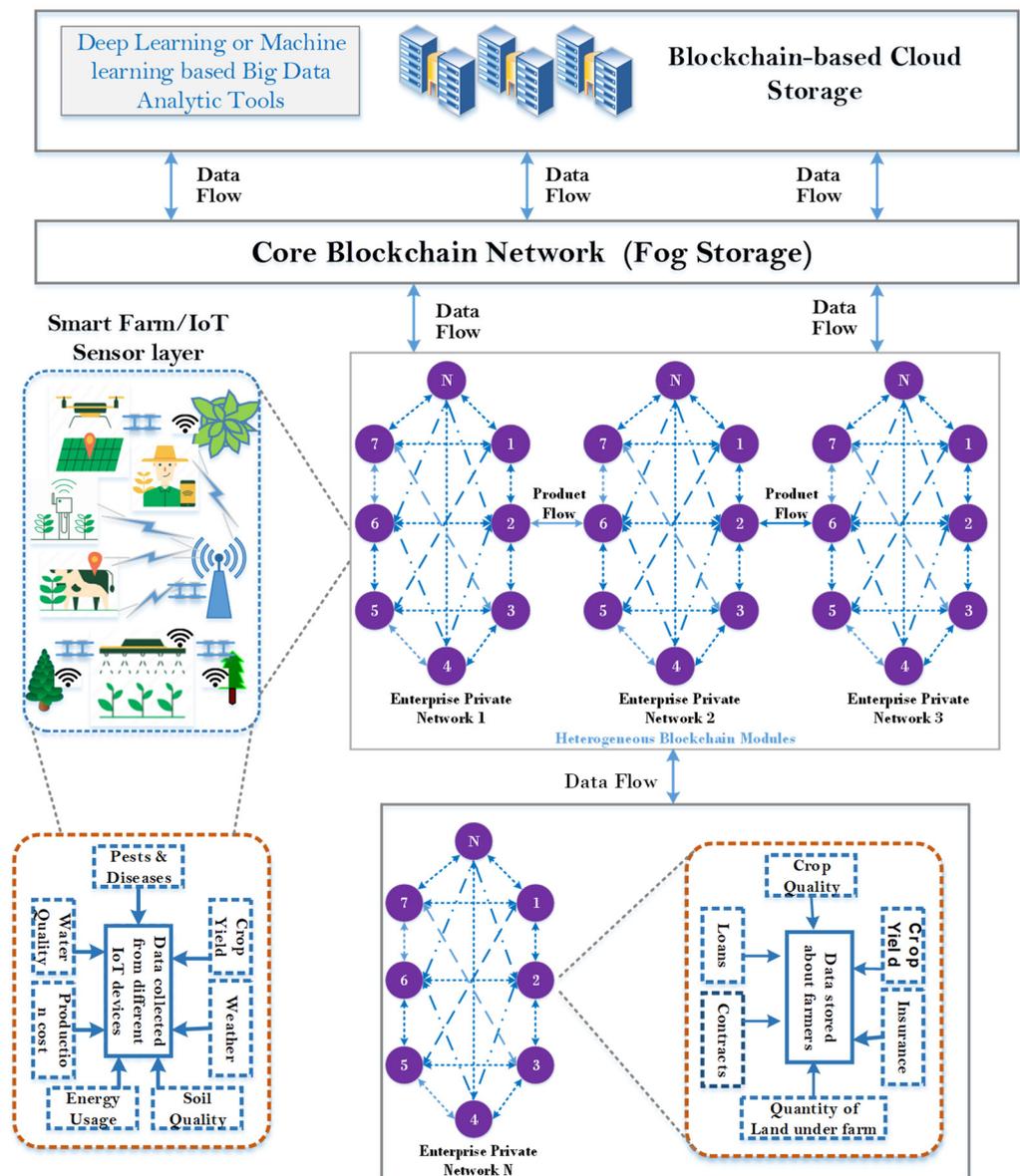


Figure 5. Proposed new Agri-SCM-BlOT Architecture.

The edge blockchain tier is responsible to process those tasks that need to be done closer to the IoT edge layer [55] for time-critical applications and transactions data gets stored on this layer. The core blockchain is used to store the recent transaction hash values only to prevent the increasing ledger size issue of the blockchain. It is also responsible for the transportation of data over IoT blockchain architecture from lower edge tiers to the cloud computing layer. Smart contracts with distributed and self-executing properties are used to automate and optimize all the processes (such as selling, purchase, asset transfer) [106] in the network. Smart contracts [107] will be used to assist in simplifying the whole process and enhance transparency throughout the supply chain. Supervisory control and data acquisition system (SCDAS) [108] is utilized by industry stakeholders to take different management decisions and control different processes in the supply chain. Therefore, the vision and concept of multi-tiered blockchain-edge architecture for multiple segment agri-supply chains is an achievable objective for providing distributed security.

Data and statistical methods can be used in big supply chain analysis to enhance decisions across the whole supply chain. The widespread use of linked devices like vehicles, RFID readers, mobile platforms, cameras, and sensor networks creates a large amount of

data. Companies may use big data analytics along with ML techniques to utilize this data to develop the attitude, skill set, and technology necessary to develop as a data factory [109]. Moreover, big data analytics [110] may contribute to the development of new approaches to enhance supply chain decision-making mechanisms, ranging from improved frontline operations to improved policy decisions, like the choice of a suitable supply chain operating model. The ML-based decision support system [111,112] can be employed at the edges itself as well as at the data servers to process the collected data. Manufacturers and distributors can properly estimate consumer demand using big data analysis and advanced predicting methodologies that take into account many elements such as weather, special events, and constantly evolving marketing trends. Amazon aims to use a predictive delivery system in the future [113], in which things are dispatched even before a buyer placed an order. Big data analytics employing deep learning and machine learning algorithms can be used to analyze the behavior of sensor nodes to detect any adversaries and potential security threats in the network. If any node is behaving maliciously, we can remove that node without affecting the rest of the network by comparing the current node behavior with the normal behavior of the node.

Thus, blockchains in food-supply chains can strengthen the growing transparency in supply chains due to the immutable transparent and decentralized nature of blockchain. It has the potential to impact each stage of the agriculture value chain. With IoT and smart contracts, blockchain could trace back the problem source, give real-time alerts on problem occurrence, assist in establishing confidence and trust between farmers, industries, and consumers. Besides, facilitate the fast execution of contracts, thus decreasing cost and delays, and could be employed for food certification. Due to its automated nature, the proposed methodology provides significant efficiency gains, which removes hidden expenses and paper burdens from the agriculture supply chain traceability process. Aside from the fundamental security and privacy of blockchain technology architecture, the presented models provide tremendous advantages regarding auditability and trust (auditable records) which can be viewed and utilized by important participants or external stakeholders such as regulators, legislators, and so on). It should also be mentioned that the suggested modeling technique has the considerable quality and reliability benefits. An immutable and decentralized traceability technology protects quality by detecting and preventing tampering with food data. As a result, the excellent quality of food items given to end-customers strengthens the agriculture food supply chain participants' business operations. The proposed system will have the following characteristics as discussed.

7.1. System Storage and Performance Enhancement

The continuous expanding nature of blockchain affects the throughput and redundancy by exhausting the system resources with managing the expanded data processing and communications [114]. The application of PoW for fast mining is a very expensive and power-intensive consensus algorithm that reduces the performance of the whole blockchain network. By applying modular architecture can solve the ever-increasing size of blockchain in the state-of-the-art by storing data on multiple blockchains. The different blockchain modules such as farm blockchain will store data related to farms and processing enterprise blockchain will data related to different enterprises. This core blockchain module is designed to store only hash values of the previous transactions to solve the expanding ledger size issues and lower blockchains (private blockchain verticals) blockchain is used to store transaction data. The bulk data is stored in the blockchain-based cloud storage for further data abstraction and processing.

7.2. Privacy and Security Enhancement

In traditional blockchain systems, the data is stored on a single ledger, and every node in the network can access that information. This enables the users to access the data that they do not require access to, thus giving rise to data confidentiality issues. Besides, there are other security vulnerabilities and threats such as 51% of attacks and

double-spending attack problems. In the proposed architecture, we have tried to reduce the security attack surface and prevent potential security risks in the supply chain by making highly sensitive information inaccessible from potential high-risk nodes. There are some master nodes in each blockchain vertical that are authorized to coordinate and communicate with other blockchain verticals. These master nodes are made highly secure and have high computational resources than other nodes, which reduces the risk of 51% attacks as well. Some of the data transactions require to get verified by multiple blockchain vertical verification. This gives an additional layer of security along with decreasing transaction congestion in one blockchain vertical as transactions get shifted to another vertical. The participating corporations or entities in the smart agriculture supply chain can keep the secrecy of their information and specify complex smart contract-based verification within the network.

7.3. Cross-Chain Communication between Heterogeneous Blockchain Platforms

In the proposed architecture, we can think through a multi-organization setup where organizations can communicate with multiple organizations (i.e., one or more). These underlying blockchain networks connected these entities could be a private or public network (permissioned or permissionless) and each cooperate has its own IoT applications and business models [106]. The proposed model proposes the amalgamation of cooperate-owned private and public blockchains that facilitates verification of private data and exchange of public data as required. The private information of different organizations makes the block generation rate unpredictable. This property makes it hard for the adversary to execute malicious activities in comparison to a public blockchain where block generation is known.

7.4. IoT Device Authentication and Data Authentication and Integrity

Due to heavy IPv6 stake for IoT devices, we will use 20-byte addressing generated by using the Elliptical Curve Digital Signature Algorithm (ECDSA) in blockchain, which will act as a global unique identity (GUID) need no individual authentication for each IoT device due to a large number of addresses generated (about 1.46×10^{48}) having exceptionally low collision likelihood. The IoT devices will authenticate and sign the data by the assigned GUI before transmission, thus authorizing the data authentication and integrity. The use of GUID can eradicate the need for a public-key management system, therefore significantly simplifying the other security protocols. Thus, lightweight security protocols can be used for communication in resource constraint devices. Big data analytics employing deep learning and machine learning algorithms can be used to analyze the behavior of sensor nodes to detect any adversaries and potential security threats in the network. If any node is behaving maliciously, we can remove that node without affecting the rest of the network by comparing the current node behavior with the normal behavior of the node.

7.5. Managerial Implications of Various Stakeholders

With the apparent technical transformations delivered by blockchain, big data, AI, and smart farming, we look to comprehend the stakeholder networks around the smart farm. These technologies have caused a significant advancement in the partner network function and how they interact with one another in the food supply chain [115]. In the proposed system architecture, the implementation of multiple blockchains for different levels is used to improve the efficiency of data management and privacy of the stakeholders in the smart agriculture system. Each stakeholder needs to manage and store the related data to that blockchain vertical. Thus, reduces the resource consumption by miners in storing the same information by different stakeholders, but the shared data of one stakeholder can be accessed by other stakeholders through a specific established authentication process (consensus process).

7.6. Transparency in the Agri-Supply Chain

Blockchain in food supply chains can strengthen the growing transparency in supply chains due to the immutable transparent and decentralized nature of blockchain. It has the potential to impact each stage of the agriculture value chain [116,117]. With IoT and smart contracts, blockchain could trace back the problem source, give real-time alerts on problem occurrence, assist in establishing confidence and trust between farmers, industries, and consumers, facilitate the fast execution of contracts, thus decreasing cost and delays, and could be employed for food certification.

8. Future Work

An absence of information security and confidentiality negatively influences the accuracy of the process, as stakeholders such as farmers are fearful of information leakage during transfer to other external systems. Moreover, participants in the agri-supply chain do not want to share their information with the business rivals in a transparent system. Even though different schemes for data security and privacy, like ring signatures, have been utilized for blockchain-based farming, there are no techniques to conceal the transaction data of senders and recipients and the amount of the transaction. Hence, information control and assurance are significant in IoT and blockchain-based agribusiness. Future studies should concentrate on how to concurrently hide the multi-party transaction information in hypothetical examination and implementation practices. Also, the roles and elements of governments in endorsing these new technological developments should be assessed. Besides, it is also critical to assess the behavior of users and hence add to information assurance, and how to lessen reservation of information sharing in blockchain-based agribusiness.

Scalability issues come in the study of both IoT and blockchain-based agri-sector. Critical problems of latency and scalability are not studied sufficiently in the blockchain-based agriculture supply chain. The convergence of different technologies like IoT and AI in the blockchain is already been investigated in academia and industry for sustainability. Then the outcome of the investigations can be applied to the innovation for agriculture industry sustainable development.

The apprehension of financial investment retrieval in the implementation of these advanced technologies among farmers is a concern. Future opportunities should utilize the “theory of inventive problem solving” to develop technologies to decrease expenses. Political scholars require researching how to encourage policymakers efficiently to devise proper policies to encourage technology innovation. High energy usage and carbon dioxide emissions are the foremost glitches, which oppose the objective of a sustainable environment. Further research needs to perform comparative studies on the development of agri-sector, based on different IoT and blockchain applications, to distinguish and promote eco-friendly and green technologies.

The nonexistence of uniform standards is the main hindrances to policies and guidelines with which participants can follow. These standards build up market stability by regulating the participants’ behavior, boosting public trust, and the adoption of technological inventions. Future investigation can study policies and standards in the agriculture sector; though, implementation of identical standards is deeply dependent on various stakeholders in the supply chain who control the equipment, systems, hardware, and software development. For imposing standards at various points of the supply chain future studies must examine the government roles and functions. Researchers should explore how management integrates resources, synchronize, addresses conflicts, and promote more schemes to enhance the impacts of these technologies in the agri-sector.

9. Conclusions

It is well understood from the literature review that the application of blockchain, AI, and IoT in agriculture is still in the developing stage. The existing work mainly comprises evocative and prescriptive studies with very few definite systems being designed and

implemented, even at the prototype level. There is a requirement of implementing a large number of real-time use cases to analyze the suggested results that many existing works claim including improved performance, intelligent decision support, security, and privacy of different acting entities throughout the supply chain, enhanced food safety, and environment-friendly techniques. Besides, there is a need to develop optimization tools to implement the existing solutions of these technologies in agriculture applications and can assist in addressing various implementation challenges. Motivated by the characteristics and solutions offered by technologies such as blockchain technology, IoT, and AI to deliver reliable, transparent, secure services and smart decision support systems for all supply chain management operations, this study presents Agri-SCM-BIoT architecture (cf. Figure 5) to address storage and scalability optimization, interoperability, security and privacy issues, and storage concerns with existing single-chain agriculture supply chain systems. The new Agri-SCM-IoT infrastructure should be built to use as minimum computing power, memory, energy, and bandwidth as possible. Because of the sensors' limited capabilities, including security elements to ensure Confidentiality, Integrity, and Availability is difficult. However, because it includes several stakeholders and diverse parties, it is necessary to develop a trustworthy blockchain-based cross-chain SCM system. The future smart and secure SCM system should be resource-efficient, appropriate, simple to implement, provide interoperability, and most importantly, trustworthy without the need for human participation. Even though the literature studied on the blockchain, AI, and IoT in the agriculture supply chain highlight remarkable growth in the sector, there are significant limitations and research gaps hindering the implementation of these technologies and extensively the sustainable development of the agriculture sector. We expect that this study will provide enhanced understanding and guidance for the further research and implementation of smart agri-supply chain management using these technologies.

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

Funding: This study is supported by the Ministry of Science and Technology (MOST) of Taiwan under the grant "MOST 109-2622-8-007-019-TE2".

Data Availability Statement: Previously reported data used to support this study and are available at DOI or other persistent identifiers. These prior studies are cited at relevant places within the text as references.

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

References

1. Bhat, S.A.; Huang, N.-F. Big Data and AI Revolution in Precision Agriculture: Survey and Challenges. *IEEE Access* **2021**, *9*, 110209–110222. [[CrossRef](#)]
2. Commission, C.A. Principles for traceability/Product tracing as a tool within a food inspection and certification system. *CAC/GL* **2006**, *60*, 1–4.
3. Charlebois, S.; Sterling, B.; Haratifar, S.; Naing, S.K. Comparison of global food traceability regulations and requirements. *Compr. Rev. Food Sci. Food Saf.* **2014**, *13*, 1104–1123. [[CrossRef](#)]
4. Bosona, T.; Gebresenbet, G. Food traceability as an integral part of logistics management in food and agricultural supply chain. *Food Control* **2013**, *33*, 32–48. [[CrossRef](#)]
5. Özer, Ö.; Zheng, Y.; Chen, K.-Y. Trust in forecast information sharing. *Manag. Sci.* **2011**, *57*, 1111–1137. [[CrossRef](#)]
6. Lu, Q.; Xu, X. Adaptable blockchain-based systems: A case study for product traceability. *IEEE Softw.* **2017**, *34*, 21–27. [[CrossRef](#)]
7. Lin, J.; Shen, Z.; Zhang, A.; Chai, Y. Blockchain and IoT based food traceability for smart agriculture. In Proceedings of the 3rd International Conference on Crowd Science and Engineering, Singapore, 28–31 July 2018.

8. Caro, M.P.; Ali, M.S.; Vecchio, M.; Giaffreda, R. Blockchain-based traceability in Agri-Food supply chain management: A practical implementation. In Proceedings of the 2018 IoT Vertical and Topical Summit on Agriculture—Tuscany (IOT Tuscany), Tuscany, Italy, 8–9 May 2018.
9. Leng, K.; Bi, B.; Jing, L.; Fu, H.C.; Nieuwenhuyse, I.V. Research on agricultural supply chain system with double chain architecture based on blockchain technology. *Future Gener. Comput. Syst.* **2018**, *86*, 641–649. [[CrossRef](#)]
10. Surasak, T.; Wattanavichean, N.; Preuksakarn, C.; Huang, S.C.H. Thai agriculture products traceability system using blockchain and internet of things. *System* **2019**, *14*, 15. [[CrossRef](#)]
11. Mao, D.; Wang, F.; Hao, C.; Li, H. Credit evaluation system based on blockchain for multiple stakeholders in the food supply chain. *Int. J. Environ. Res. Public Health* **2018**, *15*, 1627. [[CrossRef](#)]
12. Dey, S.; Saha, S.; Singh, A.K.; McDonald-Maier, K. FoodSQRBlock: Digitizing Food Production and the Supply Chain with Blockchain and QR Code in the Cloud. *Sustainability* **2021**, *13*, 3486. [[CrossRef](#)]
13. Tian, F. A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things. In Proceedings of the 2017 International Conference on Service Systems and Service Management, Dalian, China, 16–18 June 2017.
14. Demestichas, K.; Peppes, N.; Alexakis, T.; Adamopoulou, E. Blockchain in agriculture traceability systems: A review. *Appl. Sci.* **2020**, *10*, 4113. [[CrossRef](#)]
15. Menon, S.; Jain, K. Blockchain Technology for Transparency in Agri-Food Supply Chain: Use Cases, Limitations, and Future Directions. *IEEE Trans. Eng. Manag.* **2021**, 1–15. [[CrossRef](#)]
16. Tiwari, U. Application of Blockchain in Agri-Food Supply Chain. *Br. Int. Exact Sci. J.* **2020**, *2*, 574–589. [[CrossRef](#)]
17. Sharma, A.; Jhamb, D.; Mittal, A. Food Supply Chain Traceability by Using Blockchain Technology. *J. Comput. Theor. Nanosci.* **2020**, *17*, 2630–2636. [[CrossRef](#)]
18. Fernandez, A.; Waghmare, A.; Tripathi, S. Agricultural supply chain using blockchain. In Proceedings of the International Conference on Intelligent Manufacturing and Automation, Mumbai, India, 27–28 March 2020; Springer: Berlin/Heidelberg, Germany, 2020.
19. Carter, C.R.; Rogers, D.S. A Framework of Sustainable Supply Chain Management: Moving toward New Theory. *Int. J. Phys. Distrib. Logist. Manag.* **2008**, *38*, 360–387. [[CrossRef](#)]
20. Pizzuti, T.; Mirabelli, G. The Global Track&Trace System for food: General framework and functioning principles. *J. Food Eng.* **2015**, *159*, 16–35.
21. Lakhani, K.R.; Iansiti, M. The truth about blockchain. *Harv. Bus. Rev.* **2017**, *95*, 119–127.
22. Mejia, C.; McEntire, J.; Keener, K.; Muth, M.; Nganje, W.; Stinson, T.; Jensen, H. Traceability (product tracing) in food systems: An IFT report submitted to the FDA, volume 2: Cost considerations and implications. *Compr. Rev. Food Sci. Food Saf.* **2010**, *9*, 159–175.
23. Bozarth, C.C.; Handfield, R.B.; Weiss, H.J. *Introduction to Operations and Supply Chain Management*; Pearson Prentice Hall: Upper Saddle River, NJ, USA, 2008.
24. Aung, M.M.; Chang, Y.S. Traceability in a food supply chain: Safety and quality perspectives. *Food Control* **2014**, *39*, 172–184. [[CrossRef](#)]
25. Golan, E.H.; Krissoff, B.; Kuchler, F.; Calvin, L.; Nelson, K.; Price, G. *Traceability in the US Food Supply: Economic Theory and Industry Studies*; Agricultural Economic Report No. (AER-830); United States Department of Agriculture: Washington, DC, USA, 2004; pp. 1–56.
26. Baker, J.; Steiner, J. Provenance Blockchain: The Solution for Transparency in Product Supply Chains. Provenance. 2015. Available online: <https://www.provenance.org/whitepaper> (accessed on 10 September 2021).
27. Ally, M. Blockchain: Music Without the Middlemen? Retrieved May 2016, 12, 2017.
28. AgriOpenData. Available online: <https://www.agriopendata.it/> (accessed on 12 September 2021).
29. Tian, F. An agri-food supply chain traceability system for China based on RFID & blockchain technology. In Proceedings of the 13th International Conference on Service Systems and Service Management (ICSSSM), Kunming, China, 24–26 June 2016.
30. Arc-Net. Available online: <http://arc-net.io/> (accessed on 15 September 2021).
31. IBM. Available online: <http://fortune.com/2017/08/22/walmart-blockchain-ibm-food-nestleunilever-tyson-dole/> (accessed on 15 September 2021).
32. Ripe. Available online: <https://ripe.io/> (accessed on 20 September 2021).
33. Pass, R.; Shi, E. Fruitchains: A fair blockchain. In Proceedings of the ACM Symposium on Principles of Distributed Computing, Washington, DC, USA, 25–27 July 2017.
34. Dakshayini, M.; Prabhu, B.B. An effective big data and blockchain (BD-BC) based decision support model for sustainable agriculture system. In Proceedings of the EAI International Conference on Big Data Innovation for Sustainable Cognitive Computing, Coimbatore, India, 18–19 December 2020; Springer: Berlin/Heidelberg, Germany, 2020.
35. Nguyen, T.; Das, A.; Tran, L. NEO smart contract for drought-based insurance. In Proceedings of the 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada, 5–8 May 2019.
36. Haiwu, H.; An, Y.; Zehua, C. Survey of smart contract technology and application based on blockchain. *J. Comput. Res. Dev.* **2018**, *55*, 2452.
37. Delmolino, K.; Arnett, M.; Kosba, A.; Miller, A.; Shi, E. Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 22–26 February 2016; Springer: Berlin/Heidelberg, Germany, 2016.

38. 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, 23–25 May 2016.
39. Bogner, A.; Chanson, M.; Meeuw, A. A Decentralised Sharing App running a Smart Contract on the Ethereum Blockchain. In Proceedings of the 6th International Conference on the Internet of Things, Stuttgart, Germany, 7–9 November 2016; pp. 177–178, Association for Computing Machinery.
40. Gallersdörfer, U.; Matthes, F. TeSC: TLS/SSL-Certificate Endorsed Smart Contracts. In Proceedings of the 2021 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), Online Event, 23–26 August 2021.
41. Hoffman, P.; Schlyter, J. *The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA*; RFC: Marina del Rey, CA, USA, 2012.
42. Prause, G.; Mendez, M.M.; Garcia-Agreda, S. Attitudinal loyalty and trust in entrepreneurship: Building new relationships. *Int. Entrep. Manag. J.* **2013**, *9*, 531–540. [[CrossRef](#)]
43. Wu, L. Blockchain Smart Contracts in Megacity Logistics. Master’s Thesis, Department of Information Science and Technology, Pennsylvania State University, State College, PA, USA, 2018.
44. Nyhuis, P.; Wiendahl, H.-P. *Fundamentals of Production Logistics: Theory, Tools and Applications*; Springer Science & Business Media: Berlin, Germany, 2008.
45. Schmidt, M.; Münzberg, B.; Nyhuis, P. Determining lot sizes in production areas—exact calculations versus research based estimation. *Procedia CIRP* **2015**, *28*, 143–148. [[CrossRef](#)]
46. Vangala, A.; Das, A.K.; Kumar, N.; Alazab, M. Smart secure sensing for IoT-based agriculture: Blockchain perspective. *IEEE Sens. J.* **2020**, *21*, 17591–17607. [[CrossRef](#)]
47. Sarraguça, M.C.; Paulo, A.; Alves, M.M.; Dias, A.M.; Lopes, J.A.; Ferreira, E.C. Quantitative monitoring of an activated sludge reactor using on-line UV-visible and near-infrared spectroscopy. *Anal. Bioanal. Chem.* **2009**, *395*, 1159–1166. [[CrossRef](#)]
48. Schander, C.; Kenneth, H.M. DNA, PCR and formalinized animal tissue—A short review and protocols. *Org. Divers. Evol.* **2003**, *3*, 195–205. [[CrossRef](#)]
49. Renpenning, J.; Hitzfeld, K.L.; Gilevska, T.; Nijenhuis, I.; Gehre, M. Richnow HH. Development and validation of an universal interface for compound-specific stable isotope analysis of chlorine ($^{37}\text{Cl}/^{35}\text{Cl}$) by GC-high-temperature conversion (HTC)-MS/IRMS. *Anal. Chem.* **2015**, *87*, 2832–2839. [[CrossRef](#)]
50. Domon, B.; Aebersold, R. Mass spectrometry and protein analysis. *Science* **2006**, *312*, 212–217. [[CrossRef](#)]
51. Coskun, O. Separation techniques: Chromatography. *N. Clin. Istanbul.* **2016**, *3*, 156.
52. Callejón, R.M.; Rodríguez-Naranjo, M.I.; Ubeda, C.; Hornedo-Ortega, R.; Garcia-Parrilla, M.C.; Troncoso, A.M. Reported foodborne outbreaks due to fresh produce in the United States and European Union: Trends and causes. *Foodborne Pathog. Dis.* **2015**, *12*, 32–38. [[CrossRef](#)]
53. Kumarathunga, M. Improving Farmers’ Participation in Agri Supply Chains with Blockchain and Smart Contracts. In Proceedings of the Seventh International Conference on Software Defined Systems (SDS), Paris, France, 30 June–3 July 2020.
54. Mirabelli, G.; Solina, V. Blockchain and agricultural supply chains traceability: Research trends and future challenges. *Procedia Manuf.* **2020**, *42*, 414–421. [[CrossRef](#)]
55. Torky, M.; Hassanein, A.E. Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges. *Comput. Electron. Agric.* **2020**, *178*, 105476. [[CrossRef](#)]
56. Singh, P.; Singh, N. Blockchain With IoT and AI: A Review of Agriculture and Healthcare. *Int. J. Appl. Evol. Comput.* **2020**, *11*, 13–27. [[CrossRef](#)]
57. Hu, S.; Huang, S.; Huang, J.; Su, J. Blockchain and edge computing technology enabling organic agricultural supply chain: A framework solution to trust crisis. *Comput. Ind. Eng.* **2021**, *153*, 107079. [[CrossRef](#)]
58. Hou, L.; Liao, R.; Luo, Q. IoT and Blockchain-Based Smart Agri-food Supply Chains. In *Handbook of Smart Cities*; Springer: Cham, Switzerland, 2021; Volume 1, pp. 1109–1130.
59. Bermejo, F.; Aguas, M.; Chaparro, M.; Domènech, E.; Echarri, A.; García-Planella, E.; Guerra, I.; Gisbert, J.P.; López-Sanromán, A. Recommendations of the Spanish Working Group on Crohn’s Disease and Ulcerative Colitis (GETECCU) on the use of thiopurines in inflammatory bowel disease. *Gastroenterol. Hepatol. (Engl. Ed.)* **2018**, *41*, 205–221. [[CrossRef](#)]
60. Mahoney, D. Safety of fresh produce—Should consumers worry? *Food Aust.* **2021**, *73*, 28–31.
61. Shahid, A.; Almogren, A.; Javaid, N.; Al-Zahrani, F.A.; Zuair, M.; Alam, M. Blockchain-based agri-food supply chain: A complete solution. *IEEE Access* **2020**, *8*, 69230–69243. [[CrossRef](#)]
62. Huang, H.; Zhou, X.; Liu, J. Food supply chain traceability scheme based on blockchain and EPC technology. In Proceedings of the International Conference on Smart Blockchain, Birmingham, UK, 11–13 October 2019; Springer: Berlin/Heidelberg, Germany, 2019.
63. Salah, K.; Nizamuddin, N.; Jayaraman, R.; Omar, M. Blockchain-based soybean traceability in agricultural supply chain. *IEEE Access* **2019**, *7*, 73295–73305. [[CrossRef](#)]
64. Davcev, D.; Carbone, A.; Mitreski, K.; Kocarev, L.; Stankovski, V. Blockchain-based distributed cloud/fog platform for IoT supply chain management. In Proceedings of the Eighth International Conference on Advances in Computing, Electronics and Electrical Technology (CEET), Kuala Lumpur, Malaysia, 3–4 February 2018.
65. Salihoglu, G.; Salihoglu, N.K.; Ucaroglu, S.; Banar, M. Food loss and waste management in Turkey. *Bioresour. Technol.* **2018**, *248*, 88–99. [[CrossRef](#)] [[PubMed](#)]

66. Waqas, M.; Nizami, A.S.; Aburiazaiza, A.S.; Barakat, M.A.; Rashid, M.I.; Ismail, I.M.I. Optimizing the process of food waste compost and valorizing its applications: A case study of Saudi Arabia. *J. Clean. Prod.* **2018**, *176*, 426–438. [[CrossRef](#)]
67. Baralla, G.; Pinna, A.; Corrias, G. Ensure traceability in European food supply chain by using a blockchain system. 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.
68. Dasaklis, T.; Casino, F. Improving vendor-managed inventory strategy based on Internet of Things (IoT) applications and blockchain technology. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea, 14–17 May 2019.
69. Goldratt, E.M.; Cox, J. *The Goal: A Process of Ongoing Improvement*; Routledge: Abingdon, UK, 2016.
70. Abolghasemi, M.; Beh, E.; Tarr, G.; Gerlach, R. Demand forecasting in supply chain: The impact of demand volatility in the presence of promotion. *Comput. Ind. Eng.* **2020**, *142*, 106380. [[CrossRef](#)]
71. Zhou, H.; Benton, W., Jr. Supply chain practice and information sharing. *J. Oper. Manag.* **2007**, *25*, 1348–1365. [[CrossRef](#)]
72. Dong, X.; Zheng, X.; Lu, X.; Lin, X. A traceability method based on blockchain and internet of things. In Proceedings of the 2019 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCLOUD/SocialCom/SustainCom), Xiamen, China, 16–18 December 2019.
73. Hassija, V. Hassija, V.; Chamola, V.; Gupta, V.; Jain, S.; Guizani, N. A survey on supply chain security: Application areas, security threats, and solution architectures. *IEEE Internet Things J.* **2020**, *8*, 6222–6246. [[CrossRef](#)]
74. Umamaheswari, S.; Sreeram, S.; Kritika, N.; Prasanth, D. Biot: Blockchain based IoT for agriculture. In Proceedings of the 2019 11th International Conference on Advanced Computing (ICoAC), Chennai, India, 18–20 December 2019.
75. Tsang, Y.P.; Choy, K.; Wu, C.H.; Ho, G.T.S.; Lam, H. Blockchain-driven IoT for food traceability with an integrated consensus mechanism. *IEEE Access* **2019**, *7*, 129000–129017. [[CrossRef](#)]
76. Jiang, W.; Li, H.; Xu, G.; Wen, M.; Dong, G.; Lin, X. PTAS: Privacy-preserving thin-client authentication scheme in blockchain-based PKI. *Future Gener. Comput. Syst.* **2019**, *96*, 185–195. [[CrossRef](#)]
77. Shen, M.; Tang, X.; Zhu, L.; Du, X. Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. *IEEE Internet Things J.* **2019**, *6*, 7702–7712. [[CrossRef](#)]
78. Ma, M.; Shi, G.; Li, F. Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario. *IEEE Access* **2019**, *7*, 34045–34059. [[CrossRef](#)]
79. Novo, O. Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet Things J.* **2018**, *5*, 1184–1195. [[CrossRef](#)]
80. Ding, S.; Cao, J.; Li, C.; Fan, K. A novel attribute-based access control scheme using blockchain for IoT. *IEEE Access* **2019**, *7*, 38431–38441. [[CrossRef](#)]
81. Zhou, L.; Wang, L.; Lv, P.; Sun, Y. Beekeeper: A blockchain-based iot system with secure storage and homomorphic computation. *IEEE Access* **2018**, *6*, 43472–43488. [[CrossRef](#)]
82. Hammi, M.T.; Hammi, B.; Bellot, P.; Serhrouchni, A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Comput. Secur.* **2018**, *78*, 126–142. [[CrossRef](#)]
83. Derhab, A.; Guerroumi, M.; Gumaei, A.; Maglaras, L.; Ferrag, M.A.; Mukherjee, M.; Khan, F.A. Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security. *Sensors* **2019**, *19*, 3119. [[CrossRef](#)] [[PubMed](#)]
84. Sharma, P.K.; Singh, S.; Jeong, Y.S.; Park, J.H. Distblocknet: A distributed blockchains-based secure sdn architecture for iot networks. *IEEE Commun. Mag.* **2017**, *55*, 78–85. [[CrossRef](#)]
85. Chae, C.-J.; Cho, H.-J. Enhanced secure device authentication algorithm in P2P-based smart farm system. *Peer Peer Netw. Appl.* **2018**, *11*, 1230–1239. [[CrossRef](#)]
86. Patil, A.S.; Tama, B.A.; Park, Y.; Rhee, K.H. A Framework for Blockchain Based Secure Smart Green House Farming. In *Advances in Computer Science and Ubiquitous Computing*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 1162–1167.
87. Puthal, D.; Malik, N.S.; Mohanty, S.P.; Kougianos, E. Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. *IEEE Consum. Electron. Mag.* **2018**, *7*, 6–14. [[CrossRef](#)]
88. Digiteum. Available online: <https://www.digiteum.com/iot-supply-chain/> (accessed on 20 September 2021).
89. Muhtasim, M.A.; Fariha, S.R.; Rashid, R.; Islam, N. Secure data transaction and data analysis of IOT devices using blockchain. In Proceedings of the 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET), Kottayam, India, 21–22 December 2018.
90. Ponnappalli, S.; Shah, A.; Banerjee, S. RainBlock: Faster Transaction Processing in Public Blockchains. In Proceedings of the 2021 (USENIX) Annual Technical Conference (USENIX)(ATC) 21), Santa Clara, CA, USA, 14–16 July 2021.
91. Li, S.; Yu, M.; Yang, C.H.; Avestimehr, A.S.; Kannan, S.; Viswanath, P. Polyshard: Coded sharding achieves linearly scaling efficiency and security simultaneously. *IEEE Trans. Inf. Forensics Secur.* **2020**, *16*, 249–261. [[CrossRef](#)]
92. Zhou, Q.; Huang, H.; Zheng, Z. Solutions to scalability of blockchain: A survey. *IEEE Access* **2020**, *8*, 16440–16455. [[CrossRef](#)]
93. Schulte, S.; Sigwart, M.; Frauenthaler, P.; Borkowski, M. Towards blockchain interoperability. In Proceedings of the International Conference on Business Process Management, Vienna, Austria, 6–10 September 2019; Springer: Berlin/Heidelberg, Germany, 2019.
94. Bhatia, R. Interoperability solutions for blockchain. In Proceedings of the 2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), Bengaluru, India, 9–10 October 2020.

95. Decentralized Identity Foundation. Available online: <https://identity.foundation/faq/> (accessed on 30 September 2021).
96. Enterprise Ethereum Alliance's Burrow and Hyperledger. Available online: <https://www.hyperledger.org/announcements/2018/10/01/enterprise-ethereum-alliance-and-hyperledger-to-advance-the-global-blockchain-business-ecosystem> (accessed on 30 September 2021).
97. Maddikunta, P.K.R.; Pham, Q.-V.; Prabadevi, B.; Deepa, N.; Dev, K.; Gadekallu, T.R.; Ruby, R.; Liyanage, M. Industry 5.0: A survey on enabling technologies and potential applications. *J. Ind. Inf. Integr.* **2021**, *26*, 100257.
98. Reddy, P.K.; Hakak, S.; Alazab, M.; Bhattacharya, S. Unmanned Aerial Vehicles in Smart Agriculture: Applications, Requirements, and Challenges. *IEEE Sens. J.* **2021**, *21*, 17608–17619. [[CrossRef](#)]
99. Kumar, R.; Kumar, P.; Tripathi, R.; Gupta, G.P.; Gadekallu, T.R.; Srivastava, G. Sp2f: A secured privacy-preserving framework for smart agricultural unmanned aerial vehicles. *Comput. Netw.* **2021**, *187*, 107819. [[CrossRef](#)]
100. Bhat, S.A.; Sofi, I.B.; Chi, C.-Y. Edge Computing and Its Convergence With Blockchain in 5G and Beyond: Security, Challenges, and Opportunities. *IEEE Access* **2020**, *8*, 205340–205373. [[CrossRef](#)]
101. Ferrag, M.A.; Maglaras, L.; Janicke, H. *Blockchain and Its Role in the Internet of Things, in Strategic Innovative Marketing and Tourism*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 1029–1038.
102. Awan, S.H.; Ahmed, S.; Nawaz, A.; Maghdid, S.; Zaman, K.; Ali, M.Y.; Khan, Z.; Saeed, S. BlockChain with IoT, an emergent routing scheme for smart agriculture. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 420–429. [[CrossRef](#)]
103. Chinnaiyan, R.; Balachandar, S. Reliable administration framework of drones and IoT sensors in agriculture farmstead using blockchain and smart contracts. In Proceedings of the 2020 2nd International Conference on Big Data Engineering and Technology, Singapore, 3–5 January 2020.
104. Liu, X.; Chen, R.; Chen, Y.W.; Yuan, S.M. Off-chain data fetching architecture for ethereum smart contract. In Proceedings of the 2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCCBB), Fuzhou, China, 15–17 November 2018.
105. Konashevych, O. Cross-blockchain protocol for public registries. *Int. J. Web Inf. Syst.* **2020**, *16*, 571–610. [[CrossRef](#)]
106. Pillai, B.; Biswas, K.; Muthukkumarasamy, V. Cross-chain interoperability among blockchain-based systems using transactions. *Knowl. Eng. Rev.* **2020**, *35*, 1–17. [[CrossRef](#)]
107. Dietrich, F.; Turgut, A.; Palm, D.; Louw, L. Smart contract-based blockchain solution to reduce supply chain risks. In Proceedings of the IFIP International Conference on Advances in Production Management Systems, Novi Sad, Serbia, 30 August–3 September 2020; Springer: Berlin/Heidelberg, Germany, 2020.
108. Abdulrazzaq, M.; Wei, Y. Industrial Control System (ICS) Network Asset Identification and Risk Management. Master's Thesis, School of Information Technology, Halmstad University, Halmstad, Sweden, 2018.
109. Ogrea, C. Relevance of big data for business and management. Exploratory insights (Part I). *Stud. Bus. Econ.* **2018**, *13*, 153–163. [[CrossRef](#)]
110. Aliche, K.; Glatzel, C.; Hoberg, K.; Karlsson, P.-M. Big Data and the Supply Chain: The Big Supply Chain Analytics Landscape; McKinsey & Company. 2017. Available online: <https://www.mckinsey.com/business-functions/operations> (accessed on 1 October 2021).
111. Ilie-Zudor, E.; Ekárt, A.; Kemeny, Z.; Buckingham, C.; Welch, P.; Monostori, L. Advanced predictive-analysis-based decision support for collaborative logistics networks. *Supply Chain Manag. Int. J.* **2015**, *20*, 369–388. [[CrossRef](#)]
112. Merkert, J.; Mueller, M.; Hubl, M. A Survey of the Application of Machine Learning in Decision Support Systems. In Proceedings of the 23rd European Conference on Information Systems (ECIS 2015), Münster, Germany, 26–29 May 2015.
113. Amazon Patents "Anticipatory" Shipping—To Start Sending Stuff Before You've Bought It. Available online: https://techcrunch.com/2014/01/18/amazon-pre-ships/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAABeqQkKdoAfUm6xxmmQs5_zT-leA585pkcweqo-0FCgt8uIBJY3MJHqBr32MMam7UsNzchYQp3Yj5dLrMdVwC0hccuXq3GlpIFoiDqw76itdNud_uCTyTg0_uOCLD7nDQOeVEeMRj8c5A7Nd1lCkuxp_qEA8tH-k_NS0mKS2hY (accessed on 5 October 2021).
114. Awan, S.; Ahmed, S.; Ullah, F.; Nawaz, A.; Khan, A.; Uddin, M.I.; Alosaimi, W.; Alyami, H. IoT with BlockChain: A Futuristic Approach in Agriculture and Food Supply Chain. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 5580179. [[CrossRef](#)]
115. Casino, F.; Kanakaris, V.; Dasaklis, T.; Moschuris, S.; Stachtariis, S.; Pagoni, M.; Rachaniotis, N. Blockchain-based food supply chain traceability: A case study in the dairy sector. *Int. J. Prod. Res.* **2020**, *59*, 1–13. [[CrossRef](#)]
116. Saurabh, S.; Dey, K. Blockchain technology adoption, architecture, and sustainable agri-food supply chains. *J. Clean. Prod.* **2021**, *284*, 124731. [[CrossRef](#)]
117. Patra, S.S.; Misra, C.; Singh, K.; Gourisaria, M.; Choudhury, S.; Sahu, S. IoTAgriChain: IoT Blockchain Traceability Using Queueing Model in Smart Agriculture. In *Blockchain Applications in IoT Ecosystem*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 203–223.