A Literature Review of Blockchain-Based Applications in Supply Chain

Boyu Liu, Xiameng Si* and Haiyan Kang

School of Information Management, Beijing Information Science and Technology University, Beijing 100192, China
* Correspondence: sixiameng@bistu.edu.cn; Tel.: +86-1850-009-9517

Abstract: Blockchain technology is an emerging technology, and cryptocurrency is the most well-known and successful blockchain application. With the development of the concept of blockchain technology, scientists and practitioners have found the potential of blockchain technology in the supply chain, which has led to much research on blockchain applications. There have been many reviews on the subject, but most of them are specific to particular supply chains and lack specific research on published papers. This paper addresses this research gap by examining, through qualitative analysis, the study finds that blockchain applications are moving in the direction of efficient automation. Appropriate consensus algorithms in different supply chain contexts will improve efficiency while reducing costs, while smart contracts play a huge role in security. Therefore, this paper explored articles related to the topic and explored articles in recent years by keyword combination.

Keywords: blockchain technology; supply chain; application; literature review

1. Introduction

In 2008, Satoshi Nakamoto published an article named Bitcoin: A Peer-to-Peer Electronic Cash System in which he proposed the basic concept of the first cryptocurrency, Bitcoin [1]. As a well-known peer-to-peer virtual currency without a third party or a central bank, it is the first application of blockchain technology. With the rise of bitcoin, the technology underlying it has gradually drawn people’s attention. Since its birth, it has experienced many times of innovations. In the past ten years, the ‘blockchain 1.0’ is marked by encrypted digital currency and the version 2.0 is featured by smart contracts [2]. And now, the version 3.0 crosses the threshold into the stage of application, serving as the key technology that extends engagement in many areas such as finance, government affairs, supply chain, and so on [3]. Blockchain technology integrates a hash algorithm, digital signature, point-to-point transmission, consensus mechanism, and other existing technologies, so it is characterized by anti-fraud, traceability, security, and trust.

Supply chain refers to the network chain structure formed by upstream and downstream enterprises involved in the activities of providing products or services to end users in the process of production and circulation. Nowadays, globalization impacts everything, with no exception for the supply chain. The rapid development of economic globalization and the increased market competition could make the supply chain become highly complex and dynamic [4]. In recent years, customers are more demanding, e.g., expecting better-customized products and better customer service, all at an acceptable speed and cost. To effectively adapt to market changes and remain competitive, companies are now focusing on their core functions and are moving towards collective and collaborative efforts [5]. It comprises multiple stakeholders, and they could be worldwide, which leads to the high dispersion of information. Moreover, the global division of labor getting deep, modern enterprise supply chain presents the characteristics of fragmentation, complexity, and geographical dispersion [6]. To manage and share the information among these participants,
more costs are needed in the conventional supply chain, but the information asymmetry could not be fully solved. And this kind of information asymmetry could be either intentional or unintentional [4]. Therefore, information sharing and coordination of the supply chain is the key. The efficiency can be improved by enabling real-time information transfer, coordinating inventory management, increasing flexibility, and adapting to changes in demand across the supply chain [7]. However, in the process of information sharing, there may be risks of data manipulation, loss of expertise, weakened bargaining power and information disadvantage [8]. Hence, improving efficiency, boosting information sharing, and ensuring security in the supply chain at the same time became the trend of supply chain study.

As a distributed ledger, the blockchain is a chain structure connected in timestamp order through cryptography. Among them, the peer-to-peer network structure conducts the chaining or verification of transaction events through a consensus mechanism. This allows the blockchain to involve transactions between parties, and to be an immutable, secure and trustless model [9]. Therefore, there is great potential for the application of blockchain technology to supply chains. The disintermediation of blockchain can reduce the cost of transactions and information transmission, prevent fraud, and improve the transparency of information sharing. The cryptographic functions covered in it can make the sharing of information more secure. Smart contracts can improve the efficiency of transactions, automate transactions, and so on.

There are many studies on the application of blockchain technology in the supply chain, which reflects a good research prospect, but most of the related reviews are quantitative analyses. In contrast, this review will screen the papers based on the number of citations and discuss the high-quality ones. The purpose of this paper is to explore the current studies on the application of blockchain technology in the supply chain. The work aims to answer the following research question (RQ):

‘What the supply chain field needs most from blockchain technology?’

To answer the research question, we have carefully selected from the database and classified papers based on the RQ into three directions, ‘Traceability and Transparency’, ‘Trade Behavior’, and ‘Data Security and Access Control’. Reviews exist that discuss different supply chain types in terms of their application, but more often than not, the research is conducted within a specific supply chain area, which is limiting. Then this work explored the papers specifically according to the different directions.

The remainder of this paper is organized as follows. We initially provide an overview of blockchain including its origin, key features, structure, and types. We hope people could get a rough idea of blockchain in this section. And then we explain the research methodology for conducting the systematic literature review and material collection. Next, we discuss blockchain technology applications in the supply chain. Finally, it presents the discussion and conclusion.

2. Blockchain Overview

2.1. The Origin of Blockchain

In 2008, Satoshi Nakamoto published an article named ‘bitcoin: a peer-to-peer electronic cash system’, proposing a brand-new concept, bitcoin. Two months later, in 2009, the bitcoin system was published with its source code, and everyone worldwide can be a user of it. At the same time, the first block called Genesis Block was born with the initial fifty bitcoins in the world. For blockchain 1.0, Bitcoin’s enabling technology is the Blockchain Technology (BCT) as the underlying structure, which leads to the explosion of all kinds of digital cryptocurrencies based on the system. And this fever has undoubtedly drawn people’s attention to blockchain technology, which has greatly made the spread move. Besides bitcoin, people gradually tried to adopt blockchain technology in other areas, but it was hard to realize the implementation without smart contracts. The bitcoin system uses Bitcoin script to support the Unspent Transaction Output (UTXO) model and complete the Bitcoin transfer logic. Bitcoin script is extensible, and additional instructions can be added to implement more transaction types and segregated
witnesses. However, the script is in the data field of the transaction, and the logic part is coupled with the data part, which lacks flexibility. Instruction expansion is likely to cause system security risks. The script’s instruction function is Turing incomplete [10].

Smart contracts introduced into blockchain 2.0, the system logic supports users in the custom business. In 2013, the most typical system of blockchain 2.0, Ethereum, was launched. After that, considering the transparency, reliability, openness, security, immutability, and disintermediation, it is possible to adopt blockchain technology into more fields if intensive coordination is required. So far, blockchain technology has gradually expanded engagement to logistics [4], biomedical and health care [11], energy [12], and other fields.

Blockchain 3.0 is the core of the Value Internet which is a globally distributed ledger system. Although the blockchain has been applied in many industries, the blockchain applications in various industries are still independent of each other, forming information silos. However, the goal of blockchain 3.0 is to break the status quo and form an interconnected network from information silos to make big value. Through the innovation of the existing Internet system, blockchain technology will cross the threshold into the value Internet era with 5G network machine learning, the Internet of Things, and other technologies together.

In general, blockchain 1.0 is the most basic version of blockchain technology, and subsequent blockchain versions 2.0 and 3.0 are implemented based on the 1.0 framework. The blockchain 1.0 system was born to solve the shortcomings of the traditional currency system, but its application is also limited to the decentralized digital currency represented by Bitcoin. Blockchain 2.0 is marked by the development of smart contracts in Ethereum and a Turing-complete virtual machine. The biggest difference between blockchain version 2.0 and version 1.0 is the support for smart contracts. The contract program is developed through development tools, and the written content is finally deployed to the blockchain ledger. The most well-known platform is Ethereum. The function of smart contracts also enables the blockchain to expand from the original currency system to other financial application fields, including applications in securities trading, supply chain finance, banking instruments, payment clearing, anti-counterfeiting, establishing credit systems, and mutual insurance [13]. When entering the era of blockchain 3.0, its application field will go beyond the scope of digital currency or finance, and then expand to any field in need and even the whole of society. Figure 1 shows the change diagram from blockchain 1.0 to 3.0.

Figure 1. The development of blockchain technology.

2.2. The Structure of Blockchain

A blockchain should be considered as a distributed append-only timestamped data structure [14]. It is a kind of linked data structure connecting each data block in chronological order and the tamper-proof and unforgeable distributed ledger enabled by cryptography. In general, the generated data is stored in blocks, and the block connects with each other end to end in sequence to form a chain structure. At the same time, its structure and the technology within it could make the decentralized distributed ledger tamper-proof, and unforgeable and ensure security when we upload data and access the ledger. Block is the basic unit of chain structure in data storage, so it contains all transaction information. The block has two important parts, the header of the block and the body of the block.
The header of the block consists of the previous block hash, Merkle Tree Root, time stamp, and so on. The previous hash is the hash of the previous block and it is the reason why these blocks could connect with each other. Based on the previous hash, each block could find its previous block and the head is Genesis Block whose previous hash is zero. Therefore, someone could hardly deliberate and capricious alteration of some block because the manipulation would change the hash of the block and cut off the whole chain. A timestamp is complete and verifiable data that can indicate that a piece of data has existed before a certain time, usually a sequence of characters that uniquely identifies the time at a certain moment. Merkle Tree Root is a significant part of the whole block because the Merkle tree is the structure of a block. The body of the block contains all transactions in a period of time. For these transactions, they experience hash and are sorted by size to form the first layer. The value of two consecutive hash values performing the hash calculation is the element at the second layer. Repeating this process till there is only one hash value at a layer and it is Merkle Tree Root. Based on the structure, blockchain has great potential for data security. Figure 2 shows the structure of the blockchain.

![Figure 2. The structure of blockchain.](image)

### 2.3. Key Features

#### 2.3.1. Trust and Transparency

The blockchain system is decentralized forming a peer-to-peer network. The entire system is transparent to each node so that each node has the same right to send and receive messages, and all transactions in the network are transparent and visible to any node. In addition, all transactions in the network are transparent and visible to any node, and the transaction would record on the block if all nodes reach a consensus, and then each node could also record it to maintain consistency. In this way, the problem of information asymmetry in centralized systems can be easily solved. With the consensus mechanism, the blockchain ensures consistency and reliability while maintaining transparency.

#### 2.3.2. Immutability and Traceability

Immutability is a very significant part of the blockchain, which means that there is no risk of fake data or records. Immutability can attribute to two parts blockchain structure and mechanism. According to the blockchain structure we learned above, if some data is changed in a block, the information of this block would also change which leads to the next block could not find it and destroying the whole blockchain. Moreover, Merkle Tree Root is derived from all transactions through complex hash which means changing one transaction would have a totally different Merkle Tree Root. From the perspective of mechanism, the blockchain network is bound to have a consensus mechanism. Taking PBFT as an example, if someone wants to have cyber attacks, he should control more than 51-percent central processing unit (CPU) power to reach the consensus. However, the cost often outweighs more than the return, making this attack nearly impossible.

Immutability guarantees the authenticity of transactions on the blockchain, which shapes a sound environment for traceability. All transactions in the blockchain have a
complete and correct record so that participants can query all relevant information of the transaction in a certain state as needed.

2.3.3. Privacy Security

The blockchain system is a decentralized system that can achieve user privacy and security without relying on third-party protection. Through cryptography, and asymmetric encryption algorithms, users’ privacy could be well protected and transactions can be carried out without the need of disclosing their identity. Each user performs identity control through a private key, and a unique corresponding public key generates an address as a unique identity. The public key is generated from the private key, but the private key cannot be worked out from it. In the transaction process, the public key is open to other users, which can be used to encrypt the information that could only be decrypted by the corresponding private key. The private key is private and unique and is held and kept by the user. In addition to decryption, it can also act as a signature to be the user’s authorization for transactions or data.

2.4. Blockchain Type

2.4.1. Public Blockchain

The public chain, in brief, is open to everyone. In a public blockchain, each one has the right to take part in the maintenance and reading of the blockchain without the control of some central institution. The data is completely open and transparent. The public chain system is not managed by a central organization, and runs through agreed rules, and these rules can build a trusted network system in an untrusted environment. Systems that usually require public participation and maximize the transparency of data disclosure are suitable for public blockchains. For example, the bitcoin system which is one of the most well-known public blockchain systems, and its updated version Ethereum. However, in the public environment, the number of nodes is uncertain, the actual identity is unknown, and the network status is hard to confirm, these factors would also affect its reliability.

2.4.2. Consortium Blockchain

A consortium chain is usually built between multiple organizations with known identities to each other. Therefore, the alliance chain system generally requires strict identity authentication and authority management, and the number of nodes is often determined within a certain period of time, which is suitable for dealing with businesses that need to reach a consensus between organizations. Its advantages make it more popular than public blockchain. First of all, compared with the public chain, the efficiency of the consortium chain has been greatly improved. Because each participant in the consortium chain knows each other’s identities, and the number of participants is determined within a certain period of time, the number of nodes is less, and the operating efficiency of the consensus algorithm is going to be improved. Second, privacy-preserving will be more secure. The data is only accessible to the members and not accessible to non-members of the alliance. And in the same alliance, different businesses will also have isolation to a certain extent. Last, it does not need tokens to stimulate the work of the whole chain.

2.4.3. Private Blockchain

After the public chain, this part talks about the private chain. ‘Private’ means the system is not public and only serves some organizations. It is another kind of consortium blockchain that only has one member which is the organization. Private blockchain has an elaborate authority management system that all users need to carry out the authentication. In the private blockchain, everything is under control such as the number of users, and the condition of each node. Its nodes are much fewer than the public chain, and it is more efficient with safer private preserving. However, it does not fit the concept of blockchain, so it does not draw too much attention.
3. Methodology

The research methodology adopted in this study is adapted and revised from previous research [4,15–17]. This paper leverages ‘qualitative analysis’ to provide a comprehensive overview of articles on the topic of supply chains and blockchains. As blockchain and its related technologies, like smart contracts, have only just emerged in the last decade, related work, technical standards, and innovative applications are still in their infancy. This work has chosen the period 2016–2022 as the time span for this literature survey to capture the latest applications of these technologies in the supply chain.

In this work, the main purpose is to explore the application of blockchain technology in the supply chain, so it needs to specify keywords that are specific to the topic. Hence, the study utilizes the key search method to search this literature as comprehensively as can be.

- First of all, to make the search for papers more comprehensive, ‘blockchain’ with ‘supply chain’ or ‘logistics’ are combined;
- Second, to make the search more relevant to the topic, a third keyword would be added for the application, that is, ‘model’, ‘scheme’, and ‘framework’. In addition, we would add the articles with the keyword ‘smart contract’;
- Finally, based on the previous three directions, the third keywords would be replaced with ‘traceability’, ‘transparency’, ‘data’, ‘access control’, and ‘information’.

And the keyword strings are combined as shown below:

1. ‘blockchain’ AND ‘supply chain’ OR ‘logistic’;
2. ‘blockchain’ AND ‘supply chain’ OR ‘logistic’ AND ‘model’;
3. ‘blockchain’ AND ‘supply chain’ OR ‘logistic’ AND ‘framework’;
4. ‘smart contract’ AND ‘supply chain’ OR ‘logistic’;
5. ‘blockchain’ AND ‘supply chain’ OR ‘logistic’ AND ‘traceability’;
6. ‘blockchain’ AND ‘supply chain’ OR ‘logistic’ AND ‘transparency’;
7. ‘blockchain’ AND ‘supply chain’ OR ‘logistic’ AND ‘access control’;
8. ‘blockchain’ AND ‘supply chain’ OR ‘logistic’ AND ‘information’.

Through the combination of these keywords, literature was selected from the database of the Web of Science Core Collection. From the keyword combination selection, 799 papers were got from step 1 after the removal of duplicates. Then the keyword combinations 2 to 5 were executed in these 799 papers. After that, there are some papers adding for comprehensiveness with the keyword-combination 6 to 9. Finally, 285 papers were left this time. For the purpose of collecting high-quality papers, a screening standard was formulated as follows:

1. The citation of a paper in 2016 should at least 100;
2. The citation of a paper in 2017 should at least 75;
3. The citation of a paper in 2018 should at least 50;
4. The citation of a paper in 2019 should at least 25;
5. The citation of a paper in 2020 should at least 25.

The papers for 2021 and 2022 are exceptional because these papers were published over a shorter period of time. With the standard and the topic of this work, 176 papers were left. And then, an analysis of these papers was given which presented the condition from three perspectives, journal, year, and research area.

First, a word cloud of the journal is given in Figure 3. It shows the journals among the 176 papers. The bigger the font, the more the relevant paper is. As shown, ‘SUSTAINABILITY’, ‘IEEE ACCESS’, and ‘FOODS’ have more papers related to blockchain applications in the supply chain area. Second, Figure 4 gives the year-wise analysis. A substantial increase could be found in the number of papers from 2017 to 2022. From 2018 to 2019, there has been an exponential increase in the screening standard. Although 2021 shows a great boom, there is no citation standard for 2021 and 2020. Overall, the number of papers published is trending upward year on year, which also indicates that blockchain is being researched at a much faster pace in various industries. Figure 5 is the percentage ring chart of the
research area. It is very easy to find that Computer Science accounts for more than half. Telecommunications Business & Economics and Engineering are also the major areas. Food Science and Agriculture have also seen an uptrend in publishing research on blockchain applications in the supply chain area.

Figure 3. Word cloud of journal.

Figure 4. Year wise analysis.
Next, according to the RQ, the papers were classified into three directions which are ‘Traceability and Transparency’, ‘Trade Behavior’, and ‘Data Security and Access Control’. And then, papers are selected based on these directions from the 176 papers. Finally, 49 papers are left, and the selection process is summarized as shown in Figure 6. Figure 7 shows each year’s number of papers and Figure 8 shows the major journals of these papers. Therefore, the study would give the discussion and analysis of these papers in Section 4.
4. Blockchain Based Applications within Supply Chain

The continuous development and progress of blockchain technology in recent years have provided solutions to problems in the supply chain, and many articles on the application of blockchain technology to the supply chain have emerged. In this section, the work will explore the existing research from three perspectives, namely ‘traceability and transparency’, ‘Data security and access control’, and ‘trade behavior’. In addition, Figures 9–11 would show the paper refers to which method and topic in each section.
4.1. Traceability and Transparency

With the supply chain getting complex, traceability and information transparency play significant roles in the whole supply chain. Combining the two aspects, traceability and transparency, the question of ‘what, when, where, and how’ about some transaction in the supply chain can be answered [56]. Although traceability and transparency have an interconnection, they could not be used as one word and they are two different concepts. Traceability refers to the ability to track and trace information, which could create transparency in the supply chain [57]. Regarding transparency, some use the terms visibility and information sharing interchangeably. For visibility, some argue that it represents all stakeholders in the supply chain having a shared understanding and access to the product-related information they request without loss, noise, delay, and distortion [58]. And some consider that information sharing is an activity and visibility is the outcome [59]. There also is someone combining them and defining transparency as the ability to see from one end of the supply chain to the other [60]. In this study, transparency is taken as an outcome, i.e., visibility. Furthermore, traceability as the ability to track and trace information could create transparency in the supply chain [57].
With the sustained development of society and the growth of consumers’ demands, people attach much importance to the standard, origin, ways of production, and so on of their commodities. However, as the supply chain gets longer and more complex, the procedure before the product reaches the final user becomes more cumbersome, and the potential for problems is greatly increased. Blockchain could be a very suitable and important way to provide traceability data to consumers and make the supply chain more transparent [61]. Blockchain, as a distributed ledger and the way it stores digital data records, could make every participant in the network visit and view records, and at the same time, security could be promised without the necessity of a centralized certification organism. Salah et al., argued that today’s agricultural supply chain circumstance is very complex with multi-stakeholders, so it is hard to verify whether the product quality is in the line with the standard, e.g., stage of crop growth and country of origin as well as supervision implementation. They introduced blockchain technology to get rid of intermediaries in the soybean supply chain. They utilize the smart contract on the public Ethereum blockchain platform to realize interaction and the event trigger enabling participants could keep monitoring, tracing, and receiving alerts when breaches occur [62]. Thus, it can give a hand to restore the condition of the food supply chain after a violation happens. In addition, the improvement of transparency not only gives companies more opportunities to compete in the supply chain, but also builds trust among customers about the products [63]. This increased trust may lead to higher customer satisfaction and a greater willingness to pay [64].

4.1.1. Relevance to Normal Food Supply Chain

Food pollution is one of the most serious challenges that the food supply chain is confronted with, and what primarily leads to it is the leak of traceability and low transparency, which provides an opportunity for some people with bad intentions that uses food from improper sources or handles food not meeting the standard to maximize profits [65]. Once food pollution is found in the supply chain, members can trace it back immediately and find the source of contamination to handle it in time through blockchain technology. In 2011, the Food Safety Modernization Act was published, and the Food and Drug Administration of the United States needed to be able to fully recall and trace high-risk products [66]. The products recall costs a lot for companies. According to statistics, only recall would cost nearly 10 million dollars for food companies, in addition to which it also includes litigation cost, sales loss, company value loss or brand discredit [67]. In the study of Casey and Wong, they have mentioned the accident that Escherichia coli had outbroken at Chipotle Mexican Grill in 2015 [68]. Attributing to the complexity of the supply chain, the company was hard to carry out surveillance of its suppliers as there was a serious lack of transparency and accountability, which led to this accident.

Pairing blockchain technology with Internet of Things (IoT) devices, such as Radio Frequency Identification (RFID) technology, could track, analyze, identify and eliminate counterfeit products, and prevent quality issues, especially in the food supply chain. Figorilli et al., combine RFID technology, open-source technology, and blockchain technology to trace the standing tree to the final product in the supply chain [69]. There are also blockchain-based systems combined with unmanned aerial vehicles and RFID technology for traceability [70]. The proposed framework by Arena et al. [71] allowed the collection and validation of data from all the different stages of production provided by users or sensors to track the entire production process of the Extra Virgin Olive Oil.

In 2017, Blockchain technology is still a newly emerging technology and its application is still in its infancy. At that time, blockchain traceability systems were still in a centralized stage. And in the research of Tian, a conceptual architecture for a traceability system was proposed in response to the issue of food safety and the nature of blockchain technology [18]. This provided ideas at the time for the application of blockchain technology in the direction of food supply chain traceability.
Lin et al. [19] argued that the participants in the supply chain may not have a direct relationship, in which case the data request faces a trust transfer problem. Then, a food safety traceability system was proposed. Unlike most of the previous blockchain-based traceability systems which have not been fully implemented or exploited, they proposed a prototype system. The system design and analysis are given in their work. This system consists of an enterprise-user server and a consumer traceability client. The former is responsible for the acquisition and management of traceability information, and the latter can query traceability data, both of which contain blockchain modules. The blockchain module in the enterprise-user server includes two functions: one is to upload key traceability information on the chain, and the other is to give users the choice of whether to participate in blockchain maintenance or not, to become a full blockchain node or a lightweight blockchain node. The blockchain module of the consumer client can use lightweight nodes to enable consumers to request access to information on the chain and verify the legitimacy of the information. The downside is that there are no details on smart contract algorithms.

To solve the problems of low efficiency and low reliability of traditional traceability solutions for the food supply chain, Casino et al. [20] used a smart contract and table of content (ToC). Supply chain members store information about key product characteristics in the table of contents, which is stored locally, and blockchain only stores the hash of the ToC. It avoids storing a bunch of data in a blockchain, and therefore transactions would be faster due to the small amount of data. In addition, traceability would be easier as the only information needed to track the product is the corresponding TOC from each FSC member. But the model can only handle relatively simple food supply chain networks.

For the complex supply chain, a framework that combines blockchain and IoT technology to achieve traceability was proposed by Zhang et al. [21] They improved the identification method and introduced a trusted identification mechanism. In their proposed trusted identification mechanism, an identifier is generated for each product which is comprised of a prefix and a suffix, and the identifier would be verified and standardized by the smart contract which makes the process trustworthy. Essentially, the method of trusted identification is to generate a code and use a smart contract to verify it achieving secure and reliable data information for traceability.

Different from improving identification mechanisms, Wang et al. [22] gave thought about combing blockchain technology and RFID technology. In the though, the RFID reader in the system not only has the basic functions of a normal one, but also contains a blockchain layer. It could determine whether the tag is blockchain-enabled and decides what information should be written on the tag after encryption. Moreover, the RFID reader also includes a cryptographic module that calculates the hash value of the input information. Finally, the RFID reader sends the information written by the reader to the back-end blockchain platform. The designed RFID tag also contains a blockchain data structure. When the product is packaged, all relevant information is encoded by a hashing algorithm to form a genesis block. When the reader reads the tag, the information is recorded and formed into blocks. The blocks form a chain that is stored in the tag. In this way, all the information required by the user is stored and the authenticity of the information is guaranteed. The idea is innovative and, although it is still in the experimental phase, it provides a new idea for a traceability system.

4.1.2. Relevance to Perishable and Fresh Food Supply Chain

For perishable and fresh food, shelf life is relatively short, and consumers and participants in the food supply chain rely on the information of their life cycle heavily. Especially, with the rise of e-commerce, when a consumer purchases these kinds of commodities on the platform, it is hard to touch or feel their quality, in other words, it is difficult to obtain the condition of the food that he has bought. In addition, perishable and fresh food is more sensitive to the environment, so changes in food quality could happen always and anywhere, which makes complete traceability information and food data so important for ensuring the quality of food at delivery. The existing food traceability system has low
reliability, weak scalability, and poor information accuracy, and traceability processes in modern supply chain networks are time-consuming as well as complex.

Casino et al. [23] conducted a specific case study on food traceability in the context of a dairy company using three kinds of smart contracts to realize traceability. Giuseppe et al. [24] taking the Fontina PDO cheese supply chain as the scenario proposed a traceability system based on Algorand Blockchain and conducted testing and validation of the developed platform. They used the Pure Proof-of-Stake mechanism of consensus so that minimal computational power, highly scalable and environmentally sustainable could be reached.

Tsang et al. [25] believed that most blockchain consensus mechanisms are designed for cryptocurrencies and not in a retrospective context. In the proposed traceability system, traditional Proof of Work (PoW) is replaced by Proof of Supply Chain Share (PoSCS) which mimics Proof of Stake (PoS). Depending on the food traceability scenario, PoSCS would allow stakeholders in the food supply chain, rather than miners, to mint or forge blocks. The responsibilities and shares of the supply chain parties are aggregated into a standardized supply chain share to determine the creator of the new block. In addition, the logistic activity from raw material to the final consumer would be divided into multiple units to form traceable resource units combining IoT technology. All the collected data would be uploaded and managed in a cloud database while the traceability-associated IDs with a timestamp are forged in the blockchain for traceability purposes.

4.1.3. Relevance to Other Supply Chain

As shown from the statistics of previous papers, the subject of the food supply chain accounts for a large part of the supply chain field. So, in this part, the work explores the papers in other supply chain fields. There are various blockchain-based traceability methods have emerged in this part.

Omar et al. [26] used smart contracts to design a generic framework with three different types of smart contracts to address the difficulty of accurately tracking anti-epidemic supplies during COVID-19. For effective product tracking in the healthcare supply chain and to prevent the emergence of Counterfeit drugs, Musamih et al. [27] proposed an Ethereum blockchain-based approach. Smart contracts ensured the provenance of data, eliminated the need for intermediaries, and provide a secure, immutable transaction history for all stakeholders. The study presented the system architecture and the details of algorithms. In the end, the system was tested and validated to assess its effectiveness in improving traceability within the healthcare supply chain. Ahmed et al. [28] proposed a method to assess the data quality of IoT data sources. In the work, they made a standard for IoT data quality measurement and integrated the standard into traceability smart contracts. The research provides possibilities for the development of automated logistics traceability systems.

In the framework proposed by Lou et al. [6], a bidding mechanism was introduced to ensure transparency of information between entities in the supply chain. For the members, If the manufacturer needs a batch of raw materials, he would call the bidding function of the smart contract to inform the suppliers. A raw material demand order signed with the producer’s private key is created. The event then triggers the smart contract to allow all participants to bid. The ‘Tender’ function can send bid prices before the bid deadline, where the attribute ‘eprice’ refers to the bid price encrypted with the producer’s public key. After the deadline, the manufacturer can decrypt to view each bid price, and call the function to select the winning bidder. After receiving the goods, once the user finds a fake, he could scan its RFID tag and send the data stored in the RFID as parameters to the function ‘TraceGoods’. Hence, users can track not only the producers of the fakes, but also the suppliers who provide the raw materials for the fakes. The operation would trigger a smart contract to query transactions in the blockchain, and then returns the results to the user. And all the details related to the goods can be tracked at any time, which helps to resolve claims and reduce disputes related to precast constructions.

In the same thought, in paper [19], Wang et al. [29] argued that the nodes in a blockchain network were untrustworthy of each other. Therefore, it is very important to ensure effective
transactions between them. In the proposed traceability system, an event response mechanism for KYC (know your customer) verification was designed. Nodes could determine the validity of an event by verifying the signature contained in the event and deciding whether to continue trading with each other. All events could be monitored and stored permanently in the blockchain, and all events were stored permanently in the form of logs that served as a basis for handling disputes and tracking the responsible entities. Finally, the work carried out the assessment of deployment costs and security analysis.

With the globalization of the economy and the development of the Internet, cross-border e-commerce has grown rapidly in recent years. Liu et al. [30] proposed a traceability framework in the context of cross-border e-commerce. The multi-chain structure was used for data management, where data was divided into three categories based on type: transaction data, account data, and IoT data. And then the same type of data is stored in the same chain. Moreover, unlike traditional traceability labels, the proposed traceability label was logically linked to the product. When a product was traded, the change of ownership of its traceability label was also recorded in the block. Although the research background would be a little different, the idea of this work has something in common with paper [22].

4.2. Trade Behavior

In this section, the work focus on the improvement of trade behavior brought by blockchain technology. For example, blockchain technology boosts real-time information sharing and improves the quality of the information which would advance the coordination between supply chain participants; for special products, real-time monitoring could control the environment when needed, which saves cost. This work divides this whole section into four parts which are ‘Efficiency Improvement’, ‘Storage Optimization’, ‘Cost Saving’, and ‘Secure Trade’.

4.2.1. Efficiency Improvement

Blockchain technology could get rid of intermediates in the supply chain because it is able to reach information sharing among supply chain members, which builds trust among members and eliminates the necessity of middleman auditors. Thus, it would lead to the reduction of the tiers in the supply chain, reduce business waste, save trade costs and time, and improve trade performance [72]. Information sharing could accelerate the data flow between parties and enhance the efficiency of the entire supply chain. However, leak of real-time information sharing often creates fragmentation and discontinuity among the operations of supply chain members.

Wang et al. [31] taking precast construction as background proposed a blockchain-based framework for information management. Due to the characteristics of precast construction, it largely depends on the intensive coordination between up and down participants in the supply chain, so information sharing is quite significant. In the proposed framework, when the product is produced, the manufacturer will send shipping suggestions to other peer nodes through the client. Other nodes check the proposal and simulate the transaction after receiving it and send back their response to the proposal along with their signature. Through transaction simulation, other nodes will estimate the delivery of products and perform their own operations. Then real-time PC information and attribute values could be obtained by calling the ‘queryPC’ function of the ‘invoke’ function. The model could prevent the fragmentation and discontinuity of contiguous members well, improving efficiency and security. When the information is updated, it can be quickly shared through the blockchain, so that the product can be quickly deployed, the transaction speed can be accelerated, and mistakes can be reduced [68].

There are also cases where supply chain members are unwilling to share and the shared information is only beneficial to themselves, which leads to information asymmetry among supply chain members. This would lead to inefficiency in supply chain management. A blockchain-enabled data-sharing marketplace was designed and implemented by Wang et al. [32] through the Hashgraph platform. It is equipped with a novel usage-
based data valuation and pricing mechanism to facilitate data sharing in the supply chain. Mao et al. [33] proposed a credit evaluation system based on blockchain technology using a smart contract to control the reliability of information for regulators to enhance the efficiency of supervision and management in the food supply chain. Using the Hyperledger blockchain as the framework, they divide the nodes into regulator nodes, which are the main regulators, and trader nodes, which are mainly supply chain members. In addition to generating blocks, trader nodes are also mainly responsible for the credit evaluation of transactions. The regulator nodes are in charge of monitoring the transaction, the trader, and maintaining the records of traders. After the trader node evaluates the transaction through the smart contract, the system would collect the transaction and evaluation information, then analyze and process the evaluation information through the trained LSTM model, a deep learning network named Long-Short-Term Memory, and finally feeds the generated results back to the regulatory agency to supervise and manage the entire supply chain.

The consensus algorithm is a key part of blockchain technology, but at the same time, the consensus algorithm also affects its efficiency.

In the architecture proposed by Mondal et al. [34], they improve the conventional consensus mechanism PoW (proof of work) to PoO (proof of object). The modified consensus mechanism is based on the physical object concept not existing in cryptocurrency. If a node claims that he possesses a product or component, he should prove it in a cryptograph way and other nodes would verify his claim. This consensus algorithm has two advantages, one is to lower the cost, and the other is more suitable for food supply chain circumstances. Furthermore, the work also takes sensitive information into account.

Rana et al. [35] presented a model for using blockchain technology to improve the performance of the supply chain ecosystem. In the proposed model, a proof of authority consensus algorithm was used, and only pre-selected validator nodes would be required to validate transactions, which significantly reduced algorithm time improving efficiency and providing ideas for improving the performance of supply chain ecosystems.

Wang et al. [36] developed a blockchain-based model for rice supply chain information regulation, improving the PBFT algorithm into a practical Byzantine fault-tolerant consensus algorithm based on credit scoring. This mechanism effectively reduces the latency of complex data interactions in the rice supply chain and greatly reduces the cost of data storage. And by applying blockchain technology at a grain and oil company in Changde, Hunan, China, the information-based regulatory process of the rice supply chain regulator has been optimized, providing a viable solution for grain and oil quality and safety regulation. Meanwhile, Peng et al. [37] designed a concurrency mechanism based on the K-means algorithm and Bloom filter. A Supervision Practical Byzantine Fault Tolerance (SPBFT) consensus mechanism based on the PBFT consensus mechanism was designed. These mechanisms effectively reduce the latency of complex data interactions in the rice supply chain and greatly reduce the cost of data storage.

4.2.2. Storage Optimization

The blockchain is not suitable for storing a large number of records, and the processing efficiency of the blockchain will be improved if the storage problem could be solved.

Zafar et al. [38] implemented a permissioned blockchain-based framework for the secure and efficient supply chain management. From the evaluation, a small extra data memory was used to store a huge amount of the automotive data of users. In the system proposed by Kawaguchi [39], each file has a cryptographic hash. Each network node only stores content and some indexing information that helps determine where the data is stored. Participants can use InterPlanetary File System (IPFS) to process large amounts of data and put immutable, permanent IPFS links into blockchain transactions. This timestamps and protects their content without having to put the data on the chain.

In paper [19], they considered the data explosion of the traceability system during system design, so they used the on-chain & off-chain model to solve it. However, they neglected the information clipping function. Once the lifecycle is exceeded, the information
of the corresponding product would become invalid and take up memory, increasing the burden.

Fran Casino at el. [20] also used the on-chain and off-chain storage. Upstream data, that is, data about product production, is stored in a central server, and IoT technology stores information about product key characteristics in the TOC, and uses distributed storage methods such as IPFS.

Taking household electronic appliances as background, the system introduced by Xie et al. [40] stores the production data information required for traceability in the local data server of each organization node, and each character of the information will be spliced as a string. Considering the storage space problem, the MD5 algorithm of shorter bit length is selected for encryption. The resulting hash value is written to the blockchain. When a query is required, the same algorithm is used to calculate the information in the local database and compare it with the hash value in the blockchain for verification.

Zhang et al. [21] designed a master-slave multi-chain architecture, where the master chain is responsible for the query function and the slave chain is used to store the data. The database is connected to the blockchain network and the uploaded data is broadcast on the blockchain network of the slave chains. The data that passes the node validation will be uploaded and the master chain will then store the corresponding hash and product number. But it still doesn’t address the fundamental problem of data explosion, which is the deletion of invalid data. If it just simply lowers the size of the stored information, it would also face the storage problem.

Continuously real-time food data recorded in the blockchain could put pressure on the storage and computing power of the system. As a result, the concept of blockchain vaporization was proposed by Tsang et al. [25]. In the way of a lightweight blockchain to be associated with cloud computing to support IoT monitoring, after the life cycle of a batch of food is over, the blockchain used to trace this batch of food would upload the data to the cloud database and be deleted. In this way, the data in the blockchain would be finally deleted and the problem would be solved essentially. However, the work is based on a food supply chain where products have a life cycle and the data on expired food could be deleted. How to apply it to other supply chain fields needs to be studied.

4.2.3. Cost Saving

Special goods, such as fresh food and pharmaceutical items, need to be managed in real-time, thus environmental variables such as temperature and humidity could be adjusted in time to ensure the integrity of the goods. The cold chain supply chain has special demands on the physical environment, such as temperature, humidity, pressure, etc. IoT and blockchain technology could better control fleets to provide the physical environment needed for perishable food or biopharmaceutical products. Environmental conditions could also be set through smart contracts, and changes in the environment can be reported through sensors for real-time monitoring and adjustment [41].

In Good Distribution Practice, it is required to demonstrate that transport conditions, especially temperature, do not affect the quality of the medicines being transported [73]. Pharmaceutical companies could meet GDP requirements with the help of blockchain technology. At the same time, significant cost savings could be achieved for the transport of pharmaceuticals that do not require active cooling [74]. IBM connects all parties in the vaccine cold chain through the Hyperledger Fabric blockchain, including manufacturers, public health trustee organizations and authorities, as well as audit and regulatory organizations, so that there is immediate access to the location, status, and conditions of vaccine preparation and distribution [42].

4.2.4. Secure Trade

In addition, the smart contract in blockchain technology could automatically execute the transaction. Once the smart contract meets the corresponding conditions, such as the supplier’s goods reaching the delivery conditions, the contract would automatically
issue the payment after delivery, which improves efficiency. It also prevents fraudulent transactions. For example, in conventional supply chains’ financing, supplier trade credit is the main part. As a result, bargaining power directly affects loan growth, and weaker suppliers would be forced to extend payment terms or delay repayments, which will increase risk and disruption within the SC. This paper proposed a blockchain-driven supply chain finance platform BCautoSCF. By using smart contracts, it could program the transaction steps of the loan agreement between the financier and the supplier. It acts as a payment trigger when goods are delivered, and in this way, increases transaction speed while reducing transaction costs and minimizing human error and disruption in contract execution.

And Yakubu [43] used smart contracts to achieve secure trade. There are four algorithms in the designed framework. In the seed purchase stage, farmers purchase seeds from suppliers through smart contracts. Every seed product sold by the supplier is identified using a standardized identifier, such as a serialized Global Trade Identification Number (GTIN). Farmers, grow crops and deploy smart contracts with unified identification of seed traceability. Farmers are also responsible for regularly monitoring and recording crop development information and storing it in an encrypted, decentralized, tamper-proof ledger. And then, the elevator could sell to the producer. The producer sells the final product to the distributor. In the third phase, the smart contract guarantees that only registered retailers can buy goods. Likewise, it verifies that sales negotiations have been approved and that payment has been made. In the last stage the retailer sells the product to the consumer, only the products of the registered retailers are shown to the consumer, and then it is verified that payment has been negotiated. A successful sale is a success. Each rice product is accompanied by its STI and GTIN for proper traceability and identification. As a result, secure trade could make the supply chain more efficient.

In the credit scheme proposed by Patel et al. [44], the raw material provider would supply the farmer with the raw material on credit as the farmer would not pay the provider in advance, but the farmer must set aside an amount in his wallet to pay the provider to complete the payment later. If the money set aside is not enough, then the order cannot be placed. When the deadline is reached or the farmer sells the crop, a fee is paid. The whole process is carried out via smart contracts, so the money set aside is paid automatically even if the crop is not sold. And if payment is made before the deadline, then the farmer can use the available reserve funds again to buy the raw material. A certain amount of interest will be calculated on the funds set aside for the transaction. The interest amount will be given to the raw material merchant. Thus, it is a win-win situation for both stakeholders. The approach provides legal protection by meeting the social need to protect workers and the environment, while preventing the misuse of the product.

4.3. Data Security and Access Control

With the rapid development of globalization and the internet, cross-domain e-commerce has emerged, and the global supply chain is getting more and more significant and complex. In the supply chain, information sharing would yield ‘twice the result with half the effort’, increasing productivity while reducing costs. Blockchain technology could ensure the reliability and security of the data. Once some transaction or data reaches the consensus and is recorded on the blockchain, it is difficult to change or delete [75]. In the blockchain, if some data needs to be changed or deleted, it can only be done after the nodes reach a consensus. But it is impossible to change or delete data without operation records [61]. For example, authentication and certification of the commodities in the luxury supply chain feature prominently for consumers. Also, it is the most critical part of the luxury supply chain. The conventional certificate may be forged or used to authenticate the fake one. Nowadays, there are platforms like Everledger that provides unique digital fingerprints for high-value and hard-to-substitute commodities. Such fingerprints are generated by blockchain technology and stored in the blockchain with immutability.
In such a complicated situation, trade and distribution need more collaboration among supply chain participants. However, every member should be careful about protecting their privacy or personal information while having transactions or information sharing with others.

4.3.1. Security within IoT Devices

The rise of the IoT technology has extended its engagement to various industries as well as the area of the supply chain. There are a lot of IoT devices in the supply chain. The actions of the devices are verified and allowed through the settings of smart contracts. Any message having no relationship with the settings would not trigger the functions of the smart contracts, which could increase the security of the IoT platform. Transactions between IoT devices could also be protected and authenticated with cryptography technology to ensure that the sender of the message is not malware or an external intermediary [76]. Unfortunately, there is also the possibility of leakage of private data when IoT devices obtain product data [77]. Data privacy and security issues often arise during the application of this technology [78,79].

In 2017, Ouaddah et al. [45] proposed a blockchain-based model for the implementation of IoT devices. In the paper, using the blockchain framework, they set the access token which is a digital signature as the transaction and leverage the consensus mechanism to reach consistency in solving the decentralized access control problem without a centralized party.

A lightweight trust model based on blockchain technology was introduced by Al-Rakhami [46]. This model contains three key modules, data module, IoT network, supply chain, and blockchain system. Each node obtains a score through the trust score formula, and the trust score of each node can be checked. Interaction is only possible if the trust value of both nodes exceeds a given threshold. The trust value is the value obtained by summing the number of transactions of the node, multiplying the evaluation value of the node during the n transactions, and dividing by the number of transactions. The trust value of a node will give corresponding reward and punishment measures to ensure the security of information sharing.

4.3.2. Security in Medical Field

For some special industries, e.g., healthcare and the medical field, private data is generated all the time. In addition, medical and healthcare institutions hold a great amount of personal data, which should be kept carefully. Therefore, the medical-related supply chain is a big part of privacy-preserving. In recent years, several cases of cyber-attacks are about medical supply chain networks resulting in the weakness of security. If personal data is attacked, the consequences will be unimaginable.

Focusing on the feature of the medical supply chain, privacy data like personal information related to patients and their medical history is generated and transmitted unceasingly in the supply chain network. Hence this situation would place patients' information data at great risk of leakage.

Therefore, Azzaoui et al. [47] proposed a Blockchain-Based Distributed Information Hiding Framework. In this framework, they improved steganography that could encrypt desired information with another form of data, auxiliary text messages, to hide and protect them. By means of blockchain technology, pre-authenticated and honest nodes could select members who want to join the supply chain network through Practical Byzantine Fault Tolerance, which, to a great extent, can eliminate the emergence of malicious nodes in the network. Only the node that has reached the consensus could participate in the communication. The smart contract will change the secret key every time a new communication is initiated as a one-time hash, and, as a result, the risk of data leakage could be low even if a cyber attacker possesses the key to some information, enhancing the security and privacy of critical systems. To prevent huge losses caused by personal information leakage in the medical supply chain.
4.3.3. Sub-Blockchain Network

In the proposed drug supply chain system proposed by Jamil et al. [48], they introduce subnet which divides the entire network into private networks. In each private network, relevant departments can share confidential data directly with each other without exposing it to other departments, and that narrows the range of information sharing directly. Every department is allowed to build its network in the system, and they form the entire network of a hospital. If there is a need for cross-department data sharing, sub-networks could be formed between departments to achieve secure data sharing.

A blockchain system for controlled shared transactions of massive data is proposed by Si [49]. The system divides the blockchain module into two parts, consortium chain, and private chain. The consortium chain module is responsible for transactions and mainly stores transaction information, and the private chain module is responsible for data storage and mainly stores data files. The federated chain is composed of organizations, and private chains are used within the organizations. The private chain uses internal LAN for communication and is isolated from the outside to ensure the security of data.

The proposed framework by Agrawal et al. [50] also subdivides the blockchain network for data partitioning to form channels. Each channel is used for different types of transactions, while also ensuring data privacy. In the proposed framework, Agrawal et al. [51] deployed smart contracts over each channel to set rules and ensure the completion of transactions. In the paper, the smart contract was used for data collection and verification of sensor readings. They built a demonstrator that identifies the information sharing structure that is needed for the smart contracts to function. In addition, they considered the preferences of partners for customised networks and set appropriate smart contract rules which provided the dual benefit of supporting different interests while operating in a blockchain network that ensured solidarity and collaboration.

4.3.4. Access Control

In 2017, Chen et al. [52] took the laptop supply chain as the study background. For preventing classified data leakage, the smart contract was used to carry out data access control. Song et al. [53] argued the approach of making the subnet is essentially the same as creating a new blockchain service, which wastes resources. Hence, they used the method of access control to handle data spread in a small range. In the work, each company maintains a node and has a public key table for the node. This table stores the public keys of other accessible nodes. The node can access the information of nodes included in the public key table. Asymmetric encryption is used for private data storage and transmission. When transferring private data, the data is encrypted with the local private key. When delivered to the destination, the corresponding peer decrypts the data using the public key.

Wen et al. [54] introduced a blockchain-based supply chain system. In this system, if a member wants to join the blockchain network, he needs the signature of the upper layer. For example, the master node of each member in the supply chain such as a supplier or manufacturer or operator, or retailer can register to the channel by providing attributes and the principal’s signature. If a supplier wants to deploy nodes for sensors within its own company, it needs to provide signatures for nodes. According to the access policy deployed by the administrator, the nodes that meet the policy can download data from the blockchain network to the specified cloud storage or local storage to achieve data security.

Bader et al. [55] presented PrivAccIChain (privacy chain), resorting to hybrid encryption to ensure the security and privacy of data, and provide fine-grained access control to collaborators in the supply chain. The method is based on symmetric encryption for encrypting the payload as well as ciphertext-policy attribute-based encryption. In their proposed data access policy, supply chain members can improve the collusion resistance of their data records by defining a combination of attributes. They can also use the consult access control list manager to determine which attributes are best for use in its access policies, to achieve data security and privacy.
5. Discussion

Blockchain technology has received increasing attention as a potentially disruptive technology that incorporates the characteristics of a decentralized ‘trustless’ database. Through continuous exploration as well as research in the supply chain field, blockchain technology is making progress from both academic and practical perspectives. To answer the research question in this paper and to better understand the future development of blockchain, this work has attempted to fill existing knowledge gaps on blockchain applications and future research work through the findings of the literature review.

5.1. Traceability and Transparency

Due to the increasing complexity of supply chains, transparency and traceability are issues that need to be addressed urgently. With blockchain technology, issues such as centralization, transaction interchange, and food pollution can be addressed. From the study, there are lots of papers between 2017–2022. In the beginning, the study could just give the conceptual framework for traceability.

With the integration of blockchain with emerging technologies such as the Internet of Things and advanced sensing technologies, By optimizing product identification methods and mechanisms, the uploading of product data becomes secure and fast, which also improves the real-time monitoring of logistics activities [21–23,30]. With the increased transparency and traceability of the supply chain through blockchain technology, consumers will be more willing to buy in some supply chains, such as food, and since the details of the transactions are transparent and traceable, the responsible parties can be quickly identified and unnecessary disputes can be avoided.

In addition, there are many studies based on smart contracts [6,26–28]. Through the feature of smart contracts, different data can continue to be categorized and managed, and high-quality data can be obtained by selecting based on criteria when data is collected.

From the current research, it can be found that supply chain traceability systems based on blockchain technology are becoming more and more automated. The integration of data identification technology with blockchain technology will allow for less human involvement and reduce the probability of human error. Smart contracts, on the other hand, can facilitate the automation of processes and also set conditions as well as criteria in them as needed. The combination of these two will allow for the automation of traceability systems, which could be the direction of future research into traceability systems.

5.2. Trade Behavior

Blockchain technology can also improve the trading performance of the supply chain. At first, the blockchain consensus algorithm was proposed for cryptocurrency. Although its security is very high, its requirement for computing power will make the cost soar, so it is not suitable for the supply chain environment. According to the improved consensus algorithm of the supply chain background, the calculation is simplified while the cost is reduced, and the efficiency of the whole supply chain is improved [34–37].

With the help of blockchain, members who are unwilling to share information have to share information [32,68]. After that, real-time information sharing can control the temperature and humidity of special products, such as medicines and fresh food, to avoid damage and reduce costs.

However, it is important to note that blockchains are not suitable for storage, so any issues regarding data explosion can cause a reduction in blockchain processing power. In Section 4.2.2, a number of options are proposed, the most common method is using on-chain & off-chain storage, by simplifying the data for on-chain storage, while the original data is stored locally. But fundamentally, the data will accumulate and if it cannot be cleaned up, eventually the blockchain will still face storing pressure. The idea of paper [25] is therefore innovative, but there are limitations, as the data associated with expired food is invalid that can be deleted. Thus, it is uncertain whether this can be used in other supply chain fields.
The blockchain’s improvement of trade behavior is in most cases an adjunct. However, the consensus algorithm and storage aspects need to be studied separately. Different consensus algorithms may be suitable for different supply chain environments, and the improvement of algorithms can lead to lower costs and higher efficiency at the same time. The storage problem is still mostly researched through the on-chain & off-chain approach, with the specific difference being how to simplify the data to be on the chain. The gap in research currently lies in how to clean up the data in the blockchain, as the process of cleaning up is also recorded, which may be even bigger than the data that is deleted. The blockchain’s improvement of trade behavior is in most cases an adjunct. However, the consensus algorithm and storage aspects need to be studied separately. Different consensus algorithms may be suitable for different supply chain environments, and the improvement of algorithms can lead to lower costs and higher efficiency at the same time. The storage problem is still mostly researched through the on-chain & off-chain approach, with the specific difference being how to simplify the data to be on the chain. The gap in research currently lies in how to clean up the data in the blockchain, as the process of cleaning up is also recorded, which may be even bigger than the data that is deleted.

5.3. Data Security and Access Control

When blockchain technology continuously improves the transparency of the supply chain, data security issues will also arise. In the traceability system, when a large number of IoT devices are deployed, data leakage may occur, and the relevant scoring mechanism is proposed accordingly. Paper [48–51] makes different transactions by establishing channels to ensure that the data will not be leaked to the outside. However, this method is similar to building a new blockchain, which requires a lot of costs, so the implementation of the idea is doubtful. Most of the existing access control methods depend on the nature of the smart contract and encryption algorithm. According to the application scenario, it is a feasible and effective method to realize access control by setting a smart contract.

6. Conclusions

This article aims to present a systematic review and analysis of the literature about blockchain-based applications within the supply chain. It contains the latest related articles that can be downloaded. Blockchain technology has been widely used in supply chains to solve some problems of traditional supply chains, such as information blockage, low operational efficiency, fraudulent behavior, and privacy leakage. At the same time, with the development of IoT technology, the combination of the two technologies has promoted the birth of more applications in the supply chain. This paper analyzes the existing related research from three perspectives of data security and access control, traceability and transparency, and transaction performance.

Here are some views for future research directions. When blockchain technology is taken as a distributed database, it needs the development of other technology to realize innovation. Moreover, how to solve the storage problem still needs to study. Today’s supply chains are moving towards environmentally-friendly and sustainability, so the consensus algorithms need to be more efficient with less computing consumption.

However, there are limitations in our work. The papers we studied are all from the Web of Science database, which may have missed some high-quality articles in other databases. For the papers in 2021 and 2022, we have not set the screening criteria, so there may be low-quality articles included.

Author Contributions: B.L. reviewed literature, designed this study, and prepared the original manuscript; X.S. organized the study and made some suggestions for the first manuscript; H.K. supported this study and provided some suggestions for the first manuscript. All authors have read and agreed to the published version of the manuscript.
**Funding:** This work was granted by Qin Xin Talents Cultivation Program, Beijing Information Science & Technology University (No. QXTCP C202115), and the Beijing Municipal Education Commission Applied Basic Research Project (No. KM202011232022).

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

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

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

**References**

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: http://www.Bitcoin.org/bitcoin.pdf (accessed on 16 October 2022).

2. Aggarwal, S. Blockchain 2.0: Smart contracts. *Adv. Comput.* 2021, 121, 301–322.

3. Maesa, D.D.F. Blockchain 3.0 applications survey. *J. Parallel. Distr. Com.* 2020, 138, 99–114. [CrossRef]

4. Wan, P.K.; Huang, L.; Holtskog, H. Blockchain-enabled information sharing within a supply chain: A systematic literature review. *IEEE Access* 2020, 8, 49645–49656. [CrossRef]

5. Tejpal, G.; Garg, R.; Sachdeva, A. Trust among supply chain partners: A review. *Meas. Bus. Excell.* 2013, 17, 51–71. [CrossRef]

6. Lou, M.; Dong, X.; Cao, Z.; Shen, J. SESCIF: A secure and efficient supply chain framework via blockchain-based smart contracts. *Secur. Commun. Netw.* 2021, 2021, 8884478. [CrossRef]

7. Dolgui, A.; Ivanov, D. 5G in Digital supply chain and operations management: Fostering flexibility, end-to-end connectivity and real-time visibility through internet-of-everything. *Int. J. Prod. Res.* 2022, 60, 442–451. [CrossRef]

8. Yu, M.C.; Goh, M. A multi-objective approach to supply chain visibility and risk. *Eur. J. Oper. Res.* 2014, 233, 125–130. [CrossRef]

9. Chang, S.E.; Chen, Y. When blockchain meets supply chain: A systematic literature review on current development and potential applications. *IEEE Access* 2020, 8, 62478–62494. [CrossRef]

10. Sheth, H.; Dattani, J. Overview of blockchain technology. *Asian J. Converg. Technol. (AJCT)* 2021, 1–3. [CrossRef]

11. Kuo, T.T.; Kim, H.E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. *J. Am. Med. Inform. Assoc.* 2017, 24, 1211–1220. [CrossRef]

12. Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renew. Sustain. Energy Rev.* 2019, 100, 143–174. [CrossRef]

13. Xu, M.; Chen, X.; Kou, G. A systematic review of blockchain. *Financ. Innov.* 2019, 5, 1–14. [CrossRef]

14. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* 2019, 36, 55–81. [CrossRef]

15. Denyer, D.; Tranfield, D. Producing a systematic review. In *The Sage Handbook of Organizational Research Methods*; Sage Publications Ltd.: Thousand Oaks, CA, USA, 2009.

16. Kilibarda, M.; Andrejić, M.; Popović, V. Research in logistics service quality: A systematic literature review. *Transport* 2020, 35, 224–235.

17. Morashti, J.A.; An, Y.; Jang, H. A Systematic Literature Review of Sustainable Packaging in Supply Chain Management. *Sustainability* 2022, 14, 4921. [CrossRef]

18. 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, Wuhan, China, 14–16 January 2017; pp. 1–6.

19. Lin, Q.; Wang, H.; Pei, X.; Wang, J. Food safety traceability system based on blockchain and EPCIS. *IEEE Access* 2019, 7, 20698–20707. [CrossRef]

20. Casino, F.; Kanakaris, V.; Dasaklis, T.K.; Moschuris, S.; Rachaniotis, N.P. Modeling food supply chain traceability based on blockchain technology. *IFAC-PapersOnLine* 2019, 52, 2728–2733. [CrossRef]

21. Zhang, X.; Li, Y.; Peng, X.; Zhao, Z.; Han, J.; Xu, J. Information Traceability Model for the Grain and Oil Food Supply Chain Based on Trusted Identification and Trusted Blockchain. *Int. J. Environ. Res. Public Health* 2022, 19, 6594. [CrossRef]

22. Wang, L.; He, Y.; Wu, Z. Design of a Blockchain-Enabled Traceability System Framework for Food Supply Chains. *Foods* 2022, 11, 744. [CrossRef]

23. Casino, F.; Kanakaris, V.; Dasaklis, T.K.; Moschuris, S.; Rachaniotis, N.P. Blockchain-based food supply chain traceability: A case study in the dairy sector. *Int. J. Prod. Res.* 2021, 59, 5758–5770. [CrossRef]

24. Varavallo, G.; Caragnano, G.; Bertone, F.; Vernetti-Prot, L.; Terzo, O. Traceability Platform Based on Green Blockchain: An Application Case Study in Dairy Supply Chain. *Sustainability* 2022, 14, 3321. [CrossRef]

25. Tsang, Y.P.; Choy, K.L.; Wu, C.H.; Ho, G.T.S.; Lam, H.Y. Blockchain-driven IoT for food traceability with an integrated consensus mechanism. *IEEE Access* 2019, 7, 129000–129017. [CrossRef]

26. Omar, I.A.; Debe, M.; Jayaraman, R.; Salah, K.; Omar, M.; Arshad, J. Blockchain-based Supply Chain Traceability for COVID-19 personal protective equipment. *Comput. Ind. Eng.* 2022, 167, 107995. [CrossRef] [PubMed]

27. Musamih, A.; Salah, K.; Jayaraman, R.; Arshad, J.; Debe, M.; Al-Hammadi, Y.; Elahham, S. A blockchain-based approach for drug traceability in healthcare supply chain. *IEEE Access* 2021, 9, 9728–9743. [CrossRef]
28. Ahmed, M.; Taconet, C.; Ould, M.; Chabridon, S.; Bouzeghoub, A. IoT data qualification for a logistic chain traceability smart contract. Sensors 2021, 21, 2239. [CrossRef]

29. Wang, S.; Li, D.; Zhang, Y.; Chen, J. Smart contract-based product traceability system in the supply chain scenario. IEEE Access 2019, 7, 115122–115133. [CrossRef]

30. Liu, Z.; Li, Z. A blockchain-based framework of cross-border e-commerce supply chain. Int. J. Inf. Manag. 2020, 52, 102059. [CrossRef]

31. Wang, Z.; Wang, T.; Hu, H.; Gong, J.; Ren, X.; Xiao, Q. Blockchain-based framework for improving supply chain traceability and information sharing in precast construction. Autom. Constr. 2020, 111, 103063. [CrossRef]

32. Wang, Z.; Zheng, Z.; Jiang, W.; Tang, S. Blockchain-enabled data sharing in supply chains: Model, operationalization, and tutorial. Prod. Oper. Manag. 2021, 30, 1965–1985. [CrossRef]

33. Mao, D.; Wang, F.; Hao, Z.; 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]

34. Mondal, S.; Wijewardena, K.P.; Karuppuswami, S.; Kriti, N.; Kumar, D.; Chahal, P. Blockchain inspired RFID-based information architecture for food supply chain. IEEE Internet Things J. 2019, 6, 5803–5813. [CrossRef]

35. Rana, S.K.; Kim, H.C.; Pani, S.K.; Rana, A.K.; Aich, S. Blockchain-based Model to Improve the Performance of the Next-Generation Digital Supply Chain. Sustainability 2021, 13, 10008. [CrossRef]

36. Ouaddah, A.; Elkalam, A.A.; Ouahman, A.A. Towards a novel privacy-preserving access control model based on blockchain technology. PeerJ Comput. Sci. 2019, 5, 1–19. [CrossRef]

37. Peng, X.; Zhang, X.; Xu, J.; Wang, X.; Li, H.; Zhao, Z.; Kong, J. Blockchain-based information supervision model for rice supply chains. Comput. Intell. Neurosci. 2022, 2022, 2914571. [CrossRef]

38. Wang, J.; Zhang, X.; Xie, Z.; Wang, Y.; Li, H.; Zhao, Z.; Kong, J. Research on the Cross-Chain Model of Rice Supply Chain Supervision Based on Parallel Blockchain and Smart Contracts. Foods 2022, 11, 1269. [CrossRef]

39. Wanzhou, China, 14–16 May 2021; pp. 179–185. [CrossRef]

40. Fish, I.; Barnard, M. Saving money and lives with blockchain for coldchain breaks. IBM Healthcare & Life Sciences Industries Blog, 7 May 2018.

41. Xie, J.; Zhu, S.; Li, B. Research on data storage model of household electrical appliances supply chain traceability system based on blockchain. In Proceedings of the 2021 13th International Conference on Advanced Computational Intelligence (ICACI), Wanzhou, China, 14–16 May 2021; pp. 179–185.

42. Mackey, T.K.; Nayyar, G. A review of existing and emerging digital technologies to combat the global trade in fake medicines. Expert Opin. Drug Saf. 2017, 16, 587–602. [CrossRef]

43. El Azzaoui, A.; Chen, H.; Kim, S.H.; Pan, Y.; Park, J.H. Blockchain-Based Distributed Information Hiding Framework for Data Privacy Preserving in Medical Supply Chain Systems. Sensors 2022, 22, 1371. [CrossRef] [PubMed]

44. Elazzouzi, A.; Elkahlaoui, A.; Ouahman, A.A.; Al-Ahmadi, A.A.; Ullah, N. Towards a novel privacy-preserving access control model based on blockchain technology in IoT. Sensors 2021, 21, 7599. [CrossRef]

45. Jamil, F.; Hang, L.; Kim, K.; Kim, D. A novel medical blockchain model for drug supply chain integrity management in a smart hospital. Electronics 2019, 8, 505. [CrossRef]

46. Si, Y. Agricultural Cold Chain Logistics Mode Based on Multi-Mode Blockchain Data Model. Comput. Intell. Neurosci. 2022, 2022, 8060765. [CrossRef] [PubMed]

47. Agrawal, T.K.; Pal, R.; Wang, L.; Chen, Y. Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry. Comput. Ind. Eng. 2021, 154, 107130. [CrossRef]

48. Agrawal, T.K.; Angelis, J.; Khilji, W.A.; Kalaiaaras, R.; Viktorsson, M. Demonstration of a blockchain-based framework using smart contracts for supply chain collaboration. Int. J. Prod. Res. 2022, 1–20. [CrossRef]

49. Chen, S.; Shi, R.; Ren, Z.; Yan, J.; Shi, Y.; Zhang, J. A blockchain-based supply chain quality management framework. In Proceedings of the 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE), Shanghai, China, 4–6 November 2017; pp. 172–176.

50. Song, Q.; Chen, Y.; Zhong, Y.; Lan, K.; Fong, S.; Tang, R. A supply-chain system framework based on internet of things using Blockchain technology. ACM Trans. Internet Technol. (TOIT) 2021, 21, 1–24. [CrossRef]

51. Chen, S.; Shi, R.; Ren, Z.; Yan, J.; Shi, Y.; Zhang, J. A blockchain-based supply chain quality management framework. In Proceedings of the 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE), Shanghai, China, 4–6 November 2017; pp. 172–176.

52. Agrawal, T.K.; Pal, R.; Wang, L.; Chen, Y. Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry. Comput. Ind. Eng. 2021, 154, 107130. [CrossRef]

53. Agrawal, T.K.; Angelis, J.; Khilji, W.A.; Kalaiaaras, R.; Viktorsson, M. Demonstration of a blockchain-based framework using smart contracts for supply chain collaboration. Int. J. Prod. Res. 2022, 1–20. [CrossRef]

54. Chen, S.; Shi, R.; Ren, Z.; Yan, J.; Shi, Y.; Zhang, J. A blockchain-based supply chain quality management framework. In Proceedings of the 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE), Shanghai, China, 4–6 November 2017; pp. 172–176.

55. Song, Q.; Chen, Y.; Zhong, Y.; Lan, K.; Fong, S.; Tang, R. A supply-chain system framework based on internet of things using Blockchain technology. ACM Trans. Internet Technol. (TOIT) 2021, 21, 1–24. [CrossRef]
56. Pournader, M.; Shi, Y.; Seuring, S.; Kob, S.L. Blockchain applications in supply chains, transport and logistics: A systematic review of the literature. *Int. J. Prod. Res.* 2020, 58, 2063–2081. [CrossRef]

57. Sunny, J.; Undralla, N.; Pillai, V.M. Supply chain transparency through blockchain-based traceability: An overview with demonstration. *Comput. Ind. Eng.* 2020, 150, 106895. [CrossRef]

58. Hofstede, G.J.; Beulens, A.; Spaans, L. Transparency: Perceptions, practices and promises. In *The Emerging World of Chains and Networks, Bridging Theory and Practice*; Reed Business Information: Amsterdam, The Netherlands, 2004; pp. 285–310.

59. Holcomb, M.C.; Ponomarov, S.Y.; Manrodt, K.B. The relationship of supply chain visibility to firm performance. *Supply Chain Forum Int. J.* 2011, 12, 32–45. [CrossRef]

60. Zehbst, P.J.; Green, K.W.; Sower, V.E.; Bond, P.L. The impact of RFID, IIoT, and Blockchain technologies on supply chain transparency. *J. Manuf. Technol. Manag.* 2019, 31, 441–457. [CrossRef]

61. Bumblauskas, D.; Mann, A.; Dugan, B.; Rittmer, J. A blockchain use case in food distribution: Do you know where your food has been? *Int. J. Inf. Manag.* 2020, 52, 102008. [CrossRef]

62. Salah, K.; Nizamuddin, N.; Jayaraman, R.; Omar, M. Blockchain-based soybean traceability in agricultural supply chain. *IEEE Access* 2019, 7, 73295–73305. [CrossRef]

63. Roeck, D.; Sternberg, H.; Hofmann, E. Distributed ledger technology in supply chains: A transaction cost perspective. *Int. J. Prod. Res.* 2020, 58, 2124–2141. [CrossRef]

64. Petersen, M.; Hackius, N.; von See, B. Mapping the sea of opportunities: Blockchain in supply chain and logistics. *IT Inf. Technol.* 2018, 60, 263–271. [CrossRef]

65. Casey, M.J.; Wong, P. Global supply chains are about to get better, thanks to blockchain. *Harv. Bus. Rev.* 2017, 13, 1–6.

66. Cases i Torrent, D.; Ponzetto, S.; Valdés, J.L.; Lenzi, G.; Torra, V. European Union. Guidelines of 5 November 2013 on Good Distribution Practice of Medicinal Products for Human Use Text with EEA Relevance. 2013. p. 14. Available online: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:343:0001:0014:EN:PDF (accessed on 16 October 2022).

67. U.S. Food and Drug Administration: Food Safety Modernization Act (FSMA). 2018. Available online: https://www.fda.gov/food/guidance-regulation-food-and-dietary-supplements/food-safety-modernization-act-fsma (accessed on 16 October 2022).

68. Ward, T. Blockchain Could Help Us Save the Environment. Here’s How. 2017. Available online: https://futurism.com/blockchain-could-help-save-environment-heres-how (accessed on 16 October 2022).

69. Figorilli, S.; Antonucci, F.; Costa, C.; Pallottino, F.; Raso, L.; Castiglione, M.; Pinci, E.; Del Vecchio, D.; Colle, G.; Proto, A.R.; et al. A blockchain implementation prototype for the electronic open source traceability of wood along the whole supply chain. *Sensors* 2018, 18, 3133. [CrossRef]

70. Holcomb, M.C.; Ponomarov, S.Y.; Manrodt, K.B. The relationship of supply chain visibility to firm performance. *Supply Chain Forum Int. J.* 2011, 12, 32–45. [CrossRef]

71. Arena, A.; Bianchini, A.; Perazzo, P.; Vallati, C.; Dini, G. BRUSCHETTA: An IoT blockchain-based framework for certifying extra virgin olive oil supply chain. In *Proceedings of the 2019 IEEE International Conference on Smart Computing (SMARTCOMP)*, Washington, DC, USA, 12–15 June 2019; pp. 173–179.

72. Ward, T. Blockchain Could Help Us Save the Environment. Here’s How. 2017. Available online: https://futurism.com/blockchain-could-help-save-environment-heres-how (accessed on 16 October 2022).

73. European Union. Guidelines of 5 November 2013 on Good Distribution Practice of Medicinal Products for Human Use Text with EEA Relevance. 2013. p. 14. Available online: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:343:0001:0014:EN:PDF (accessed on 16 October 2022).

74. White Paper: Data Integrity for Supply Chain Operations Powered by Blockchain Technology. 2018. Available online: https://whitepaper.io/document/213/modum-whitepaper (accessed on 16 October 2022).

75. NBlockchain Beyond Bitcoin: How Blockchain Will Transform Business in 3–5 Years. 2017. Available online: https://www.inc.com/john-koetsier/how-blockchain-will-transform-business-in-3-to-5-years.html (accessed on 16 October 2022).

76. Kashyap, S.; Kshetri, N. Can blockchain strengthen the internet of things? *IT Prof.* 2017, 19, 68–72. [CrossRef]

77. Malik, N.; Alkhathib, K.; Sun, Y.; Knight, E.; Jararweh, Y. A comprehensive review of blockchain applications in industrial Internet of Things and supply chain systems. *Appl. Stoch. Model. Bus. Ind.* 2021, 37, 391–412. [CrossRef]

78. Tan, B.Q.; Wang, F.; Liu, J.; Kang, K.; Costa, F. A blockchain-based framework for green logistics in supply chains. *Sustainability* 2020, 12, 4656. [CrossRef]

79. Guan, Z.; Zhang, Y.; Wu, L.; Wu, J.; Li, J.; Ma, Y.; Hu, J. APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT. *J. Netw. Comput. Appl.* 2019, 125, 82–92. [CrossRef]