applied sciences

MDPI

Review

Blockchain-Enabled Supply Chain Management: A Review of Security, Traceability, and Data Integrity Amid the Evolving Systemic Demand

Özgür Karaduman * and Gülsena Gülhas

Department of Software Engineering, Faculty of Engineering, Fırat University, Elazığ 23119, Türkiye; gulsenagulhass@gmail.com

* Correspondence: okaraduman@firat.edu.tr

Abstract: As supply chains become increasingly digitized and decentralized, ensuring security, traceability, and data integrity has emerged as a critical concern. Blockchain technology has shown significant potential to address these challenges by providing immutable records, transparent data flows, and tamper-resistant transaction logs. However, the effective application of blockchain in real-world supply chains requires the careful evaluation of both architectural design and technical limitations, including scalability, interoperability, and privacy. This review systematically examines existing blockchain-based supply chain solutions, classifying them based on their structural models, cryptographic foundations, and storage strategies. Special attention is also given to underexplored humanitarian logistics scenarios. It introduces a three-dimensional evaluation framework to assess security, traceability, and integrity across different architectural approaches. In doing so, it explores key technological enablers, including advanced mechanisms such as zero-knowledge proofs (ZKPs) and cross-chain architectures, to meet evolving privacy and interoperability demands. Furthermore, this study outlines a conceptual cross-chain interaction scenario involving permissioned and permissionless blockchain networks, connected through a bridge mechanism and supported by representative smart contract logic. The model illustrates how decentralized stakeholders can interact securely across heterogeneous blockchain platforms. By integrating quantitative metrics, architectural simulations, and qualitative analyses, this paper contributes to a deeper understanding of blockchain's role in next-generation supply chains, offering guidance for researchers and practitioners aiming to design resilient and trustworthy supply chain management (SCM) systems.

Keywords: blockchain; supply chain management; security; traceability; data integrity; smart contracts; cross-chain security; interoperability; transparency; disaster relief

Academic Editor: Hui Li

Received: 7 April 2025
Revised: 4 May 2025
Accepted: 5 May 2025
Published: 6 May 2025

Citation: Karaduman, Ö.; Gülhas, G. Blockchain-Enabled Supply Chain Management: A Review of Security, Traceability, and Data Integrity Amid the Evolving Systemic Demand. *Appl. Sci.* **2025**, *15*, 5168. https://doi.org/10.3390/app15095168

1. Introduction

Modern supply chains have evolved into complex, globally distributed ecosystems that demand high levels of data integrity, system transparency, and secure collaboration to function reliably. As these systems grow in scale and complexity, ensuring transparency, traceability, and secure data sharing has become increasingly difficult. Cyberattacks, counterfeiting, data tampering, and a lack of trust among actors undermine the effectiveness and resilience of supply chain ecosystems. These vulnerabilities are particularly severe in critical domains, such as food traceability, pharmaceutical distribution, and humanitarian logistics, where failures may lead to regulatory, economic, or even humanitarian consequences. One of the key drivers behind this complexity is the growing diversity of products,

dynamic geopolitical factors, and the exponential increase in data generated throughout supply chain operations [1–3].

Traditional SCM systems, which often rely on centralized and opaque infrastructures, struggle to manage these realities effectively. They remain vulnerable to data tampering, counterfeiting, and cyber threats. In response, blockchain technology has emerged as a promising enabler, offering decentralized, tamper-resistant, and transparent ecosystems that may align better with the demands of modern SCM [4,5].

Blockchain's potential in SCM lies in its ability to automate trust through smart contracts, enhance traceability via immutable ledgers, and ensure data integrity through consensus mechanisms and cryptographic techniques. However, while the technology has shown promise across various industries, its integration into real-world SCM operations is not without barriers. Organizational readiness, standardization gaps, and legal uncertainty remain key obstacles [5,6].

Although blockchain promises significant improvements in transparency, data reliability, and decentralized trust across supply chain networks, these benefits may not always be fully realized in practice. Real-world implementations demonstrate that aligning blockchain technology with the complex and evolving nature of SCM remains a nuanced task. Challenges such as adoption resistance, fragmented standards, smart contract limitations, and persistent interoperability constraints across diverse contexts continue to hinder the widespread implementation of blockchain in real-world supply chain systems [1,6].

Moreover, the continuous evolution of systemic demands, driven by factors such as quantum threats, the proliferation of IoE systems, and AI-enhanced logistics, has redefined what security, traceability, and data integrity mean within supply chain ecosystems. These technologies not only introduce new capabilities but also shift the architectural expectations of blockchain-enabled systems [7]. In this dynamic landscape, ensuring trust, traceability, and data integrity is no longer a static design concern but a forward-looking imperative that requires continuous technological alignment and adaptive policy frameworks [8].

1.1. Contributions

This review provides a comprehensive and structured synthesis of blockchain-enabled SCM, with a focus on the evolving requirements of security, traceability, and data integrity. This study goes beyond conventional perspectives by integrating cross-sectoral evidence, technological foresight, and socio-organizational dimensions. The key contributions of the paper are as follows:

1. *The cross-sectoral evaluation of blockchain applications in supply chains*: The present study reviews how blockchain is implemented across diverse sectors, such as logistics, healthcare, agriculture, retail (particularly pharmaceuticals), and humanitarian supply chains. It compares strategies and contextual constraints to understand the role of sector-specific dynamics in shaping blockchain adoption.
2. *The identification of key SCM security risks and blockchain's mitigation capabilities*: this study identifies recurring supply chain security challenges, such as product counterfeiting, traceability breakdowns, and data tampering, and examines how blockchain mechanisms, like decentralization, smart contracts, and cryptographic assurance, address them.
3. *The analysis of the new security challenges introduced by blockchain itself*: In addition to addressing external threats, this paper analyzes security concerns that arise from blockchain's own architecture. These include the rigidity of smart contracts, oracle dependencies, the lack of interoperability, and issues with off-chain data validation, each of which poses potential operational vulnerabilities.

4. *The inclusion of humanitarian use cases to expand the existing literature*: by integrating disaster relief, refugee logistics, pandemic responses, and donation transparency into the review, this study highlights blockchain's underexplored potential in high-risk and resource-constrained environments, thereby extending the boundaries of current SCM research.
5. *The examination of organizational barriers and socio-technical adoption constraints*: This review addresses non-technical adoption barriers, such as institutional resistance, skill shortages, regulatory uncertainty, and concerns over privacy and transparency. These are critical for evaluating blockchain's real-world viability beyond prototypes.
6. *Thematic mapping between SCM risks and blockchain architectures*: A conceptual framework is presented that links classified supply chain risks with corresponding blockchain-based countermeasures. This mapping assists both researchers and practitioners in selecting appropriate blockchain designs for specific operational contexts.
7. *Positioning blockchain within the context of evolving systemic demands*: This paper evaluates how emerging paradigms, like the IoE, edge computing, and quantum threats, are reshaping trust, traceability, and data assurance in supply chains. It emphasizes the need for blockchain systems to adapt to dynamic and future-oriented environments.
8. *Recommendations and research directions for future blockchain–SCM integration*: it outlines key gaps in the literature and suggests future research topics, such as post-quantum cryptography, scalable architecture design, privacy-preserving smart contracts, and real-time integration through edge computing.
9. *The formal analysis of ZKP principles in an SCM context*: This study introduces a structured mathematical framing of zero-knowledge proof (ZKP) properties, completeness, soundness, and zero-knowledge, and analyzes their relevance within supply chain systems. By highlighting how these principles support trust, privacy, and auditability, the work bridges abstract cryptographic logic with practical SCM requirements, such as secure traceability and data confidentiality.
10. *Conceptual cross-chain architecture for supply chain interoperability*: This study introduces a conceptual cross-chain architecture that demonstrates how supply chain stakeholders, such as suppliers, retailers, and auditors, can operate across heterogeneous blockchain platforms, including Hyperledger Fabric and Ethereum. By incorporating ZKP-based validation and oracle-assisted communication via a Chainlink bridge, the model outlines a secure and interoperable structure for coordinating distributed supply chain processes while ensuring data integrity, transparency, and traceability. In this regard, it provides a guiding framework for the design of blockchain-enabled SCM systems.

1.2. Methodology

This study applies a multi-layered and structured review methodology to evaluate how blockchain technologies enhance SCM, with particular attention to security, traceability, and data integrity. The methodological approach comprises the following stages:

1. *The selection of studies and data sources*: A wide range of peer-reviewed journal articles, industrial white papers, and case studies were collected from recognized scientific databases, such as IEEE Xplore, Elsevier, Springer, MDPI, Wiley, ACM, and Taylor & Francis, and Emerald. No single publisher was prioritized. Instead, studies were selected based on their relevance to blockchain applications in SCM, particularly those addressing security vulnerabilities, traceability mechanisms, and data integrity concern.
2. *Timeframe and inclusion criteria*: In selecting the references for this study, priority was given to recent and high-impact publications that reflect the evolving landscape of blockchain-enabled supply chain systems. While emerging research was emphasized

to ensure relevance, foundational works were also incorporated to provide theoretical completeness and contextual continuity.

3. *Search strategy and keywords*: Keyword-based searches were conducted using combinations of terms such as "blockchain supply chain security", "blockchain traceability", "data integrity in blockchain SCM", "smart contract vulnerabilities", "cross-chain interoperability", "privacy-preserving blockchain mechanisms", "confidential transactions in SCM", and "blockchain for humanitarian logistics". These search queries were carefully selected to capture recent advancements and reflect the evolving technological and systemic challenges discussed in the literature.
4. *The thematic classification of supply chain risks and blockchain-based mitigations*: The identified studies were classified based on recurring SCM risk categories, including product counterfeiting and authenticity concerns, data tampering and inconsistency, limited traceability across multi-tier networks, and Internet of Things (IoT)-related security weaknesses. Each risk category was analyzed alongside relevant blockchain-based mechanisms, such as smart contracts for automation and enforcement, cryptographic hashing for data integrity, decentralized consensus protocols for trust-building, and oracles and interoperability standards for external data integration.
5. *The sectoral assessment of blockchain applications in SCM*: Blockchain adoption was analyzed across logistics, agriculture, food, healthcare, and retail supply chains. This stage aimed to extract
    - Adoption variations across sectors;
    - Context-specific implementation challenges;
    - Legal and regulatory concerns;
    - Sector-specific use cases demonstrating blockchain's impact on traceability, security, and data reliability.
6. *The comparative evaluation of blockchain's contribution to SCM pillars*: this study further assessed how blockchain addresses the core pillars of SCM:
    - *Security*: by enabling tamper resistance, fraud prevention, and secure access control;
    - *Traceability*: through real-time visibility, end-to-end product tracking, and provenance assurance;
    - *Data integrity*: via synchronized, immutable ledgers shared across stakeholders.
7. *The visualization and synthesis of the findings*: To enhance clarity and comparative insight, the results are presented using structured tables, conceptual mappings, and thematic summaries. These visual elements highlight the trade-offs among blockchain technologies across different supply chain layers, offering practical guidance for future research and system design under evolving systemic demands.

The remainder of this paper is structured as follows. In Section 2, the major security threats encountered in traditional supply chains are analyzed and categorized under the headings of the lack of traceability, data integrity issues, counterfeit products, IoT vulnerabilities, and cyberattacks. Section 3 discusses the core security advantages offered by blockchain technology against these threats, providing an evaluation based on components such as immutable records, smart contracts, cryptographic signatures, and decentralization. Section 4 presents a comprehensive examination of the security vulnerabilities and attack methods observed in blockchain-enabled supply chains. Section 5 presents an in-depth exploration of solution mechanisms and integration models for blockchain-based supply chain security. It covers the architectural and operational distinctions between permissioned and permissionless systems and further examines advanced privacy-preserving technologies, such as ZKPs, confidential transactions, and cross-chain interoperability frameworks. The section also introduces a conceptual architectural model and smart contract logic tailored

for decentralized SCM environments. Section 6 explores blockchain applications across various sectors, such as healthcare, agriculture, food, and logistics, through a comparative analysis, assessing the impact of the technology based on the specific risk profile of each sector's supply chain. This section also provides an in-depth review of blockchain implementation in humanitarian supply chains. Section 7 evaluates the systemic challenges faced by blockchain-based systems in terms of sustainability, interoperability, data privacy, and governance and discusses the implications of emerging technologies, such as quantum threats, AI-driven logistics, and the IoE. Finally, Section 8 outlines future solution proposals and research directions for blockchain-supported supply chain systems, in light of existing gaps in the literature and current research trends.

2. Key Security Challenges in Traditional Supply Chain Management

A supply chain is an integrated system that encompasses all activities involved in delivering a product or service from the supplier to the final consumer, as well as the coordination among these activities and associated information flows [1–3]. Within this system, certain challenges are encountered, including significant issues such as counterfeiting, traceability, data integrity, and cyber-attacks [4,5]. To address these challenges, blockchain technology has started to be implemented in supply chains. Integrating blockchain into supply chains provides a more transparent and secure system for both consumers and producers by reducing security vulnerabilities. This technology plays a critical role in verifying product origin, ensuring data integrity, and combating counterfeiting [6]. As illustrated in Figure 1, security issues in the supply chain can be categorized under five main headings: the lack of traceability, data integrity risks, counterfeit products and record deficiencies, data security issues in IoT integration, and supply chain attacks. Security vulnerabilities in supply chain networks emerge during interactions among various actors throughout processes ranging from production to the final consumer. In this context, raw material suppliers, intermediate producers, logistics providers, and retailers face diverse risks during digital data exchange and physical product movement. Malicious individuals or groups may exploit these vulnerabilities, compromising supply chain integrity, tampering with critical components, or accessing sensitive data illicitly. Consequently, security breaches within supply chains not only diminish operational efficiency but also severely damage brand reputation and customer trust.

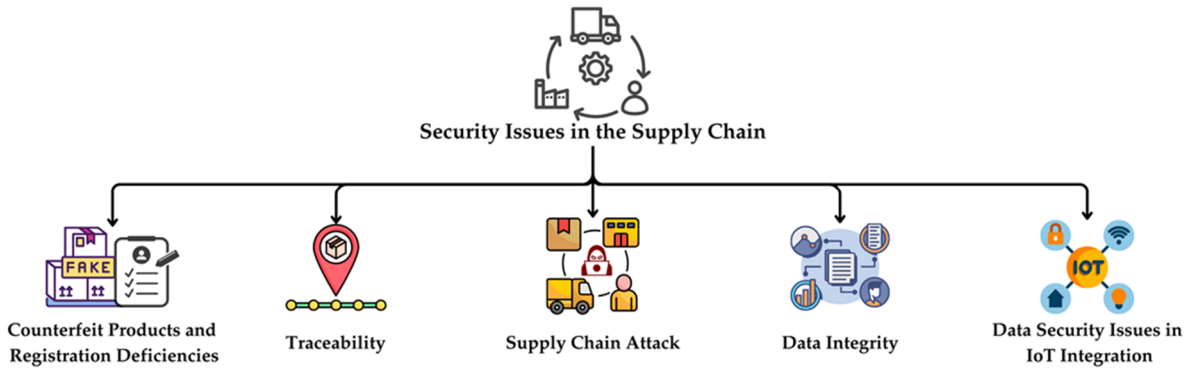

Figure 1. Major security issues in traditional supply chain management.

2.1. Traceability Deficiencies in Traditional Supply Chains

Traceability in a supply chain, as demonstrated in Figure 2, involves monitoring products through various stages, beginning from production, continuing through logistics and warehousing, distribution and transportation, processing, or points of sale, and ultimately reaching the consumer. However, a lack of traceability emerges as a significant issue when products cannot be adequately tracked throughout their lifecycle, from raw materials to

finished goods. This situation leads to various problems, such as the inability to verify product origin, non-transparent production processes, and losses occurring during distribution stages. In particular, differences in data formats and management systems among stakeholders, the absence of standardized data representation methods, and inadequacies in reliable data storage mechanisms are the primary reasons behind the lack of traceability [7].

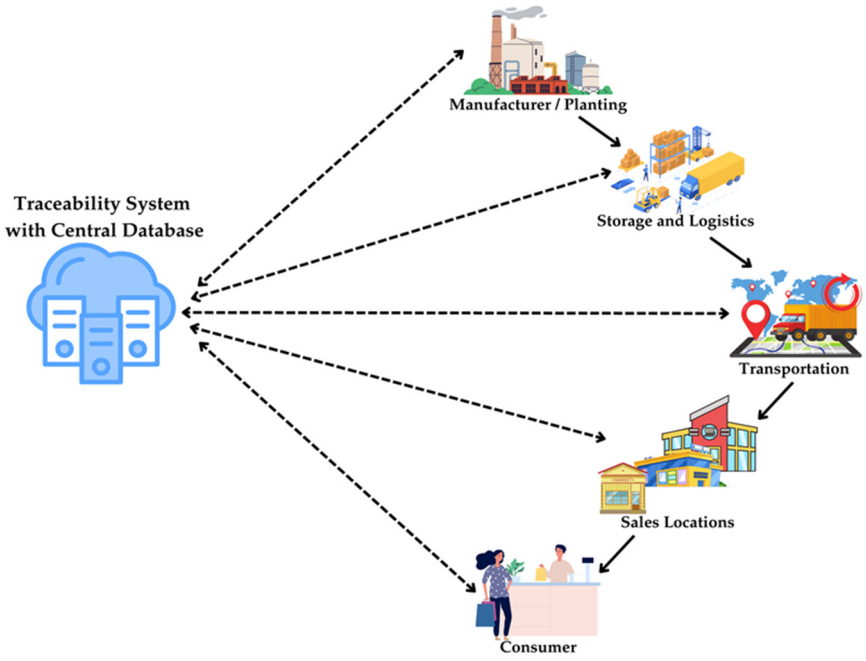

Figure 2. Traditional supply chain process.

The lack of traceability poses significant risks in critical areas such as food safety. For instance, the inability to identify the source of contaminated products can pose threats to public health. Additionally, failure to achieve transparency in the supply chain can undermine consumer confidence, thereby damaging brand reputation. An effective traceability system not only enhances quality and safety but also improves the operational efficiency of businesses, thereby facilitating better decision-making processes [8].

2.2. Data Integrity Risks

Data integrity refers to the capability of maintaining the accuracy, completeness, and consistency of information within a supply chain. Traditional centralized data management systems may contain vulnerabilities that allow unauthorized individuals to alter or manipulate this information. Such vulnerabilities can lead to critical supply chain data being compromised by malicious actors or unforeseen technical issues. For example, in the pharmaceutical industry, the incorrect recording of vital data, such as dosage and manufacturing dates, has the potential to cause severe health consequences. In contrast, blockchain-based systems significantly prevent data manipulation by encrypting each transaction and storing it through distributed ledger technology. Consequently, while protecting all data within the supply chain, any unauthorized changes can be immediately detected, enabling swift preventive measures.

2.3. Counterfeit Products and Record Deficiencies

Counterfeit products and record deficiencies arise particularly in scenarios where information about product origin and quality is intentionally altered. Such situations undermine consumer trust in purchased products, potentially causing businesses to suffer reputational damage and financial loss [5]. The presence of counterfeit goods within

supply chains is regarded as a serious issue, resulting in significant economic losses and decreased consumer confidence. Particularly in sectors such as pharmaceuticals, food, and luxury consumer goods, the introduction of counterfeit products into the market can pose substantial threats to public health and safety. Traditional record-keeping systems are limited in verifying the authenticity of products, while incomplete records within supply chains can facilitate counterfeit activities. In this context, blockchain technology establishes a digital identity for each product, integrating production, distribution, and sales processes into an immutable record infrastructure. Consequently, the detection of counterfeit products becomes feasible, enabling consumers and businesses to reliably verify product origins.

2.4. Data Security Issues in IoT Integration

The IoT is a network of devices designed to collect and share data over the internet. This technology enables everyday objects to become smart and provides benefits across numerous sectors including industry, agriculture, and healthcare [9]. The IoT holds significant importance within supply chains, enhancing their performance through real-time data collection and monitoring capabilities. With IoT devices, a continuous data flow throughout supply chain stages is achieved via sensors [10]. Thus, the IoT offers the following advantages:

- Enables real-time traceability, increasing transparency at every stage of the supply chain.
- Ensures continuous data flows, allowing more accurate inventory management and timely deliveries.
- Reduces human intervention through automated systems, accelerating processes and enhancing operational efficiency.
- Anticipates potential supply chain disruptions or deviations, thereby supporting risk management.

However, as IoT devices generate large volumes of data and maintain continuous communication with servers and storage systems throughout the supply chain, they are exposed to various security risks, including data privacy concerns, unauthorized access, and network attacks [11]. Due to their dependence on centralized systems, they can become vulnerable to cyberattacks, potentially leading to data manipulation, traceability issues, and privacy risks [9]. At this point, blockchain technology holds promise for addressing IoT-related security issues. With its decentralized architecture, cryptographic methods, and immutable record features, blockchain enables secure data exchange among IoT devices, maintains data integrity, and reduces dependency on centralized servers, thus improving network resilience [12].

2.5. Supply Chain Attacks Exploiting Trusted Software Channels

Supply chain attacks target security vulnerabilities occurring during the development and distribution phases of software components, enabling attackers to infiltrate systems, often through trusted updates or open-source projects. Such attacks, particularly those exploiting software updates designed to patch security vulnerabilities, have become increasingly prevalent, posing severe threats to business continuity and financial stability [5,13].

In particular, zero-day vulnerabilities and malicious software infiltrating at various stages of the supply chain can result in significant consequences, such as data breaches, operational disruptions, and financial losses. Ransomware and Distributed Denial of Service (DDoS) attacks disrupt logistics and manufacturing processes, while vulnerabilities associated with third-party suppliers also jeopardize the integrity of the supply chain. Additionally, phishing and social engineering attacks targeting employees can lead to unauthorized access to supply chain systems [14]. Insider threats, through misconfigurations and erroneous changes, further compromise the security of the supply chain. The

classification of various cyber threats affecting supply chains, along with their targets, attack methods, and potential impacts, is summarized in Table 1.

Table 1. Classification of cyber threats targeting supply chain security.

Cyber Threat	Targeted Asset	Attack Method	Potential Impact
Phishing [14]	Credentials	Fake Emails, SMS, Websites	Data leakage, unauthorized access
Insider Threats [15]	Data, Systems, Networks	Unauthorized Access, Data Leakage, Identity Theft, Sabotage	Data loss, operational disruption, financial loss, loss of trust
DDoS [14]	Network Infrastructure, Services	Botnets, System Overload, Flooding	Service disruption, customer loss, reputational damage
Ransomware [16–19]	Data, Systems	Malware, File Encryption, Ransom Demands	Operational downtime, data loss, financial loss
Zero-Day [14,20]	Software, Hardware	Undiscovered Vulnerabilities, Exploits	Unauthorized access, system manipulation, data breach
Malware [14,19,21]	Systems, Networks	Viruses, Trojans, Keyloggers	Data theft, financial losses
Man-in-the-Middle [22,23]	Network Traffic, Communications	Unencrypted Networks, DNS Spoofing, Packet Sniffing	Data theft, privacy violation, system compromise
Social Engineering [24]	Human Factor, Credentials	Phone Calls, Fake Support	Credential theft, fraud

3. Enhancing Supply Chain Security Through Blockchain Technology

Having examined the technical and sectoral dimensions of blockchain in SCM, this section synthesizes the key insights and presents broader discussions on integration, sustainability, and security trade-offs. Blockchain offers a decentralized and secure data storage mechanism through cryptographically linked blocks, supporting the confidentiality, integrity, and accessibility of data [25–27].

3.1. Security Advantages of Blockchain in Supply Chains

The core elements underpinning blockchain security include immutable records, automated and reliable transactions, cryptographic signatures, and decentralization. These features enhance the resilience of blockchain-based systems against manipulation, thus securing data integrity. Immutable records eliminate the risk of data manipulation by preventing retroactive alterations of information recorded in blocks. Smart contracts accelerate data verification processes by executing predefined mechanisms automatically when specified conditions are met. Cryptographic signatures ensure the accuracy and authenticity of each transaction, safeguarding data integrity. Lastly, decentralization allows for the establishment of a trustworthy tracking mechanism within supply chain processes, independent of a single central authority. These elements, classified in Figure 3, are discussed in detail in the following subsections.

3.1.1. Immutable Records Ensuring Data Integrity in Supply Chains

The immutability characteristic of blockchain technology plays a critical role in preventing data manipulation within supply chains. Blockchain records each transaction into a cryptographically secured chain of blocks, which are verified by all the participants through a distributed ledger. Once a block is added to the chain, altering data in previous blocks becomes practically impossible, as any change would create inconsistencies, disrupting the consensus mechanism of the entire network. This mechanism ensures data integrity, making transactions conducted at any stage of the supply chain irreversible [25,28]. For

instance, in sectors such as food, pharmaceuticals, or logistics, all activities from production to delivery to the final consumer are recorded securely, thus preventing the manipulation of these records. This facilitates the detection and tracking of counterfeit products, preventing fraudulent transactions and false declarations within the system.

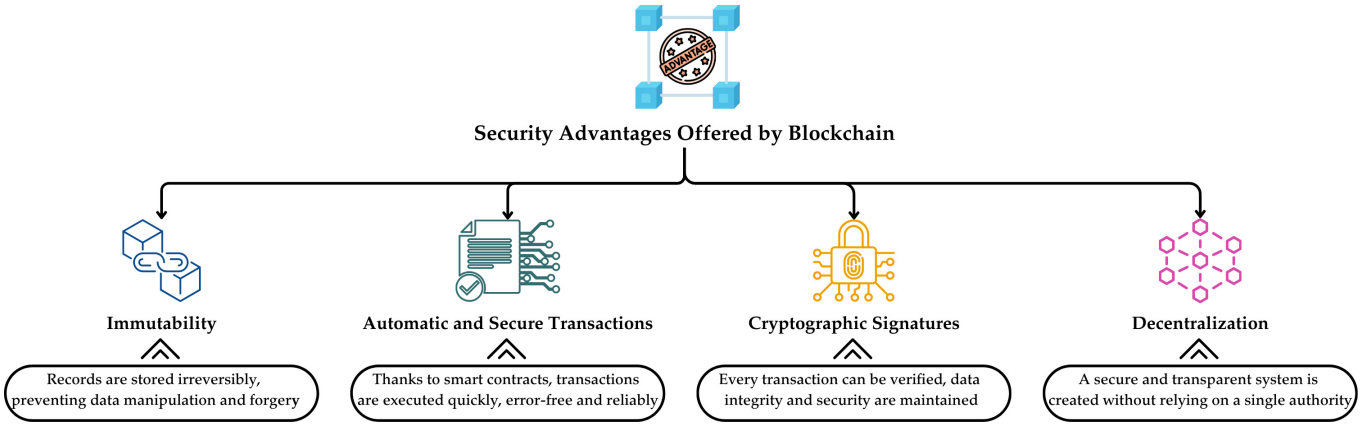

Figure 3. Security advantages of blockchain in supply chains.

In sectors such as the food industry, blockchain's immutable and transparent structure has been shown to strengthen trust across supply chain actors, which indirectly supports the prevention of counterfeiting and fraud [29]. Moreover, blockchain technology enhances transparency, traceability, and security, accelerates processes, reduces costs through the use of smart contracts and cryptocurrencies, prevents fraud, and eliminates the need for intermediaries. Additionally, blockchain-based web platforms have been developed to establish traceability and trust within supply chains, enabling the detection of counterfeit products [30]. Through such systems, retrospective alterations to blockchain-recorded supply chain transactions are prevented, significantly increasing transparency.

3.1.2. Automated and Reliable Transactions

Smart contracts operating on blockchain are digital protocols executed automatically based on predefined rules, without external intervention. By removing the human factor, these contracts enhance transaction reliability and reduce costs. Integrated with IoT devices, especially in areas such as supply chains, smart contracts facilitate functionalities including payment automation, buyer verification, and triggering necessary actions in cases of non-compliance with contractual conditions [31].

By automating traditional processes in various sectors, smart contracts significantly enhance security and efficiency, accelerate transactions, and minimize human errors [32]. In supply chains, smart contracts offer transparency and reliability at every stage. Since all transactional data are securely stored on digital ledgers, the need for third-party verification is eliminated, ensuring authenticity and security in areas such as transportation and food processing. Within IoT applications, smart contracts enable automatic communication between devices, thus creating more autonomous structures in smart cities, homes, and environmental monitoring projects.

Table 2 summarizes various studies on smart contract utilization in supply chain management, highlighting their primary focus areas and advantages. Enabling only verified stakeholders to interact through smart contracts has been emphasized as a means of enhancing trust and transparency among participants [33]. Another study aims to develop a secure product traceability system using blockchain and smart contracts, demonstrating improved data security through decentralized architecture, as well as validated accessibility and tamper-resistance during testing [34]. Ethereum-based smart contracts have been iden-

tified as significantly improving transparency, trust, and efficiency within supply chains, although some limitations regarding flexibility and volatility have been acknowledged [35]. Additionally, a framework integrating Ethereum-based smart contracts developed in Solidity into supply chain management has been proposed, enhancing transparency, traceability, and security. This system increases reliability by preventing data manipulation via smart contracts and automating supply chain processes using distributed ledger technology [36].

Table 2. Analysis of smart contract applications in supply chain management.

References	Focus Area	Advantages
[33]	Interaction of verified stakeholders via smart contracts, enhancing trust and transparency.	Increased trust and transparency
[34]	Blockchain and smart contracts for secure product traceability system.	Data security, accessibility, tamper-resistant
[35,36]	Ethereum-based smart contracts for transparent, reliable, efficiency and traceable supply chain management.	Transparency and traceability, security, cost and time savings, recycling tracking, cold chain tracking

3.1.3. Cryptographic Signatures

Cryptographic signatures (digital signatures) are utilized to verify data origin and prevent unauthorized access [37]. Operating on the principle of asymmetric cryptography [38], this system encrypts data using a private key held by the signer. The resulting signed data can subsequently be validated by any verifier using a corresponding public key. If a logical outcome is obtained during the verification stage, the data are accepted as both authentic and unchanged. Consequently, by keeping the private key confidential, identity fraud and unauthorized alterations of documents are significantly prevented.

In distributed ledger structures, such as blockchain, cryptographic signatures play a critical role in verifying the authenticity of blocks or transactions created by multiple authors. Each transaction or block is signed using the author's private key, and other network participants validate this signature with the author's public key, confirming both the source and the integrity of the data. Thus, trust is established among the network participants, ensuring overall system transparency [39]. A blockchain and IoT-integrated model has been proposed to enhance data privacy and transparency within supply chain management [40]. In the proposed model, IoT devices are employed to securely collect and store data, while cryptographic techniques and a permissioned blockchain network safeguard data privacy and integrity.

3.1.4. Decentralization as a Foundation for Supply Chain Trust and Integrity

Blockchain is the most widely implemented form of distributed ledger technology (DLT) [41]. Distributed ledger technology is a system where data are shared among multiple participants without the need for a central authority. Each participant maintains a copy of the ledger and can independently verify transactions using this copy. To ensure data integrity and prevent discrepancies, a trust mechanism is required. This mechanism functions through a consensus protocol, enabling all the participants within the network to collectively agree upon transactions [42]. The distributed ledger is independently managed by each node, allowing the creation of new blocks without reliance on a centralized authority [43]. The decentralized structure offered by blockchain technology can be integrated across various network types and use cases. Particularly in fields where data security and integrity are critical, the advantages provided by distributed ledger technologies become increasingly significant. In this regard, blockchain-based security mechanisms hold

considerable importance for sensitive industries, such as supply chain management. A blockchain-based decentralized application (DApp) has been developed to address counterfeiting issues within supply chains and has been utilized to enhance transparency in supply chain management [44].

3.2. Comparison of Traditional and Blockchain-Based Supply Chains

Traditional supply chains face various security and efficiency challenges due to their centralized structures. These systems exhibit significant limitations regarding data integrity, traceability, and operational efficiency, introducing risks such as counterfeiting, data manipulation, and a lack of transparency in processes. In this framework, blockchain-based supply chains aim to address these centralization-induced issues by offering secure, transparent, and automated solutions that enhance the overall system integrity and reliability. A detailed comparative analysis of traditional and blockchain-based supply chains is presented in Table 3.

Table 3. Comparative analysis of traditional and blockchain-based supply chains.

Criterion	Traditional Supply Chain	Blockchain-Based Supply Chain
Transparency [43]	Limited data sharing between actors; potential lack of trust.	Secure and verifiable ledger accessible to all stakeholders.
Data Management [44,45]	Uses centralized databases; data can be altered or deleted.	Immutable records prevent data manipulation.
Traceability [46]	Product histories tracked manually or by separate systems; lack of transparency.	End-to-end traceability throughout supply chain; real-time verification of product histories.
Data Integrity [43,47]	Centrally managed data; a single error may impact all processes.	Data immutability ensured through cryptographic signatures and hashing algorithms.
Counterfeiting and Manipulation [47]	Possible entry of counterfeit products; manual verifications required.	Tokenization and digital identities verify product origin and history.
Security [48]	Vulnerable to cyberattacks; database breaches can lead to extensive data losses.	DLT minimizes central attack risk.
IoT Integration [49]	Limited data security with IoT devices; risks of data loss and manipulation.	IoT data securely stored in immutable blockchain records.
Smart Contracts [50]	Manual execution of transactions; reliance on third-party validation.	Automated processes through smart contracts reduce human error.
Operational Efficiency [51]	Delays due to manual validations and intermediaries.	Automated, reliable, and accelerated transaction processes.
Costs [43,51]	High dependency on intermediaries and manual processes increases costs.	Reduced operational costs by minimizing intermediary reliance.

4. Security Threats and Attack Methods in Blockchain-Based Supply Chain Management

The previous section discussed how blockchain technology can enhance the security of traditional supply chain systems. This section, by contrast, focuses on the specific security threats inherent to blockchain-based architectures, examining the unique risks that arise from their decentralized structure. While the integration of blockchain technology into supply chains provides an effective solution to enhance security and transparency, these systems are not entirely immune to malicious attacks. Malicious actors may exploit vulnerabilities within supply chain processes to manipulate data related to product origin, transportation, and storage. Technologies commonly utilized in supply chains, such as IoT devices, RFID tags, or sensors, are particularly susceptible to the risks of data manipulation and unauthorized

access. Attacks targeting these devices can result in the generation of false information or compromise the integrity of the system. Furthermore, blockchain systems themselves may present vulnerabilities. Weaknesses inherent in blockchain code structures or consensus mechanisms could potentially be exploited to alter transaction data or disrupt network operations. Consequently, developing more robust defense mechanisms against these threats is critical for ensuring supply chain security [48]. Figure 4 presents a classification of security threats and attack methods specific to blockchain-based supply chains.

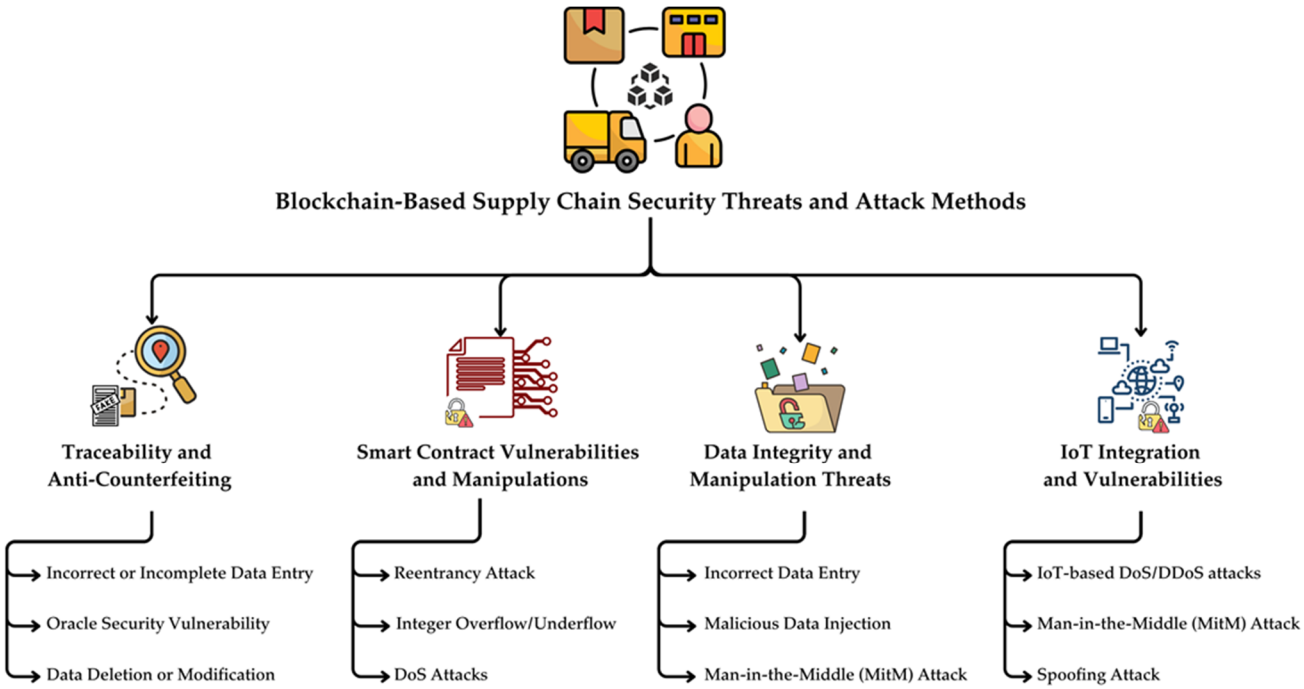

Figure 4. Classification of security threats and attack methods in blockchain-based supply chain.

4.1. Traceability and Anti-Counterfeiting Measures

Centralized structures and opaque data sharing in traditional supply chain systems create information gaps, significantly complicating anti-counterfeiting efforts [52]. In this regard, blockchain technology provides crucial contributions by transparently recording the movement of products along the supply chain onto an immutable ledger, thereby preventing the spread of counterfeit goods [7]. Nevertheless, despite blockchain's inherent advantages of security, auditability, and immutability, ensuring the accuracy and integrity of the data entered into the system remains a critical issue [53]. In particular, incorrect or incomplete data entry, when combined with the reliability concerns associated with off-chain data sources, poses a considerable threat to overall supply chain security. These security threats and attack methods are detailed below:

- *Incorrect or incomplete data entry*: The accuracy of blockchain data depends directly on the reliability of the information provided at entry points. Incorrect or incomplete data entries can lead to flawed records on the blockchain, undermining anti-counterfeiting efforts [54]. For instance, if suppliers or manufacturers deliberately or negligently misreport product origins, consumer deception and market trust erosion become significant risks.
- *Oracle vulnerabilities*: The reliability of external data sources constitutes a critical vulnerability in blockchain-based supply chains. The transfer of logistical data, quality control reports, and certificates onto the blockchain relies heavily on oracle mechanisms. However, oracles are susceptible to technical attacks and can be manipulated by malicious actors. Additionally, companies may provide false data to achieve competitive advantages, undermining the transparency and reliability of the entire system [55]. Due

to blockchain's immutable nature, transactions based on incorrect data provided through oracles cannot be reversed, posing substantial risks for stakeholders [56]. Although solutions such as multi-source verification and reputation-based validation have been proposed, the absolute security of external data sources remains elusive. It is emphasized that oracle security should be supported not only by technical measures but also by regulatory frameworks [57]. A trust model using blockchain-based supply chain traceability has been proposed to overcome these oracle-related security concerns [58]. For instance, an Italian dairy company employed blockchain technology to combat product counterfeiting but had to implement additional measures to address oracle-related security risks. Independent certification authorities and incentive mechanisms were introduced to enhance the data accuracy and strengthen the system's reliability.

- *Data deletion or modification*: The ability to alter historical records in traditional databases significantly increases the risk of manipulation and counterfeiting in supply chains. For example, manufacturers or distributors can retrospectively modify delivery records of products that fail quality standards, misrepresenting these products as safe or compliant. Although blockchain data are immutable, inadequate integration between blockchain and traditional systems or the failure to reflect certain records onto the blockchain continues to pose counterfeiting risks [47,54].

Table 4 presents a comparative overview of various studies employing blockchain technology to combat counterfeiting. An Ethereum-based blockchain system was developed to prevent counterfeit products, allowing manufacturers to transparently record product information on the blockchain. This system enables consumers to independently verify product authenticity through smart contracts and digital signatures, providing a cost-effective, decentralized anti-counterfeiting solution [59]. Blockchain's impact on anti-counterfeiting and traceability in wine supply chains was analyzed using Stackelberg game theory, revealing that blockchain enhances transparency and reduces counterfeiting, though its adoption is influenced by cost and privacy factors [60]. A novel blockchain-based system named Janus was introduced to enhance drug traceability and prevent counterfeit drugs from entering the supply chain.

Table 4. Analysis of blockchain-based traceability and anti-counterfeiting studies in supply chains.

Ref.	Objective	Methodology	Outcome
[59]	Developing an Ethereum-based blockchain system to prevent counterfeit products	Manufacturers record product details on blockchain, creating a verification mechanism using smart contracts and digital signatures	Provides a low-cost, decentralized anti-counterfeiting solution
[60]	Preventing counterfeiting and enhancing traceability in wine supply chains	Blockchain-based monitoring systems analyzed using Stackelberg game theory	Blockchain enhances transparency but adoption is influenced by cost and privacy concerns
[61]	Developing the blockchain-based system Janus to prevent counterfeit drugs from entering the supply chain	Clone-resistant hologram labels and a multi-quorum consensus protocol ensure secure traceability	Creates a transparent tracking system providing load balancing and fairness
[62]	Enhancing traceability and security in food supply chains through a blockchain-based model	Performance evaluated using simulations on Hyperledger Fabric	Blockchain strengthens food traceability but faces scalability and data privacy constraints
[63]	Improving security and traceability in tea supply chains using a Hyperledger Fabric-based system	System ensures data integrity and transparency using Hyperledger Fabric, ECDSA, and IPFS; performance assessed by Hyperledger Caliper	System performance successful in terms of transaction latency and volume

Utilizing clone-resistant hologram labels and a multi-quorum consensus protocol, this system offers transparent and secure traceability, emphasizing load balancing and fairness [61]. Another blockchain-based model aimed at enhancing traceability and security in food supply chains demonstrated efficient transaction volumes and latency through simulations conducted on Hyperledger Fabric. The results indicated that blockchain could significantly strengthen food safety despite certain limitations related to scalability and data privacy [62]. Additionally, a Hyperledger Fabric-based system was developed to improve security and traceability in tea supply chains. Employing ECDSA for authentication and IPFS for data storage [64], the system's performance was positively evaluated with Hyperledger Caliper, showing satisfactory results regarding transaction latency and volume [63].

4.2. Data Integrity and Manipulation Threats

While data integrity aims to preserve the accuracy and reliability of information, inadequate data validation, a lack of encryption, and reliance on untrusted third-party components pose significant risks. Outdated systems become vulnerable to attacks, such as SQL injection and cross-site scripting (XSS), while unencrypted data traffic and improperly configured network settings pave the way for unauthorized access. These vulnerabilities can result in data manipulation within supply chains, severely compromising the overall system security [48]. In this sense, major threats to data integrity can be categorized into three groups: incorrect data entry, malicious data injection, and Man-in-the-Middle (MitM) attacks. Firstly, incorrect data entry leads to permanent errors due to blockchain's immutable nature. Secondly, malicious data injection deliberately introduces misleading information, undermining data integrity. Lastly, MitM attacks exploit communication vulnerabilities, facilitating data manipulation. These threats are explored in more detail below:

- *Incorrect data entry*: Due to blockchain's immutability, incorrect or incomplete data entries represent a critical security risk. Once erroneous information is recorded, it becomes permanent and cannot be corrected [54]. This can lead to poor decision-making and operational disruptions within supply chains. Because manual data entry inherently carries risks of user errors or intentional manipulation, effective data validation mechanisms must be rigorously implemented.
- *Malicious data injection*: This threat involves unauthorized actors deliberately inserting inaccurate or manipulated data into the system. Such attacks can lead to false product movement records and the creation of fraudulent entries within the supply chain. Particularly, unverified data from external sources, such as IoT devices, can lead to the system operating on deceptive information. To mitigate this risk, it is essential to apply data source verification methods and secure data-entry procedures utilizing smart contracts [55,56].
- *MitM attacks*: These attacks threaten data integrity by intercepting and altering the data transmitted between systems. Systems utilizing unencrypted or weak communication protocols become particularly vulnerable. For example, when delivery information is modified during transit, products may be misdirected, or fraudulent receivers may intervene. To prevent such risks, end-to-end encryption, secure communication protocols, such as TLS and SSL, and robust authentication mechanisms must be enforced. A TLS-based authentication mechanism has been proposed for Industry 4.0 supply chains to mitigate MitM attacks, significantly enhancing security while reducing the communication overhead by 50%. Test results confirmed the proposed method's resilience against MitM attacks [22].

4.3. Smart Contract Vulnerabilities and Manipulation Threats

While smart contracts employed in supply chains enhance trust and efficiency through decentralized and autonomous operations, they can also harbor vulnerabilities arising from programming errors or malicious attacks. Such vulnerabilities may result in data manipulation, a loss of funds, or operational disruptions within the supply chain.

- *Re-entrancy attacks*: Re-entrancy attacks occur when attackers exploit vulnerabilities in smart contracts by invoking a function multiple times before the target contract updates its state [65]. Within the supply chain context, malicious actors can manipulate payment processes or withdraw additional tokens from contracts. This poses a significant threat to secure payments or deliveries managed through smart contracts in supply chains.
- *Denial of Service* (*DoS*) *attacks*: DoS attacks disrupt the operation of smart contracts in blockchain systems, causing resource exhaustion and transaction delays. Attackers may execute transactions that consume excessive gas, preventing smart contracts from functioning properly, or overwhelm the mempool with unnecessary transactions, obstructing transaction verification [66]. In supply chain management, such attacks can disrupt critical processes, like product tracking, payment transactions, and inventory updates, causing delivery delays and inventory inaccuracies. To mitigate these risks, smart contracts should undergo rigorous security audits, gas limits must be optimized, and protections against spam transactions should be implemented.
- *Integer overflow/underflow*: Smart contracts utilized in supply chain management perform crucial calculations related to inventory tracking, product deliveries, and payments. However, vulnerabilities, such as programming errors and integer overflow or underflow, can lead to significant financial losses [67]. For example, a warehouse smart contract tracking inventory could generate incorrect inventory data due to integer boundary violations, spreading these inaccuracies throughout the supply chain. Attackers could exploit these calculation errors to gain unauthorized access, block order completions, or trigger unintended deliveries [68,69]. Integer boundary violations in Solidity may cause incorrect calculations by the Ethereum Virtual Machine (EVM) [68]. Since traditional tests are insufficient to detect these errors, secure mathematical libraries such as SafeMath or the automated error detection provided in Solidity version 0.8.0 should be utilized. Alternatively, a safer language such as Vyper may be preferred [70,71].

4.4. IoT Integration and Security Vulnerabilities

The increased use of IoT devices in blockchain-based supply chains has significantly enhanced the transparency, efficiency, and traceability of various operational processes, ranging from logistics to inventory management. However, the proliferation of IoT devices has simultaneously created an environment susceptible to widespread threats due to inadequate security measures within these devices. While blockchain technology provides critical advantages, such as data integrity and immutability, through its distributed ledger structure, ensuring the protection of IoT components at the edges of the supply chain and maintaining secure, continuous data flows represent a complex, multi-dimensional challenge.

- *DoS/DDoS attacks*: Denial of Service (DoS), one of the most prevalent and impactful attacks targeting IoT devices, aims to prevent legitimate users from accessing data and services promptly, typically by isolating devices from the network or exhausting available resources. Distributed Denial of Service (DDoS) attacks differ from DoS attacks in terms of the resources utilized to launch the attack. In DDoS attacks, multiple devices, such as desktop computers, servers, IoT devices, or other network-connected equipment, are simultaneously utilized to perform the attack [72–76], as depicted in Figure 5.

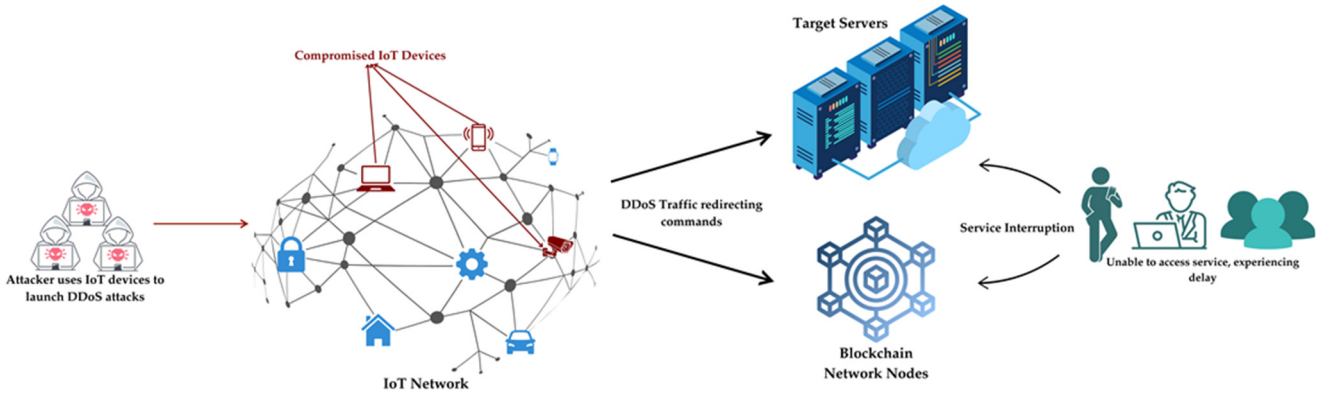

Figure 5. DDoS attack diagram in IoT network.

- *MitM attacks in IoT network*: MitM attacks occur during data transmission between IoT devices and the blockchain network, potentially leading to the theft or alteration of critical supply chain data. In these attacks, the attacker positions themselves between two IoT nodes, intercepts communication, and manipulates data flows by interacting with both parties [77]. IoT components commonly utilized in supply chains, such as RFID devices and smart sensors, are particularly susceptible to these attacks. Attackers can register falsified data onto the blockchain, manipulating the product origin, temperature monitoring, or delivery information. This may result in counterfeit products appearing authentic and severely compromising supply chain security. For instance, in a pharmaceutical supply chain, RFID tags and sensors record temperature data onto the blockchain. An attacker could intervene at the IoT node to inject false temperature data, causing improperly stored drugs to appear safe, potentially posing severe health risks. Implementing secure communication protocols and data encryption methods is essential to mitigate such attacks.
- *Spoofing attacks*: Spoofing attacks occur when malicious actors impersonate legitimate devices, users, or systems to gain unauthorized access [77]. These attacks utilize various methods, including IP spoofing, email spoofing, and targeting device authentication processes [78]. Attackers may deceive systems by transmitting falsified data packets or impersonating device identities to execute unauthorized operations. Spoofing attacks are especially common in IoT-based systems due to weaknesses in authentication mechanisms [77,78]. In blockchain-based supply chains, these attacks can manifest through the introduction of fake IoT devices or nodes that generate incorrect data. For example, counterfeit RFID readers or sensors integrated into a supply chain network could provide false information about the product location, temperature, or delivery status. Additionally, fake nodes might record inaccurate inventory data on the blockchain, manipulating stock levels or falsely indicating that non-existent products have been delivered. Such attacks compromise system integrity, causing reliability and transparency issues within supply chain processes.

5. Blockchain-Based Supply Chain Security Solutions and Integration Models

After discussing implementation challenges, this section presents various blockchain architectural models that offer practical design solutions tailored to SCM contexts.

Ensuring security in blockchain-based supply chains depends heavily on the blockchain architecture utilized, data privacy solutions, and integration mechanisms across different blockchain networks. Significant security differences exist between permissioned and permissionless blockchain models, while techniques such as ZKPs and confidential

transactions play a critical role in enhancing data privacy. Furthermore, interoperability between different blockchain networks and cross-chain security are essential for creating integrated supply chain structures.

5.1. Security Comparison of Permissioned and Permissionless Blockchains

Blockchains are classified into two main categories based on access control: permissioned and permissionless. Permissioned blockchains, such as Hyperledger Fabric, permit only authorized users to perform transactions, whereas permissionless blockchains, such as Bitcoin and Ethereum, allow open participation to anyone [79]. Sidechains bridge these two types of blockchains, increasing the transaction capacity and facilitating asset transfers. Table 5 provides a detailed comparative analysis between permissionless and permissioned blockchain systems, specifically highlighting Ethereum and Hyperledger Fabric as widely adopted representatives of these blockchain types.

Table 5. Comparative analysis of permissionless and permissioned blockchains.

Features and Security Criteria	Permissionless Blockchain	Permissioned Blockchain
Governance	Community-driven, open governance (Ethereum Developers).	Consortium-based governance (Linux Foundation).
Permission Structure	Open participation, no access restrictions.	Restricted participation, controlled access.
Application Domains	DeFi, NFTs, gaming, decentralized apps (dApps), public sector.	Supply chain, finance, healthcare, logistics, enterprise applications.
Consensus Mechanisms	Proof-of-stake (PoS), formerly proof-of-work (PoW).	Modular: Raft, Kafka, PBFT, customizable.
Smart Contracts	Solidity language, Ethereum Virtual Machine (EVM), widely decentralized.	Chaincode (smart contracts) written in Go, JavaScript, Java.
Data Privacy and Anonymity	Low privacy, pseudonymous transparency, fully transparent ledger.	High privacy, confidential transactions, channel-based privacy control.
Trust and Immutability	Fully immutable, trustless validation by all network nodes.	Controlled immutability, selective trust, transactions reversible by governance.
Attack Resistance	Risk of 51% attacks, computationally intensive	Reduced risk due to restricted participation
Data Integrity and Security	High (cryptographic validation, decentralized verification).	High (access control, stronger identity authentication).
Scalability	Lower transaction throughput (~15–30 TPS), limited scalability.	Higher transaction throughput (hundreds to thousands TPS), highly scalable.
Authorization and Access	No explicit authorization, open for all users.	Explicit authorization mechanisms, controlled user roles and permissions.
Operational Efficiency	Moderate (due to consensus mechanisms and decentralization).	High (fast transaction validation, lower latency).
Energy Consumption	Higher (especially PoW-based implementations), recently improved (PoS).	Lower, energy-efficient due to simplified consensus.

Permissionless blockchains are decentralized systems that are open to participation from any user without requiring a central authority. These systems typically utilize cryptographic consensus mechanisms, such as proof-of-work (PoW) or proof-of-stake (PoS), to achieve a consensus among nodes. Bitcoin pioneered this blockchain category by offering an immutable ledger for transparent and verifiable transactions. Other permissionless blockchains, such as Ethereum, enable more complex applications through smart contracts. However, permissionless blockchains face several challenges, including intensive computational requirements for transaction validation, limited transaction capacity, and concerns regarding data privacy [80].

Permissioned blockchains are closed systems that permit participation exclusively to authorized users, specifically designed for enterprise-level use. In these blockchains, network management is handled by selected organizations, and transactions can only be executed by verified participants. Such systems require the participants to identify themselves but do not necessarily require mutual trust [81]. Platforms like Hyperledger Fabric offer infrastructure suitable for enterprise applications due to high transaction throughputs and enhanced data privacy. However, the central control mechanisms slightly reduce decentralization [80]. Additionally, permissioned blockchains provide benefits such as faster transaction processing and lower energy consumption, thus offering improved operational efficiency compared to public blockchains [81].

Ethereum's key feature is its smart contract technology, allowing automatic program execution when predefined conditions are met via the Ethereum Virtual Machine (EVM). Ethereum's current consensus mechanism is proof-of-stake (PoS), which reduces energy consumption and offers improved scalability [82]. Additionally, Ethereum provides flexibility for creating and managing tokens through standards like ERC-20 and ERC-721, which are widely used in token-based projects and digital asset development [83].

Hyperledger Fabric, an open-source permissioned blockchain platform developed under the Linux Foundation's Hyperledger project, has been widely adopted for enterprise-level applications in areas such as supply chain management, finance, and healthcare [84,85]. Due to its permissioned structure, it restricts network participation to authorized entities, enabling secure and efficient transaction management. A notable feature of Hyperledger Fabric is its modular architecture, allowing the flexible integration of components with various roles and functions. Data privacy is facilitated through the concept of channels, permitting confidential data sharing exclusively among the designated participants. Furthermore, Hyperledger Fabric utilizes a programming model known as chaincode, similar to smart contracts, typically developed in languages such as Go, Java, or Node.js. This feature enables the automated execution of transactions [85].

5.2. Data Privacy with Zero-Knowledge Proof (ZKP) and Confidential Transactions

Blockchains are increasingly adopted in enterprise processes, such as trade finance, supply chain management, and contract execution. While companies prefer permissioned blockchains to protect commercial privacy, certain information must be transparently shared to ensure investor trust and traceability. In this context, striking a balance between commercial privacy and transparency is critical. To achieve this balance, transaction data can be protected through homomorphic encryption, while transparency can be maintained by employing zero-knowledge proofs. Thus, the validity of transactions can be verified without revealing sensitive information to unauthorized parties, and identities can be disclosed when necessary [86]. ZKP is a cryptographic technique that allows a prover to demonstrate the validity of a statement to a verifier without revealing any additional information. This mechanism ensures that the verifier can confirm the correctness of the provided information without accessing the underlying data itself [87].

ZKP protocols are grounded in three core mathematical properties: completeness, soundness, and zero-knowledge. These properties ensure that a party called the prover can convince another party, called the verifier of the truth of a statement, without revealing any information beyond the validity of the statement itself.

While these definitions originate in theoretical cryptography, they translate into critical functionality for supply chain systems where privacy, trust, and fraud resistance are operational priorities [87,88].

Completeness ensures that a valid statement is always accepted. In other words, if the stated claim is true, the verifier must always accept the proof, as defined in Equation (1):

$$\forall \in L,\ if\ P(x)\ is\ honest \Rightarrow V(x) = accept \tag{1}$$

where x represents an instance from the language, L; $P(x)$ is the prover generating the proof; and $V(x)$ is the verifier's decision. In supply chains, this guarantees that genuine data, such as IoT-recorded cold-chain temperature logs, will always be accepted by the verification system, supporting accurate compliance audits.

Soundness ensures that false claims are rejected with high probability. If the statement is false, the verifier must not accept fraudulent proof, as stated in Equation (2)

$$\forall \notin L,\ Probability[V(x) = accept] < \mathcal{E} \tag{2}$$

where $x \notin L$ denotes an invalid instance, and $\mathcal{E}$ is a negligible probability bound. This property is critical in preventing counterfeiters or malicious actors from introducing fraudulent data, such as fabricated certificates or falsified shipment origins.

Zero-knowledge ensures that no information is revealed beyond the validity of the claim. That is, the prover must not reveal any information other than proving that the statement is true, which is formalized in Equation (3):

$$\exists S : S(x) \approx View_v(P(x)) \tag{3}$$

where $S(x)$ is a simulator's output, and $View_v(P(x))$ denotes the verifier's view during the interaction with the honest prover, P. This protects commercial secrets within the supply chain. For instance, a manufacturer can prove that a delivery occurred within the agreed pricing terms, without revealing the actual price or contract details.

These foundational ZKP properties, though originating from theoretical computer science, address real-world challenges in supply chains. Table 6 presents the mathematical foundations of ZKP and maps each property to a direct implication in blockchain-based supply chain management. These properties serve as the foundational logic of zero-knowledge-based transaction verification in modern supply chains. Their applicability spans scenarios from pharmaceutical traceability to donor verification in humanitarian logistics. By enabling trust without disclosure, ZKP mechanisms enhance both privacy and operational integrity, which are increasingly vital under evolving systemic demands.

Table 6. Formal definitions of ZKP properties and their direct implications in blockchain-enabled supply chain management.

ZKP Property	Mathematical Definition	SCM Implication
Completeness	$\forall \in L,\ if\ P(x)\ is\ honest \Rightarrow V(x) = accept$	Valid supply data (e.g., temperature logs) from honest actors are always accepted.
Soundness	$\forall \notin L,\ Probability[V(x) = accept] < \mathcal{E}$	False claims (e.g., counterfeit goods) are reliably rejected by the verification.
Zero-Knowledge	$\exists S : S(x) \approx View_v(P(x))$	Business secrets (e.g., pricing, recipes) are protected while still proving validity.

ZKPs enable a proving party to demonstrate the truth of a statement to a verifying party without disclosing any additional information. In blockchain-based systems, ZKPs are widely used to preserve privacy, verify asset ownership, and facilitate secure authorization. For example, a user can prove their possession of a certain amount of funds without revealing the exact amount or transaction details [87,89,90].

Among ZKP variants, several protocol families have emerged with distinct trade-offs in terms of computational efficiency, cryptographic assumptions, and integration requirements. As illustrated in Figure 6, the most commonly implemented protocols in modern blockchain infrastructures are zk-SNARK, zk-STARK, Bulletproofs, and Ligero. These protocols all adhere to the core ZKP principles of completeness, soundness, and zero-knowledge, yet differ in how they achieve performance, scalability, and trust guarantees in practice.

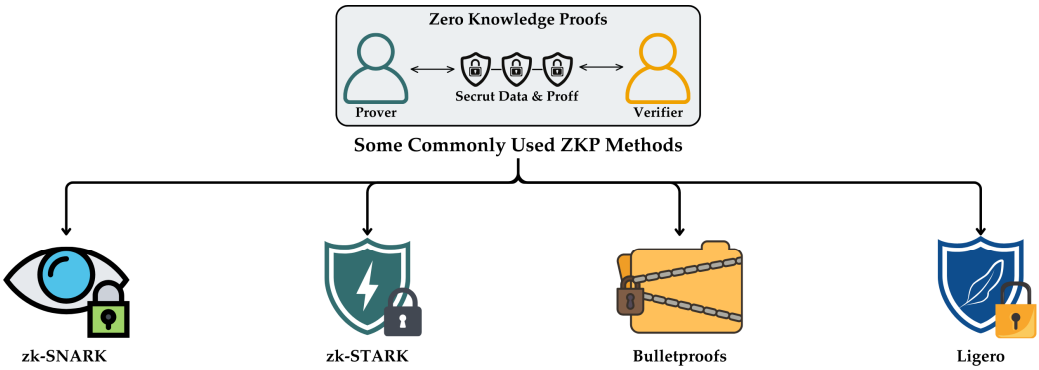

Figure 6. Widely used zero-knowledge proof protocols in blockchain systems.

While these protocols share the same foundational ZKP principles, their implementation profiles differ substantially. Factors such as proving time, verification efficiency, and trusted setup requirements directly affect their integration into blockchain-based supply chains [72,73]. Table 7 provides a quantitative comparison of these protocols, highlighting their suitability for diverse logistical and regulatory environments.

Table 7. Quantitative comparison of widely used ZKP protocols based on performance metrics and supply chain suitability.

Protocol	Proof Size (Byte)	Proving Time (ms)	Verification Time (ms)	Trusted Setup Req?	Quantum Resistant	SCM Suitability
zk-SNARK	(via Rust Language) 192 (15 rounds) 192 (4095 rounds)	(via Go Language) 1299 (15 rounds) 61,512 (4095 rounds)	(via Go Language) 1138 (15 rounds) 5733 (4095 rounds)	Yes	No	High: compact, fast verification, efficient, enterprise-ready, widely deployed, S/T/-
zk-STARK	6657 (15 rounds) 55,132 (4095 rounds)	0.552 (15 rounds) 44,876 (4095 rounds)	0.052 (15 rounds) 0.452 (4095 rounds)	Setup-free	Yes	Moderate–High: large size, quantum-safe, S/T/I
Bulletproofs	737 (15 rounds) 1249 (4095 rounds)	6756 (15 rounds) 3,614,500 (4095 rounds)	0.899 (15 rounds) 1,271,200 (4095 rounds)	Setup-free	No	Moderate–High: compact, setup-free, optimal for lightweight SCM, -/T/-

The SCM suitability classification reflects a multi-dimensional evaluation of each ZKP protocol's compatibility with supply chain requirements, taking into account both computational metrics (e.g., proof size, proving and verification times, trusted setup) and conceptual alignment with the three fundamental principles defined in the paper title: security, traceability, and data integrity (S/T/I).

zk-STARK demonstrates full alignment with all three principles (S/T/I), offering quantum resistance, transparency, and high verification performance. However, its large proof size and lower implementation maturity present integration challenges, especially in constrained environments, and is therefore considered Moderate–High in suitability.

Bulletproofs, while lacking quantum security and offering only partial integrity coverage, remain highly attractive for real-time, lightweight SCM use cases due to their compact-

ness, no setup requirement, and ease of integration. Their classification as Moderate-High (-/T/-) reflects this contextual strength despite certain technical limitations.

zk-SNARK, though lacking in transparency and quantum resistance, stands out with its ultra-compact proof size, mature tooling, and efficient verification, enabling cost-effective, fast, and scalable deployments. Its widespread adoption in real-world blockchain systems, like Ethereum and Zcash, reflects its maturity and readiness for enterprise-oriented supply chains, particularly in scenarios where efficiency and seamless integration are critical (S/T/-).

Beyond protocol-level comparisons, real-world blockchain platforms such as Ethereum are integrating zk-SNARKs and related mechanisms to enhance on-chain privacy [90]. Building upon these developments, Table 8 shows recent academic studies that explore the implementation of zero-knowledge proofs within blockchain-based supply chains. Protecting commercial confidentiality in supply chain processes is critical for maintaining the competitive advantage and data security. In traditional blockchain systems, transaction data are transparently recorded, making commercial agreements, pricing policies, and supply chain information publicly visible. This exposure can enable competitors to access strategic information and allow suppliers to gain bargaining power through price comparisons. To address these risks, the confidential transactions protocol was developed, ensuring that transaction amounts and party information remain accessible only to authorized users, while independently verifying the validity of transactions. Techniques such as homomorphic encryption, Pedersen Commitments, and Bulletproofs (all forms of ZKP) preserve transaction details while ensuring blockchain reliability and integrity.

Table 8. Comparative analysis of zero-knowledge proof studies in blockchain-based supply chains.

Ref.	Description	Advantages	Limitations
[87]	Secure traceability in industrial production using blockchain and ZKP.	Privacy, reliability, transparency, collaboration, auditability.	Cost, data reliability, scalability, standardization needs, blockchain security.
[91]	BeHSCM model enhancing privacy and security in healthcare supply chains using ZKP-enabled blockchain.	Privacy, authorization, security, automation.	Cost, scalability, integration, regulatory compliance.
[92]	Multi-chain blockchain model for grain supply chains.	Reduces data redundancy, reliable data sharing, preserves privacy.	Real-world integration difficulties, increased storage demands with large data volumes.
[93]	Secure data sharing and traceability in healthcare supply chains with blockchain, zk-SNARKs, and RBAC.	Security, privacy, transparency, access control, decentralization, low transaction cost.	Output privacy issues, inability to maintain identity anonymity, high computational cost, scalability challenges.
[94]	Using zk-SNARKs for protecting privacy in supply chains.	Decentralization, privacy, low cost, high efficiency.	Scalability, lack of incentives, security risks.
[95]	Data privacy in Quorum networks using ZKP.	Protection of trade secrets, safeguards against data manipulation, reliable transaction model.	High computational requirements, potential performance degradation, complex and costly development.

Confidential transactions achieve a balance between privacy and auditability in supply chains, protecting commercial information while allowing authorized auditors to validate transactions. For instance, a large retail company's private pricing agreements with various suppliers can be secured on the blockchain, ensuring visibility exclusively to authorized parties, thus maintaining competitive advantages. Additionally, these protocols minimize data security threats such as MitM attacks, protecting sensitive information from misuse. Conse-

quently, confidential transactions represent a crucial solution for enhancing commercial confidentiality and data security within blockchain-based supply chain systems [22].

A blockchain-based approach named B-CONFIDENT was proposed to ensure enterprise privacy in blockchain-based supply chains [96]. Using a permissioned blockchain architecture and smart contracts, the approach leverages PrivateFor and ConfidentialFor lists to restrict sensitive data access solely to authorized actors, ensuring transparency while preserving confidential information. Utilizing the GoQuorum platform and the Tessera private transaction manager, the method securely transmits transactions, relying on blockchain-based access controls instead of traditional public-key encryption methods for maintaining data privacy.

In SCM applications, especially in multi-stakeholder supply chains, achieving a balance between commercial data privacy and transparency is vital [91,94]. For example, information, such as pricing policies, special conditions in supply agreements, or quality control reports, needs to be verifiable without compromising confidentiality. Cryptographic approaches like ZKPs and confidential transactions provide trustworthy verification along the supply chain, allowing transactions without disclosing sensitive data to unauthorized parties [87,93,95]. Consequently, these methods protect competitive commercial secrets while ensuring regulatory compliance and internal trust. Ultimately, these cryptographic techniques not only enhance data security but also facilitate privacy-oriented designs within the digital transformation of SCM processes [86,90].

5.3. Cross-Chain Supply Chain Management Systems: Interoperability, Security Risks, and Architectural Design

In blockchain-based supply chain systems, interoperability is critically important for secure data and asset transfers between different blockchain networks [97]. Today, supply chains often involve blockchain solutions provided by various platforms, making cross-chain transactions inevitable [98]. For instance, a supplier might maintain records on a permissioned blockchain network based on Hyperledger Fabric, while a distributor or financial institution operates on a permissionless blockchain, such as Ethereum. Ensuring secure data and asset transfers between these systems is essential for maintaining supply chain integrity. However, interactions across different blockchain networks introduce vulnerabilities to cross-chain attacks, complicating the maintenance of fundamental security principles such as data integrity, authentication, and authorization.

Blockchain bridges are among the most prevalent applications facilitating cross-chain transactions. These bridges consist of smart contract mechanisms designed to transfer assets or data between two or more chains. However, these bridges can represent single points of failure and become attractive targets for attackers. Malicious actors can exploit vulnerabilities in bridge-based smart contracts, enabling unauthorized asset transfers or the manipulation of cross-chain transaction verification processes. Particularly, centralized or semi-centralized bridges are susceptible to large-scale security breaches. Recent high-profile blockchain bridge attacks have underscored the severity of these risks.

As demonstrated in Figure 7, security risks associated with cross-chain transactions can be summarized as follows: Centralized bridge structures rely on single verification mechanisms, making them attractive targets for attackers and introducing risks to cross-chain asset transfers. Attackers exploiting smart contract vulnerabilities may manipulate asset transfers, steal funds, or execute fraudulent transactions. Oracle manipulation poses another significant risk, enabling the introduction of false or fraudulent data into supply chain validation processes, potentially allowing counterfeit products to enter the system and reducing the overall reliability. If data security from oracles cannot be ensured, the integrity of the entire chain is compromised, creating opportunities for fraud. Additionally, incompatibility between consensus algorithms used by different blockchain networks may

introduce vulnerabilities during validation processes, complicating inter-chain interactions and negatively affecting system reliability [99].

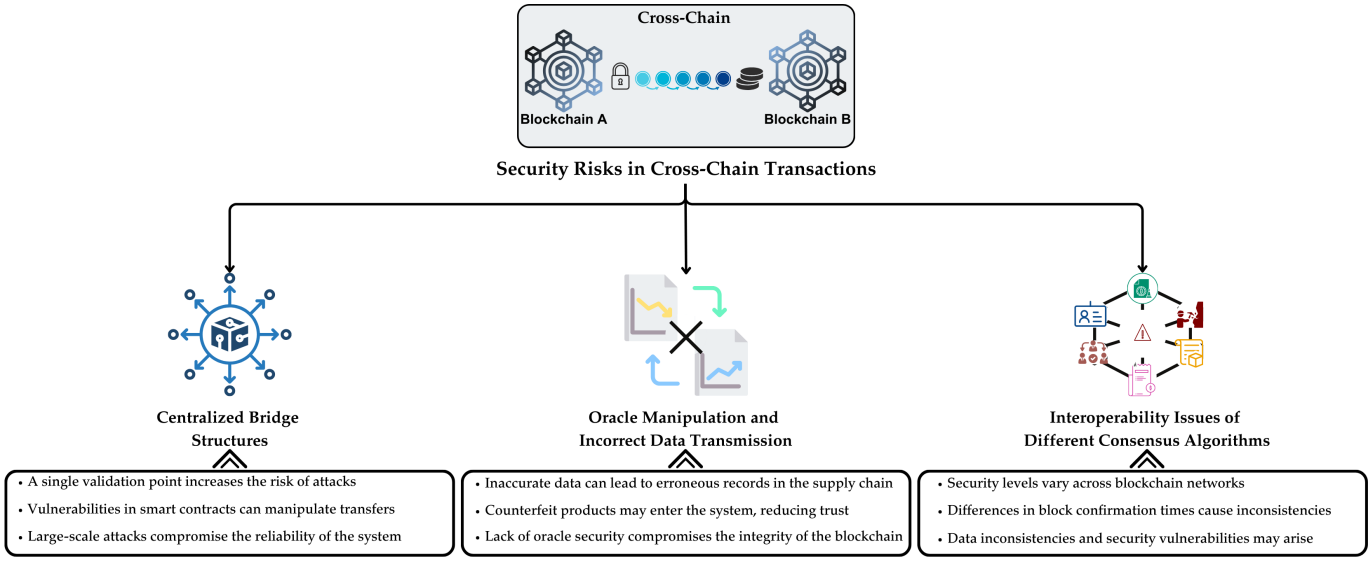

Figure 7. Classification of security risks in cross-chain transactions.

To mitigate these risks, cross-chain bridges should adopt decentralized verification mechanisms. Techniques such as multi-signature and threshold encryption can enhance security by preventing a single authority from gaining control over cross-chain transaction validations. Additionally, secure software development processes such as formal verification can be employed to identify vulnerabilities in cross-chain smart contracts. Auditing smart contract codes helps detect potential security risks, such as re-entrancy attacks and integer overflow/underflow, in advance.

Regarding oracle security, it is essential to adopt distributed oracle architectures. Instead of relying on a single centralized oracle provider, utilizing multiple independent oracle sources can increase the accuracy and reliability of data. Moreover, integrating cryptographic techniques, such as ZKP, can verify whether the oracle-provided data have been altered or tampered with. These methods reinforce data integrity within supply chains and help prevent fraud attempts. A parallel blockchain and smart contract-based cross-chain model for rice supply chain auditing has been proposed, employing a combination of hash lock + smart contract + relay-chain to secure data sharing. The K-means algorithm and SPBFT consensus mechanism improve the transaction speed and reliability, achieving lower costs, reduced latency, and effective auditing [100]. Similarly, an SCT-CC traceability system based on cross-chain technology utilizing Hyperledger Fabric with smart contracts and a multi-chain architecture has been proposed, significantly enhancing data integrity, transparency, and security. Testing results demonstrated query speeds of 110 TPS and write capabilities of 102 TPS, indicating the system's scalability and applicability [101].

5.3.1. Comparative Evaluation of Cross-Chain Interoperability

In blockchain-based supply chains, cross-chain protocols do not merely serve as communication bridges between networks: they fundamentally shape how data security, transparency, and operational integrity are maintained across enterprise boundaries. To this end, Table 9 offers a multi-dimensional analysis that connects technical properties with real-world supply chain requirements, particularly through the lens of the STI (security, traceability, and integrity) framework.

Table 9. Cross-chain interoperability comparison for SCM.

System	Oracle Security	Attack Risk	TPS	Delay (ms)	STI Alignment	SCM Suitability
Chainlink Bridge	Moderate	High (3.1)	30	140	S/–/T	Moderate
Polkadot XCMP	High	Medium (2.5)	1000	80	S/T/I	High
Cosmos IBC	High	Low (2.2)	800	50	S/T/I	High
ZKP-Based Custom Bridge	Very High	Very Low (1.2)	100	180	S/–/I	Moderate–High

Chainlink-based bridges, on the other hand, offer flexibility and existing adoption advantages but suffer from centralized oracle risks and limited throughput, reducing their alignment with data integrity (I) and real-time traceability. As a result, they are rated Moderate, better suited to non-critical or loosely coupled supply chain components where interoperability is secondary to availability [102]. Polkadot XCMP and Cosmos IBC are rated as highly suitable due to their robust decentralized architectures, low latency, and support for parallel validation. These properties make them ideal for real-time traceability (T), data consistency (I), and low-risk authentication (S), all of which are fundamental in large-scale logistics, perishable goods tracking, or international trade compliance [103,104]. ZKP-based custom bridges, while slightly limited in throughput and latency, offer exceptionally strong privacy guarantees and cryptographic security. These make them ideal in sensitive SCM scenarios involving proprietary data or regulatory requirements for confidential auditing, such as pharmaceutical or defense supply chains. Their Moderate–High rating reflects this domain-specific strength, despite lower general scalability [105,106]. Importantly, the SCM suitability column in Table 9 is not a replication of STI alignment, but a practical synthesis, incorporating protocol maturity, real-world integration feasibility, and responsiveness to SCM-specific demands. This separation allows researchers and practitioners to distinguish between theoretical alignment and operational fitness.

5.3.2. Architectural Model for Cross-Chain Supply Chains and Smart Contract Design

As supply chains evolve into decentralized, multi-stakeholder ecosystems, ensuring interoperability between different blockchain platforms has become a functional necessity. Traditional single-chain deployments fall short when actors operate on separate permissioned and permissionless networks.

Figure 8 presents a proposed conceptual cross-chain architecture that facilitates secure and verifiable data exchange between heterogeneous blockchain networks through a Chainlink bridge and ZKP validation mechanisms. This architecture operationalizes the core principles of security, traceability, and integrity (STI) within real-world supply chain contexts [87,89].

In this model, data flows between distinct blockchain domains are mediated by the bridge, which serves as a transport and interoperability layer. Information such as inventory records, production details, delivery confirmations, and payment requests can be exchanged across chains through cryptographically verified oracle inputs, ensuring accurate and trusted data transfer [55,56].

The ZKP Validator ensures that transactions are validated without exposing sensitive data, preserving commercial confidentiality and enabling secure contract enforcement. This mechanism, depicted as the ZKP Validator layer in the center of the architecture, also reduces reliance on trusted intermediaries and strengthens the privacy model [87,89–91].

The architecture embeds the three fundamental principles of STI as follows:

- Security is enforced through cryptographic mechanisms and ZKP-based validation, ensuring that data remain tamper-proof and accessible only to authorized parties during cross-chain operations [91,92]. While platforms like Hyperledger Fabric natively support

authentication and access control, this model incorporates additional authentication and access control mechanisms, explicitly illustrated in the center of the architecture, to ensure secure and policy-compliant data exchange at the cross-chain layer. These controls are especially critical at the bridge and ZKP validation stages, where heterogeneous blockchain systems interact and trust boundaries must be enforced.

- Traceability is achieved by maintaining end-to-end audit trails, enabling all stakeholders to track assets, documents, and transactional states across multiple chains in real time [87,89].
- Integrity is preserved via immutable ledger entries and consistency validations, ensuring the accurate reconciliation of supply chain activities [4,43].

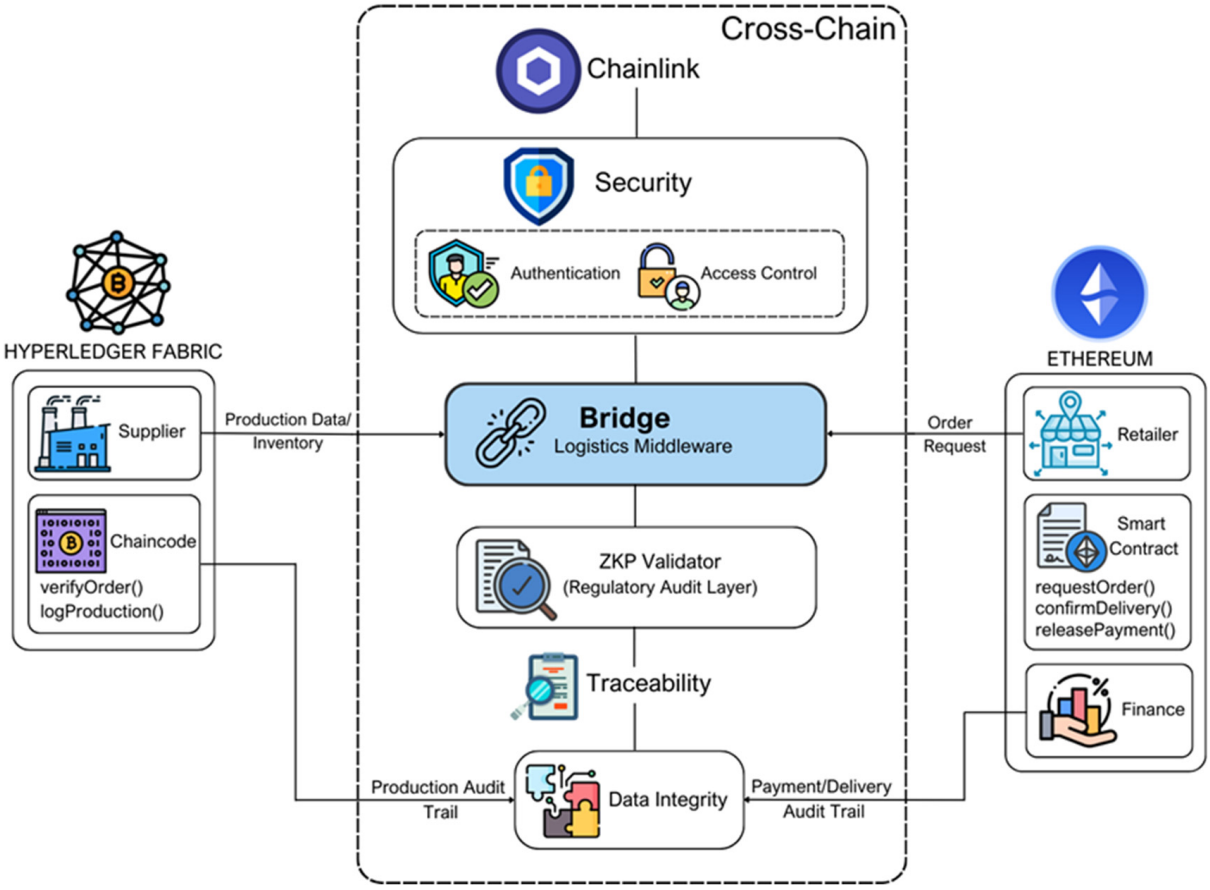

Figure 8. Conceptual cross-chain architecture for blockchain-based supply chain management, illustrating how permissioned and permissionless platforms can securely exchange data through interoperability layers. In this example, Hyperledger Fabric and Ethereum are connected via a Chainlink bridge with zero-knowledge proof validation, supporting the principles of security, traceability, and integrity (STI).

This model supports hybrid ecosystems where different organizations retain their preferred blockchain infrastructure while maintaining interoperability, visibility, and regulatory compliance across the network [48].

To further clarify the operational flow of the cross-chain supply chain architecture demonstrated in Figure 8, this section introduces a set of representative pseudocode functions executed on both permissioned and permissionless blockchain platforms. These logic components embody the automation backbone of decentralized supply chain ecosystems, handling verification, logging, validation, and payment release processes across blockchain domains.

On the Hyperledger Fabric side, internal functions, such as *verifyOrder*() and *logProduction*(), ensure the correctness of orders and the integrity of production events, protecting private business logic from external exposure. Meanwhile, on the Ethereum side,

outward-facing processes, including *requestOrder*(), *confirmDelivery*(), and *releasePayment*(), are executed as smart contracts, often triggered by cross-chain events and external data sources, such as oracles or zero-knowledge proof verifiers.

These components, as further detailed in Algorithms 1 through 5, are designed to work synergistically through the Chainlink bridge, which orchestrates secure data exchange and enables trustless validation between disparate networks. By linking smart contracts and chaincode modules across blockchain layers, the system not only ensures interoperability and traceability but also satisfies core requirements of security, traceability, and integrity (STI) in distributed SCM systems.

What follows is a breakdown of five core functions, each of which corresponds directly to a process stage depicted in Figure 8. These algorithms are intentionally abstracted for clarity, yet they reflect realistic logic structures used in practical blockchain applications. Their role in managing decentralized operations is explained below, prior to the pseudocode listings.

The following pseudocode routines illustrate typical operations executed on each side of the system. These are simplified abstractions, serving to demonstrate how logic components are structured around key supply chain events. The integration of oracle inputs and cryptographic proofs, such as ZKPs, further strengthens trust and auditability.

Algorithms 1 and 2 are executed on the permissioned blockchain (Hyperledger Fabric), modeling the internal logic of supply chain actors such as suppliers or auditors.

Algorithm 1. *verifyOrder*()

```
Input: orderID, productID, quantity
Output: Boolean
 if not isAuthorized(caller) then
     return false
 endif
 order ← getOrderDetails(orderID)
 if order.productID ≠ productID or
 order.quantity ≠ quantity
 then
     return false
 endif
 if checkInventory(productID) < quantity then
     return false
 endif
 logAuditTrail("Order verified", orderID)
 return true
```

Algorithm 1: *verifyOrder*() corresponds to the initial step in the supplier network, where an internal chaincode function validates incoming orders. It ensures that the caller is authorized, the product and quantity match expectations, and sufficient inventory is available. This verification step is essential for establishing trust before engaging in cross-chain interaction.

Algorithm 2: *logProduction*() reflects the supplier's internal process of logging production data on a permissioned ledger. This function records batch-specific metadata with a timestamp, providing a verifiable trace for downstream auditing. In Figure 8, this corresponds to the flow of production data from the supplier to the bridge.

Algorithms 3–5 represent public smart contracts deployed on the Ethereum blockchain.

Algorithm 2. *logProduction*()

```
Input: batchID, productID, timestamp
Output: Boolean
 if batchIDExists(batchID) then
    return false
  endif
  if timestamp = null then
     return false
  endif
  productionRecord ← {
   batchID: batchID, productID:productID,
   timestamp: timestamp, status: "Completed" }
  success ← ledger.append(productionRecord)
  if success = false then
    return false
  endif
  return true
```

Algorithm 3: *requestOrder*() is executed on the public blockchain side, where a retailer (or other requester) initiates an order. By emitting a verifiable event and updating the requester's status, this function creates a signal that can be captured by the bridge and verified against internal order records.

Algorithm 4: *confirmDelivery*() captures the delivery validation phase. After the shipment is completed, an oracle fetches delivery proof from an external system. This function verifies that the data are authentic before confirming delivery and emitting a confirmation event. This step strengthens traceability by linking physical delivery data with on-chain commitments.

Algorithm 3. *requestOrder*()

```
Input: productID, quantity
Output: Boolean
  if productID = null or
    quantity ≤ 0
    then
        return false
    endif
    if not isWhitelisted(sender)
    then
        return false
    endif
    emit OrderRequested(
        sender,
        productID,
        quantity)
    status[sender] ←
    "PendingVerification"
     return true
```

Algorithm 4. *confirmDelivery*()

```
Input: orderID, deliveryProof
Output: Boolean
  if orderID = null or
   deliveryProof = null
   then
      return false
   endif
   if verifyOracle(deliveryProof)=false
   then
      return false
   endif
   deliveries[orderID] ←
   "Confirmed"
    emit
    DeliveryConfirmed(orderID)
    return true
```

Algorithm 5. *releasePayment*()

```
Input: orderID, zkProof
Output: Boolean
  if orderID = null or zkProof = null then
    return false
  endif
  if verifyZKP(orderID, zkProof) = false then
    return false
  endif
  amount ← calculateAmount(orderID)
  recipient ← supplier[orderID]
  if recipient = null or amount ≤ 0 then
    return false
  endif
  success ← transfer(recipient, amount)
  if success = false then
    return false
  endif
  emit PaymentReleased(orderID)
  return true
```

Algorithm 5: *releasePayment*() addresses privacy-preserving payments and represents the final phase in which a ZKP-enabled validation is required before any payment is issued. After verifying the zero-knowledge proof associated with order fulfillment, the contract initiates the payment transfer. This step encapsulates both integrity and privacy, with the payment being conditional on verifiable fulfillment, without exposing sensitive logistical details.

6. Sectoral Supply Chain Applications: Areas Secured by Blockchain Technology

Blockchain technology is increasingly adopted to ensure supply chain security across various industries. In sectors such as logistics, agriculture, healthcare, pharmaceuticals,

food, and retail, blockchain addresses critical security concerns such as data integrity protection, counterfeit prevention, ensuring traceability, and secure data sharing. Smart contracts, distributed ledger architectures, and cryptographic verification mechanisms make supply chain processes more secure and transparent.

Table 10 summarizes the security issues and proposed solutions addressed by blockchain-based approaches within various industry-specific supply chains.

Table 10. Sectoral applications of blockchain-based security solutions in supply chain management.

Sector	Ref.	Security Issue	Blockchain Solutions
Logistics	[107]	Data integrity, traceability, vulnerabilities, risk management.	Distributed ledger, cryptography, smart contracts, MCDA-based decision framework.
	[108]	Data security, data integrity.	Cryptography, consensus mechanisms, smart contracts.
	[109]	Fraud and manipulation.	Smart contracts, permissioned blockchain, DLT.
	[110]	Transaction fraud, data manipulation, traceability.	Smart contracts, DLT.
	[111]	Data manipulation, counterfeiting, traceability.	Smart contracts, DLT.
Agriculture	[95]	Transparency and security in agricultural SCM.	Quorum network, smart contracts.
	[112]	Product traceability, data security.	Blockchain, MetaMask integration.
	[113]	Resource and quality monitoring.	Ethereum, smart contracts, cryptography.
	[114]	Data manipulation, counterfeiting, data storage.	Redactable blockchain, IPFS.
	[115]	Data manipulation, counterfeiting.	Ethereum-based ERC-721 smart contracts, NFT-based unique identifiers.
	[116]	Data integrity, traceability, and transparency.	Blockchain-based system, smart contracts.
	[117]	Fake seeds, data manipulation, intermediary fraud, record loss, unfair logistics competition.	Ethereum network, NFT-based traceability, smart contracts, transparent auction system, immutable records.
	[118]	Data manipulation, counterfeiting, lack of traceability, secure payments, central data storage risks, price manipulation.	Smart contracts, Rice Coin (RC), IPFS.
Healthcare	[119]	Patient data, medicine tracking	Hyperledger Fabric, access control, encryption.
	[120]	Data privacy, integrity, authorization, and traceability.	Hyperledger Fabric, asymmetric encryption, smart contracts, decentralized data storage.
	[121]	Data manipulation, unauthorized sharing.	Private and permissioned blockchain, smart contracts, PoW, hash functions.
	[122]	Data integrity, unauthorized access, privacy violation.	Permissioned blockchain immutability, digital certificates, smart contracts.
	[123]	Medicine source tracking.	Ethereum, smart contracts, NFT.
	[124]	Data privacy and integrity, manipulation, traceability.	Hyperledger Fabric smart contracts, DLT, PBFT, private blockchain network.
Pharmaceutical	[125]	Data integrity, authorization, accessibility, MitM attacks.	Ethereum-based blockchain platform, smart contracts, off-chain, MSMA and MSA tokens.
	[126]	Fake vaccines, data integrity.	dPoW, scalable blockchain.
	[127]	Lack of interoperability, lack of data standardization, data manipulation, counterfeiting, data storage.	Verifiable credentials, off-chain, standardized data formats.
	[128]	Drug counterfeiting, manipulation.	DLT, smart contracts, hash functions.
	[129]	Drug counterfeiting.	Hyperledger Fabric, SI-HLLR, DLT.

Table 10. *Cont.*

Sector	Ref.	Security Issue	Blockchain Solutions
	[130]	Counterfeit drug production, manipulation, incorrect distribution points.	Hyperledger Fabric-based private blockchain, chaincode.
	[131]	Fake vaccines, lack of traceability, data manipulation.	Hyperledger Fabric.
	[132]	Preventing pharmaceutical counterfeiting and data manipulation.	Ethereum-based consortium blockchain, smart contracts.
Food	[133]	Oil counterfeiting, data manipulation, traceability.	Ethereum blockchain, smart contracts.
	[134]	Data manipulation, food safety, privacy, authorization, smart contract security.	Cryptographic hash functions, chain structure, permissioned blockchain.
	[135]	Counterfeiting, mislabeling, product safety.	Proof-of-work.
	[136]	Data manipulation, counterfeiting, imitation.	Immutable records; decentralized, verifiable transactions.
	[137]	Unauthorized access, data manipulation.	On-chain and off-chain, consensus algorithms.
	[138]	Data security.	AES-256, PBFT.
	[139]	Data loss, data manipulation, counterfeiting.	Hyperledger Fabric, decentralization, storing hash values in blocks.
	[140]	Data manipulation, counterfeiting, food safety and quality.	Ethereum-based smart contracts, Ethereum Virtual Machine, PoS.
	[141]	Grain traceability.	Public blockchain, Ethereum, IPFS, ML-based validation.
	[142]	Manipulation and counterfeiting, data security, lack of standardization.	Permissioned blockchain, smart contracts.
Retail	[143]	Data manipulation and counterfeiting, cyber-attacks, erroneous and incomplete records, financial risks.	BIOT, smart contracts, DLT.
	[144]	Data manipulation, counterfeiting, traceability.	DLT, blockchain.
	[145]	Cyber-attacks, counterfeiting and data manipulation, fraud.	DLT, smart contracts, immutability.

6.1. Blockchain Applications in Humanitarian Supply Chains: Real-World Case Study Examples

While Section 6 offers a broad perspective on blockchain applications across various industrial sectors, this section focuses specifically on humanitarian logistics and donation-based scenarios, where the ethical, urgent, and socially impactful nature of operations necessitates a distinct analytical context.

Humanitarian supply chains operate under extreme constraints, often in contexts of natural disasters, armed conflicts, refugee crises, or health emergencies. These supply chains require rapid deployment, real-time coordination among diverse actors, and a high degree of trust and transparency. Traditional systems are frequently hindered by fragmented data sharing, a lack of traceability, and the potential misuse of resources.

Blockchain technology has emerged as a potential enabler of secure, transparent, and accountable systems in humanitarian logistics. By leveraging decentralized architectures and immutable record-keeping, blockchain can ensure that aid, donations, and critical supplies are delivered to the right place, at the right time, and to the right people. In this section, we examine the application of blockchain in key humanitarian domains, including disaster relief, refugee logistics, pandemic responses, and charitable donation tracking. Each subdomain is evaluated in terms of its approach to security, traceability, and data integrity, the core dimensions explored throughout this review.

6.1.1. Blockchain Applications in Disaster Relief Supply Chains: Transparency, Traceability, and Trust

Ensuring the transparent, reliable, and traceable delivery of humanitarian aid in disaster-stricken areas is among the most complex and critical components of the supply chain. Traditional systems are often plagued by challenges, such as the misuse of donations, material loss, a lack of visibility, and poor coordination among stakeholders. In response to these shortcomings, blockchain technology has been increasingly integrated into humanitarian logistics to enhance trust, traceability, and data integrity [146,147]. Table 11 provides a comparative overview of blockchain-based humanitarian aid applications, detailing their core focus areas, employed technologies, and the specific security, traceability, and data integrity features they implement, while also highlighting the technical challenges encountered in practice.

Table 11. Evaluation of blockchain-based disaster relief studies by security, traceability, and data integrity.

Ref.	Application Focus	Blockchain Role	Key Technologies	Technical Challenges	Security Feature	Traceability Feature	Data Integrity Feature
[146]	Disaster relief donation logistics.	Permissioned blockchain for coordination and transparency.	Role-based access control, stakeholder nodes.	Multi-party coordination, fraud prevention.	Role-based stakeholder authentication.	Donor-to-recipient ledger tracking.	Immutable ledger records (platform unspecified).
[147]	Optimizing disaster supply chain with decision logic.	Smart contracts for execution of supply logic.	Neutrosophic programming, multi-objective modeling, smart contracts.	Logistics optimization under uncertainty.	Smart contract enforcement.	Contract-level transaction flow.	Immutable contract execution logs.
[148]	SCP design for long-term crises.	Conceptual model only.	System-level protection logic (no blockchain platform).	SCP protection and resource flow resilience.	Conceptual access control.	Abstracted stakeholder mapping.	Not technically validated.
[149]	Transparency in aid distribution.	Simulated blockchain model.	Voucher–token logic, simulated chain (no platform).	Distribution transparency, agency accountability.	Simulated security model.	Token-based aid tracking.	Basic simulated immutability.
[150]	Post-disaster resource management.	Node-based decentralized architecture design.	Stakeholder roles, proposed node logic (platform unspecified).	Resource coordination, system decentralization.	Suggested access policies.	Aid path visual representation.	Theoretical immutability.
[151]	Donation management in disaster response.	Public blockchain for donor verification and fund transparency.	Ethereum, smart contracts, DApp frontend.	Misuse of funds, donation tracking.	Ethereum-based smart contract validation.	Donor-to-project transaction history.	Fully auditable chain records.
[152]	Relief SC design with risk and robustness analyses.	Optimization model with blockchain suggestion.	Multi-layered SCP model (platform not implemented).	Risk-tolerant SC routing.	Model includes conceptual resilience logic.	Risk-based node flow modeling.	No concrete ledger or system.

Table 11. *Cont.*

Ref.	Application Focus	Blockchain Role	Key Technologies	Technical Challenges	Security Feature	Traceability Feature	Data Integrity Feature
[153]	Blockchain in disaster management systems (review paper).	General overview of disaster BC uses.	Review of 28 studies, various platforms.	Conceptual SC transparency.	Summarized by studies.	Multiple case references.	General overview, not implemented.
[154]	Food SC resilience in disaster via Industry 5.0 tools.	Smart contracts and IoT for resilient SC.	Industry 5.0 integration, Ethereum-based architecture.	SC adaptability, disruption mitigation.	Smart device integration with smart contracts.	Real-time tracking of food shipments.	Resilient ledger structure.
[155]	Transparency in donations to disaster zones.	Public DApp for donation campaign tracking.	Polygon (EVM-compatible), smart contract, Metamask frontend.	Campaign-level traceability.	Smart contract + digital wallet validation.	Donation trace from donor to project.	Immutable EVM-based logging.
[156]	Medical relief SC during pandemics.	IoMT platform integrated with blockchain.	IoT sensors, Blockchain ledger.	Cold-chain distribution integrity.	Sensor validation and access policy.	End-to-end item flow.	Environmental + ledger validation.
[157]	Disaster risk management and preparedness.	Blockchain to enhance transparency, trust, and coordination in disaster phases.	Smart contracts, decentralized data management, consensus protocol.	Multi-agency coordination, data sharing, system scalability.	Decentralized access control, tamper-resistance.	Multi-agency coordination, data sharing, system scalability.	Immutable ledger of disaster operations.
[158]	Lightweight disaster relief distribution (DTN).	Blockchain + smartphones in ad hoc networks.	Ethereum, DTN, phone-to-phone syncing.	Communication breakdown resilience.	Smart contract-based verification.	Physical package + contract mapping.	Immutable TX data.
[159]	Decentralized humanitarian aid governance.	Ethereum-based governance and routing.	Smart contracts, fund traceability, multi-stakeholder system.	Coordination without central control.	Cryptographic address and smart contract control.	Household-level aid path.	Smart contract state proof.

In particular, blockchain has been utilized in donation workflows to provide secure and traceable architectures through role-based access control [146], smart contract-enforced fund governance [147,151,155], and end-to-end ledger records [151,154,157]. Some studies propose conceptual frameworks without specifying a platform [148–150,152], while others have implemented Ethereum or EVM-compatible DApps for real-time tracking [151,155,158,159]. For instance, a donation monitoring platform based on Ethereum allows stakeholders to transparently track how each contribution is transferred to a beneficiary [151]. Similarly, a Polygon-based solution integrates wallet applications and smart contracts to enable donation traceability across campaigns [156].

Several studies further enhance transparency by combining blockchain with IoT technologies, enabling the real-time monitoring of aid materials under environmental conditions [154,156]. This integration secures not only the digital transaction history but also the physical movement and storage conditions. Lightweight blockchain architectures that utilize smartphone-based peer-to-peer synchronization have also been proposed to

function even in the absence of infrastructure [158]. On the other hand, certain contributions remain at the conceptual level or provide limited technical depth. Systematic reviews and framework papers contribute to the literature from a theoretical perspective without implementing real systems [153]. Models lacking platform specification or concrete implementation often fall short in terms of technical soundness for security and data integrity [148–150]. Additionally, complex requirements, such as off-chain data integration, cold chain monitoring, or scenario-based donation routing, are either minimally addressed or entirely omitted in several works [152,156]. Overall, blockchain-enabled supply chain applications exhibit significant potential in strengthening transparency, traceability, and data integrity in disaster responses. A hybrid architecture combining permissioned blockchain platforms (e.g., Hyperledger Fabric) with public systems (e.g., Ethereum, Polygon) may offer both scalability and operational security.

6.1.2. Refugee Logistics and Identity Management

Refugee logistics pose a dual challenge: ensuring access to humanitarian aid and enabling secure, verifiable identity management for displaced populations. Refugees often arrive in host countries without valid identification or having lost documents during the migration. Traditional centralized identity systems are ill-equipped to handle such scenarios, especially across borders. Blockchain technology has emerged as a transformative tool to address these limitations by enabling tamper-proof, decentralized identity verification mechanisms. Various approaches have been introduced to empower refugees through Self-sovereign identity (SSI) frameworks, digital certificates, and decentralized identity wallets. One implementation in Switzerland employed a blockchain-based SSI platform to enhance identification processes for Ukrainian refugees by eliminating paper dependency and enabling individuals to control their own identity data [160]. Another solution utilized Ethereum-based smart contracts to issue verifiable educational and employment certificates through immutable digital records [161].

Ensuring access to vital records, such as health, education, and identity documents, for refugees, especially children, has been recognized as a key challenge in displacement contexts. Blockchain-based systems have been proposed to address this gap by enabling the decentralized and tamper-proof storage of such documents, even in regions with limited infrastructure, thereby reducing the risk of long-term exclusion for vulnerable populations [162].

Regulatory and ethical challenges, such as the absence of unified legal frameworks, continue to limit the broader adoption and deployment of these systems [163]. Many implementations in this field remain at the proof-of-concept stage, lacking scalability and long-term viability. Some projects have been critiqued for prioritizing funding appeal over addressing underlying systemic issues [164]. These initiatives highlight the potential of blockchain to enhance security, traceability, and data integrity in refugee logistics and identity management. However, challenges related to interoperability, adoption barriers, and regulatory compliance persist. Table 12 presents key contributions and gaps identified across the reviewed studies.

Table 12. Summary of blockchain-based identity and logistics applications for refugees.

Ref.	Application Focus	Blockchain Role	Key Technologies	Technical Challenges	Security Feature	Traceability Feature	Data Integrity Feature
[160]	Refugee identity via SSI (Ukraine; Switzerland).	Self-sovereign identity (SSI) wallets for refugees.	GaaP architecture, digital ID.	Scalability, cross-organization integration.	Private key protection, user-controlled access.	Credential issuance and access logs.	Immutable storage of verified ID records.

Table 12. *Cont.*

Ref.	Application Focus	Blockchain Role	Key Technologies	Technical Challenges	Security Feature	Traceability Feature	Data Integrity Feature
[161]	Certificate generation and validation (India).	Smart contract-based digital certificate issuance.	Ethereum, DID.	Legal validity, cross-border interoperability.	On-chain access permissions.	Credential usage logs via transaction history.	Certificates anchored to unalterable contract state.
[162]	Refugee logistics and identity management.	Decentralized coordination of aid distribution and identity.	Smart contracts, digital ID, DLT platforms.	Lack of infrastructure, corruption in aid processes, ID verification, cross-border aid coordination.	Encrypted digital ID systems and access control.	Blockchain-based tracking of aid/resource allocation across actors.	Immutable storage of identity and aid records using decentralized ledger.
[163]	Refugee child records across borders.	Interoperable ID/health/education system (conceptual).	Cross-border storage vision.	Portability, lack of global record linkage.	Conceptual only.	Theoretical chain of personal history tracking.	Not realized technically.
[164]	Biometric aid delivery pilot (camps).	Blockchain-linked biometric wallets for aid verification.	Biometrics, smart wallets.	Pilot lacked metrics, governance gaps.	Identity matched to biometric hash.	Transaction logs of aid interactions.	Immutable record of aid disbursement.

6.1.3. Pandemic and Medical Relief Logistics

The COVID-19 pandemic exposed critical vulnerabilities in global medical supply chains, including widespread shortages, delays, and the proliferation of counterfeit medical products. In these frameworks, blockchain technology has been rapidly explored and adopted as a means to improve the security, traceability, and data integrity of pandemic-related logistical processes. From vaccine distribution and personal protective equipment (PPE) tracking to cold-chain monitoring for pharmaceuticals, blockchain-enabled systems demonstrated measurable impacts in enhancing transparency and coordination across global and local supply networks [165,166].

Several studies investigated blockchain's role in maintaining cold-chain compliance, particularly for temperature-sensitive supplies. For example, one system implemented smart contracts to automatically verify that pharmaceuticals were transported under proper conditions, logging every event on-chain and issuing alerts upon threshold violations [165,166]. In other cases, smart contracts were integrated with QR codes and IoT sensors to confirm supply authenticity and enforce regulatory compliance [167]. These efforts notably improved stakeholder trust, auditability, and response times. In addition, blockchain has been applied to support vaccine supply network design, helping address route instability and fluctuating demand across logistics partners [168]. Emerging approaches also explored the fusion of AI with blockchain to forecast supply demands using social data, contributing to more responsive pandemic logistics strategies [11]. From a security perspective, blockchain provided protection against data tampering and the unauthorized manipulation of supply records. For traceability, distributed ledger technologies ensured continuous visibility from manufacturers to points of care, enabling real-time validation of origin, handling, and delivery milestones. In terms of data integrity, immutability and consensus mechanisms facilitated transparent, verifiable, and auditable records: critical features for post-crisis evaluation and policy development.

However, as summarized in Table 13, these systems often faced technical limitations, such as interoperability with legacy health information systems, the high energy consumption of public chains, data latency, and challenges in scaling across jurisdictions. While pilot deployments demonstrated promise, many lacked mature governance models or widespread adoption beyond proof-of-concept stages. Nevertheless, the pandemic served as a global stress test for blockchain-enabled medical supply chains, offering valuable lessons for future crisis preparedness and logistics resilience.

Table 13. Selected blockchain-based solutions for enhancing pandemic-era medical supply chains.

Ref.	Application Focus	Blockchain Role	Key Technologies	Technical Challenges	Security Feature	Traceability Feature	Data Integrity Feature
[165]	Emergency dispatch with cold-chain control.	Route compliance and environmental monitoring.	GPS, IoT temperature tags.	Spoilage prevention, route compliance.	Smart alerts on threshold violations.	Timestamped route and status logs.	Immutable status history with environmental metadata.
[166]	Emergency cold-chain medicine logistics.	Smart contracts for condition tracking and alerts.	IoT sensors, HACCP, smart contracts.	Real-time anomaly detection, cold-chain compliance.	Tamper-proof monitoring via smart contract rules.	Real-time sensor logs of shipment status.	Automated validation with immutable logs.
[167]	Transparency in PPE/medicine supply chains.	Product verification and compliance logging.	QR codes, hybrid consensus.	Counterfeit prevention, visibility gaps.	Anti-counterfeit validation using smart contract logic.	Unique QR-linked transaction chains.	On-chain event logging and proof of delivery.
[168]	Vaccine supply network design.	Blockchain logging of distribution flow.	Hybrid logistics, optimization.	Route instability, fluctuating demand.	Not explicitly implemented.	Routing histories recorded across stakeholders.	Immutable proof of delivery events.
[169]	AI + Blockchain for pandemic supply insights.	Forecasting demand from social data with blockchain logging.	AI models, DLT fusion.	Data harmonization, unstructured input data.	Not covered.	External sentiment-derived demand trace.	No integrity mechanism described.

6.1.4. Charity and Donation Transparency Platforms

Charitable organizations and humanitarian NGOs often face public scrutiny concerning how donations are allocated, managed, and reported. To address concerns about trust, fraud, and inefficiency, blockchain technology has been increasingly integrated into donation platforms. These systems enable tamper-proof financial records, the real-time tracking of funds, and smart contract-based disbursement, enhancing both donor confidence and organizational accountability. Several blockchain-based solutions have emerged to ensure transparency across the donation lifecycle. For instance, a disaster relief-focused platform uses Ethereum smart contracts to record and display donation flows in real time through a MetaMask-compatible web interface [170]. Another approach combines crowdfunding, charitable giving, and corporate social responsibility (CSR) into a unified platform, leveraging ring signatures for anonymous yet verifiable transactions [171]. These systems provide auditable logs, donor privacy, and campaign-specific traceability. In more innovative use cases, blockchain is used alongside NFTs to represent donations or conduct secure charity auctions, ensuring both the provenance and traceability of contributions [172,173]. The incorporation of decentralized identity (DID) mechanisms further improves authenticity in donor–beneficiary interactions [26]. Additional models explore hybrid frameworks that

integrate blockchain with insurance-based fallback mechanisms to mitigate risks of fraud or system failure [174]. From a security perspective, these systems apply cryptographic proof, digital signature mechanisms (e.g., ECDSA), and consensus validation to prevent fund manipulation and unauthorized access [170,172]. For traceability, smart contracts, QR codes, and public ledgers allow donors to monitor how their funds are utilized, including milestone-based disbursements and campaign progress [171,175].

Finally, data integrity is ensured through immutable and decentralized storage, often complemented by off-chain systems like IPFS, to protect transaction records even under adverse conditions [64,173,175]. The technological diversity and implementation scope of blockchain-based donation platforms are provided in Table 14, highlighting their strengths in enhancing security, traceability, and data integrity across humanitarian fundraising ecosystems.

Table 14. Blockchain-based solutions for donation transparency platforms.

Ref.	Application Focus	Blockchain Role	Key Technologies	Security	Traceability	Data Integrity	Technical Challenges
[170]	Disaster relief donations.	Ethereum-based donation tracking system.	Smart contracts, ReactJS, Web3.0.	Immutable ETH transactions.	Real-time donation verification.	Ledger permanence for audits.	Device inconsistency, limited to ETH, MetaMask dependency.
[171]	Unified charity, CSR, crowdfunding.	Smart contract platform with anonymous ring signatures.	Ring signature, blockchain ledger.	Encrypted donor anonymity.	Campaign-level tracking.	Immutable cross-sector ledger.	Interoperability, data privacy, accessibility issues.
[172]	NFT-based donation platform.	NFT charity auction using Fisco Bcos.	Multi-sig, smart contracts, IPFS.	Verified NFT transactions.	Auction-based donation traceability.	Decentralized file storage.	High gas cost, auction process complexity.
[173]	NFT and ID-based charity registry.	Ethereum-based donation registry.	NFTs, decentralized ID, smart contracts.	Identity verification via DIDs.	NFT-campaign linkages.	Distributed proof of donation.	System complexity, NFT market volatility.
[174]	Blockchain + insurance for charities.	Charitable model with fallback insurance layer.	Hybrid blockchain, insurance contract.	Fraud protection through insurance.	Public auditing with Merkle Trees.	Smart contract-based trust mechanism.	Node trust issues, lack of inspection tools.
[175]	Cultural heritage donation tracking.	Provenance and traceability of donations.	Ethereum, donation logs.	Protection against misappropriation.	Transparent donation lineage.	Distributed donation proof.	Data storage and off-chain linkage limitations.
[176]	Crypto-altruism overview.	Review of blockchain potential in humanitarian aid.	Programmable contracts, tokens.	Secure token exchange.	Funding flow visibility.	Long-term transparent records.	Trust cost, usability barriers.

6.1.5. Food Security and Agricultural Aid

In conflict-affected and climate-vulnerable regions, ensuring the continuity and integrity of food supply chains has emerged as a top humanitarian priority. Blockchain-enabled food aid systems have been deployed to improve logistics efficiency, reduce food waste, and combat fraud in the distribution of scarce resources [177]. By leveraging smart contracts and real-time IoT integrations, such as RFID and QR-code tagging, these platforms monitor the conditions and movements of food items across the supply chain [177,178]. A prominent case is the World Food Programme's Building Blocks initiative, where blockchain

was used to distribute digital food vouchers to Syrian refugees in Jordan. Through biometric authentication and blockchain wallets, beneficiaries were able to securely access aid while avoiding unnecessary intermediaries, reducing transaction fees and enhancing auditability [177,179]. From a security perspective, blockchain eliminates manual errors and unauthorized access by ensuring role-based access control, tokenized credentials, and secure peer validation [179,180]. For traceability, each unit of aid is tracked from donor input through logistics nodes to the end recipient, maintaining full visibility across the chain, especially with smart irrigation, PDS grain distribution, and sustainability-tagged food items [179–182]. Regarding data integrity, immutable blockchain records enable the long-term verification of logistics actions and support needs-based planning, policy evaluation, and environmental compliance [177,181]. These capabilities align with the goals of sustainable humanitarian logistics by combining transparency, accountability, and real-time coordination. Table 15 summarizes selected blockchain applications supporting food security and agriculture in humanitarian contexts, along with their corresponding strengths in enhancing security, traceability, and data integrity.

Table 15. Blockchain applications in food security and agricultural aid.

Ref.	Application Focus	Blockchain Role	Key Technologies	Technical Challenges	Security Features	Traceability Features	Data Integrity Features
[177]	Food traceability and anti-fraud.	Immutable ledger to verify origin and condition of food items.	Smart contracts, QR codes, RFID, IoT.	Food fraud, poor visibility, manual inspections.	Verified identities, secure tokens.	Real-time condition + location tracking.	Tamper-proof audit trails and logs.
[178]	Blockchain-IoT integration for food supply chain.	Enhance reliability, transparency, and trust via consensus blockchain.	Optimized consensus, IoT, real-time logs.	Fragmented data, lack of verifiability, weak network transparency.	Encrypted blocks with consensus trust.	Live product journey tracing.	Synchronized transaction and sensor data.
[179]	Agricultural PDS traceability systems.	End-to-end traceability for food grain procurement and delivery.	Decentralized storage, process tracking.	Manual PDS inefficiencies, food leakage, governance gaps.	Node-based transaction validation.	One-step forward and backward traceability.	Immutable transaction storage with stakeholder linkage.
[180]	Blockchain adoption in IoT-based agri systems.	Blockchain-backed water distribution and input optimization.	IoT, smart irrigation + blockchain.	Water waste, input inefficiency, manual logging.	Authorized sensor data use.	Environmental condition traceability.	Sensor-integrated real-time immutable records.
[181]	Circular agriculture and food sustainability.	Transparency and record-keeping for eco-practices and food flow.	Blockchain + sustainability labels.	Lack of sustainability verification and fraud risk.	Verified eco-credentials.	Tracking origin and environmental footprint.	Continuous environmental compliance logging.
[182]	Digital transformation framework for food supply chains.	Enabling digital integration via IoT–CC–BDA synergy.	IoT, Cloud Computing, Big Data Analytics.	Fragmented systems, lack of integration, weak data management practices.	Enhanced data governance and infrastructure-level safeguards.	Real-time data visibility across FSC layers.	Structured data pipelines ensuring traceability and integrity.

6.2. Future Directions and Recommendations

Current research in blockchain-enabled supply chain security clearly demonstrates significant advantages in combating counterfeiting, ensuring data integrity, and enhancing traceability [48,53,54]. However, several challenges, security threats, and technical

limitations encountered in large-scale implementations indicate the need for further research. Strengthening data verification mechanisms is particularly crucial for effectively integrating blockchain systems into supply chain processes [55,56]. Security vulnerabilities associated with smart contracts and risks arising from cross-chain transactions necessitate the development of unified standards and protocols [64–68]. Privacy-focused solutions, such as ZKP and homomorphic encryption, should be extensively explored to enhance data security and confidentiality [86,87,90,95].

Furthermore, interoperability issues between different blockchain platforms present significant obstacles for the effective management of supply chain networks. Enhancing security in cross-chain transactions and developing decentralized verification mechanisms could mitigate these vulnerabilities [97,98,100,101]. Additionally, multiple verification techniques to improve the reliability of external data sources should be considered to address oracle security weaknesses [55,57,58]. The advancement of security protocols is essential for making blockchain-enabled supply chains safer and more efficient in the future. Improvements in existing security standards and the creation of new protocols should be supported by research specifically aimed at enhancing smart contract security and ensuring cross-chain transaction security [66,70,71]. Stronger authentication mechanisms will protect data from unauthorized access, significantly raising the overall security level of blockchain networks [77,78]. In addition, artificial intelligence (AI)-supported security solutions will play a crucial role in the future of blockchain technology. AI-based analytical systems can effectively detect anomalies and analyze fraud in supply chain processes. Machine learning algorithms can identify vulnerabilities within smart contracts and proactively detect potential threats, optimizing intervention mechanisms. Integrating AI-supported security solutions into blockchain systems will enable proactive threat management, thereby establishing more secure supply chain structures [73–75]. On the other hand, advancements in quantum computing technology represent a substantial threat to existing blockchain security systems. The potential of quantum computers to break classical encryption methods poses a significant risk to blockchain networks [48,86]. Therefore, developing solutions based on post-quantum cryptography is necessary to make blockchain systems resistant to quantum attacks. New-generation cryptographic approaches, such as lattice-based encryption and quantum-resistant signatures, will play a critical role in ensuring the long-term sustainability of blockchain security [87,89]. In the context of quantum threats, post-quantum cryptography (PQC) stands out as a critical solution to protect blockchain-based systems against potential attacks from quantum computers. PQC algorithms are designed to remain secure, even in the presence of quantum adversaries, and are generally categorized into lattice-based, hash-based, multivariate polynomial, and code-based cryptography. Prominent examples include CRYSTALS-Kyber for key encapsulation, CRYSTALS-Dilithium for digital signatures, and SPHINCS+, a stateless hash-based signature scheme. These algorithms are currently undergoing standardization by NIST and are considered promising candidates for enabling quantum-resistant security in blockchain architectures [88–90].

In blockchain-based supply chain management systems, the long-term integrity and confidentiality of traceability records are of paramount importance. Therefore, adopting quantum-resistant cryptographic structures, particularly in permissioned networks expected to operate over extended periods, ensures sustainable data security against future quantum-era threats [89,90]. Furthermore, some studies have conducted performance comparisons of zero-knowledge proof protocols, such as zk-SNARK, zk-STARK, and Bulletproof, in the context of post-quantum security, discussing their potential integration into future blockchain systems [72,73].

Finally, establishing regulatory frameworks and enhancing cross-sector collaboration are critical components for securing blockchain-based supply chains. Developing

international security standards will ensure compliance and enhance technology reliability. Encouraging academic research and industry collaboration will accelerate blockchain adoption, creating a robust ecosystem for supply chain security [86,91,93].

7. Discussions

Having examined the technical and sectoral dimensions of blockchain in SCM, this section synthesizes the key insights and presents broader discussions on integration, sustainability, and security trade-offs.

7.1. Integration of Blockchain into Existing Supply Chains: Practical Complexities

Although blockchain offers convincing advantages in terms of security, traceability, and data integrity, its integration into existing supply chains remains highly complex. In particular, centralized ERP systems and traditional databases already used in supply chain processes are not inherently compatible with blockchain infrastructures [1,26]. This misalignment requires significant infrastructure transformations and extensive interorganizational collaboration. Furthermore, since many actors in the supply chain are SMEs, a digital divide emerges due to disparities in technical capabilities and investment resources [6]. These constraints hinder the holistic implementation of blockchain systems across the entire supply chain.

7.2. Privacy vs. Transparency Paradox

Supply chains are typically complex, multi-actor systems expected to remain both transparent and competitive. However, the level of transparency required to enable traceability may risk disclosing trade secrets or sensitive business information. For example, exposing supplier identities, pricing structures, or strategic logistics data can lead to competitive disadvantages [85]. Although emerging solutions, such as ZKPs and confidential transactions, aim to mitigate this conflict, their maturity for supply chain implementations remains limited [87,88].

7.3. Smart Contracts and Their Operational Limitations

Numerous external factors, such as delivery delays, weather disruptions, or logistical bottlenecks, can affect contractual conditions in supply chains. However, the rigid and deterministic nature of smart contracts may struggle to reflect such real-world variability [31,34]. For instance, an automatic penalty triggered by a delayed delivery could undermine operational flexibility or human judgment. Additionally, vulnerabilities in smart contract code pose considerable security risks for large-scale supply chain operations [36]. These concerns are further presented in Table 16, which outlines the key technical limitations of smart contracts and their practical implications within supply chain environments.

Table 16. Limitations of smart contracts and their implications for supply chains.

Smart Contract Limitation	Implications for Supply Chains	References
Immutable code	Inflexible agreements	[34,36]
Lack of legal enforceability	Legal uncertainty in dispute resolution	[31,36]
Oracle dependency	Critical reliance on external data sources	[31,34]
Code vulnerabilities	Risk of operational disruption and reputational damage	[27,36]

7.4. Cross-Chain Interoperability and Standardization Issues

Global supply chains span across countries and industries, involving numerous heterogeneous systems. Yet, most blockchain solutions function as isolated ecosystems, limiting

end-to-end visibility and seamless data exchange [97,98]. Cross-chain communication is hindered not only by technical incompatibility but also by the absence of common standards and diverse data policies. Although emerging solutions aim to bridge this gap, their integration into supply-chain-specific scenarios remains underdeveloped and insufficiently tested [100].

7.5. Sustainability Concerns and Green Blockchain

In recent years, supply chains have increasingly emphasized sustainability metrics, including the carbon footprint, ESG (Environmental, Social, and Governance) compliance, and green logistics. In this regard, blockchain's transparency and traceability can support environmental goals. However, the energy consumption of certain consensus mechanisms, particularly proof-of-work, raises concerns about alignment with sustainability objectives. Although alternatives such as proof-of-stake offer greater efficiency, energy sustainability in large-scale logistics systems remains an open debate [108,137].

7.6. The Human Factor: Organizational Resistance and Skill Gaps

One of the most significant barriers to digital transformation in supply chains is not technological but organizational. Reconfiguring internal processes around blockchain logic often generates resistance and uncertainty among employees [43]. Furthermore, the shortage of skilled personnel in blockchain technologies hampers implementation. Therefore, beyond technical readiness, synchronized organizational transformation strategies are essential for successful adoption [136].

7.7. The Role of Emerging Technologies in Blockchain-Enabled Supply Chains

Beyond architectural and interoperability concerns, the role of emerging technologies further reshapes blockchain-enabled SCM frameworks. The increasing complexity and interconnectedness of modern supply chains, driven by real-time responsiveness, multi-actor coordination, and global scalability, has introduced new systemic demands on data security, traceability, and integrity. Emerging technologies, such as quantum computing, edge computing, and the IoE, are deeply reshaping the operational and architectural foundations of blockchain-enabled supply chains.

Quantum computing introduces computational capabilities that challenge traditional cryptographic assumptions. In supply chains where blockchain ensures immutable transaction records and identity authentication, the emergence of quantum attacks calls for post-quantum cryptography to maintain long-term security guarantees [89,90].

Edge computing, by shifting data processing closer to the data source, complements blockchain's decentralized ethos. In latency-sensitive environments, like cold-chain logistics or just-in-time manufacturing, edge computing enhances traceability by enabling faster, localized decision-making and reducing reliance on centralized servers [48,49].

The IoE, encompassing not just devices, as in the traditional IoT, but also people, processes, and contextual intelligence, amplifies the scale and complexity of data exchanged across supply chain layers. While this fosters hyper-connectivity and visibility, it simultaneously creates new vulnerabilities. Blockchain offers promising foundations for managing trust, ensuring data provenance, and coordinating actions in such heterogeneous, data-rich environments [9,10,49]. These trends highlight a key insight that the evolving systemic demands are not just about integrating more technologies but about aligning them with scalable, secure, and interoperable supply chain solutions. Future research must focus on hybrid frameworks that combine blockchain with edge-native consensus protocols, quantum-resistant cryptographic schemes, and data governance models capable of adapting to the high-velocity and high-variety nature of IoE-driven systems. As these technologies continue to mature, their intersection with blockchain introduces both opportunities and challenges in achieving secure, transparent, and trustworthy supply

chains. Figure 9 illustrates how emerging technologies, such as quantum computing, edge computing, and the IoE, impact the three core dimensions of security, traceability, and data integrity, highlighting both their benefits and the associated challenges.

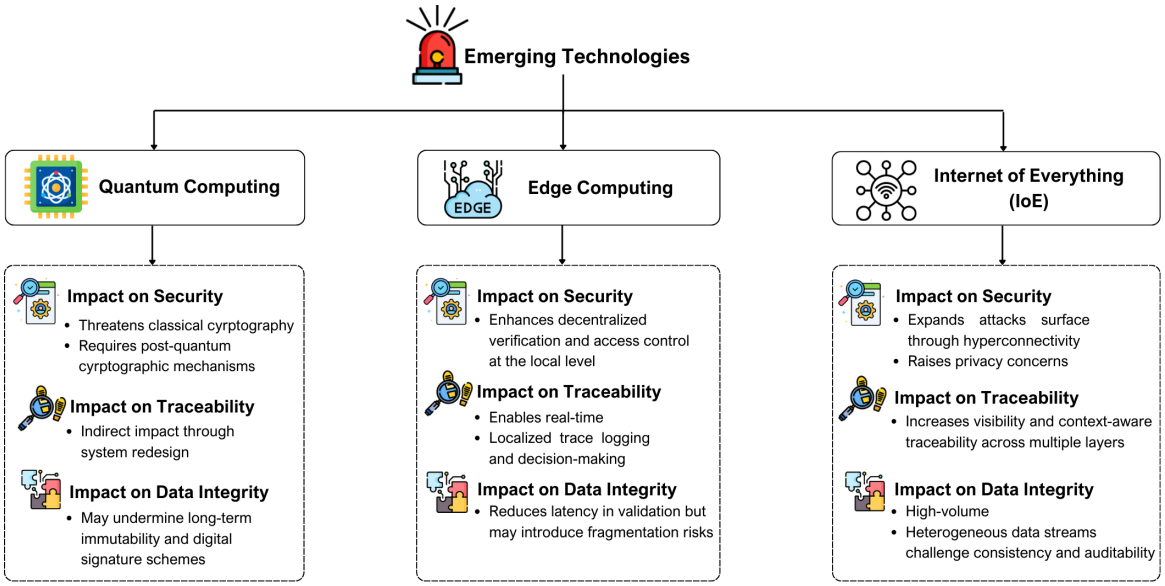

Figure 9. Impact of emerging technologies on security, traceability, and data integrity in blockchain-enabled supply chains.

7.8. Scalability and Sustainability Trade-Offs in Blockchain-Based SCM

Based on the previous analyses, this subsection outlines emerging research opportunities and unresolved challenges that merit further exploration.

While the use of blockchain technology in supply chains offers significant advantages in terms of security, traceability, and data integrity, it also entails certain limitations, particularly concerning scalability and sustainability in large-scale systems. For instance, PoW-based systems involve high energy consumption and long transaction confirmation times, which pose substantial challenges for SCM scenarios that demand real-time data synchronization and high transaction throughputs. In contrast, alternative consensus algorithms, such as PoS and PBFT, are more advantageous in terms of energy efficiency; however, they introduce different limitations related to security and decentralization. A comparative analysis of different consensus mechanisms in terms of transaction speed, energy consumption, and their suitability in SCM contexts is presented in Table 17.

In this context, permissioned blockchain platforms (e.g., Hyperledger Fabric) offer more suitable solutions in terms of both energy efficiency and transaction speed. When selecting the appropriate system architecture, operational sustainability criteria, such as energy and processing costs, should be considered alongside the balance between security and privacy.

In addition to consensus-related trade-offs, broader system-level cost drivers also shape the feasibility of blockchain adoption in SCM. Table 18 summarizes the key technical factors that influence the setup and operational costs of blockchain-based supply chain systems. The evaluation is based on metrics such as resource consumption and processing capacity, which are inherently tied to the architectural components and infrastructure requirements of the system. Specifically, factors such as the number of virtual machines (VMs) deployed on cloud-based infrastructures, energy consumption, transaction throughput (TPS), data storage strategy, and integration complexity have a direct impact on the total cost of ownership [84,85,108,183]. For instance, PoW-based systems are generally unsustainable for large-scale enterprise SCM applications due to their high energy consumption (~800 kWh/tx) and low TPS (~7) [80,82,83,183,184]. In contrast, PBFT-based frameworks,

such as Hyperledger Fabric, offer significantly lower energy consumption (~0.0001 kWh/tx) and higher transaction capacity (1000+ TPS), while requiring a predictable VM infrastructure (3–4 VMs) and offering greater integration flexibility [84,85,183]. Furthermore, their compatibility with off-chain data storage strategies can reduce costs in data-intensive applications [108,137]. Regarding PoS-based systems like Ethereum 2.0, recent studies estimate that the energy consumption per transaction has dropped to ~0.0087 kWh/tx after the shift from PoW to PoS, assuming an average throughput of 30 tx/s [185]. This efficiency gain enhances their viability in sustainability-sensitive supply chain applications. In addition, long-term sustainability of the system requires ongoing maintenance, updates, and training efforts. Factors such as platform integration, user onboarding, and security policy enforcement also contribute significantly to initial implementation costs [81,108]. This comparative analysis aims to assess the operational cost implications of blockchain infrastructure in the context of supply chain systems from a technical perspective.

Table 17. Comparative analysis of consensus mechanisms in terms of energy efficiency, scalability, and applicability to supply chain management.

Consensus Mechanism	Energy Consumption (kWh/tx)	TPS (Throughput)	SCM Suitability	Trade-Offs	References
PoW (Bitcoin)	High (~800)	~7	Low	Extremely secure, but unsustainable and slow.	[80,82,83,108,183,184]
PoS (Ethereum 2.0)	Low (~0.01) (~0.0087 for 30 tx)	~15–210	Moderate to High	Energy-efficient, evolving TPS, some centralization.	[81,82,108,137,183,185]
PBFT (Hyperledger)	Very Low (~0.0001)	~1000–2500	High	High throughput, permissioned, scalable, but limited decentralization.	[81,84,85]
PoA/Raft	Low	1000+	High	Efficient for enterprise, but centralized trust model.	[85,108,137]

Table 18. Key operational cost factors in blockchain-based supply chain systems: a comparative overview of performance, infrastructure demands, and integration complexity.

Blockchain Model	TPS	Energy Consumption (kWh/tx)	Estimated VM Count	Data Storage Need	Integration Cost	SCM Suitability
PoW (Bitcoin)	~7	~800	6–8 VMs	High (on-chain)	High	Low
PoS (Ethereum 2.0)	~15–210	~0.01	4–6 VMs	Medium (mixed)	Moderate	Moderate
PBFT (Hyperledger)	1000–2500	~0.0001	3–4 VMs	Low (off-chain)	Moderate	High
PoA/Raft	1000+	Low	2–3 VMs	Low	Low	High

7.9. Future Research Directions

This review highlights several key research gaps in the current literature that require further exploration:

- Lightweight and scalable blockchain architectures tailored to supply chain scenarios.
- Legally compliant and adaptable smart contract models.
- Trust-building mechanisms in multi-stakeholder decision-making environments.
- The integration of AI and blockchain for predictive analytics and decision support.
- Real-time data integration through edge computing.
- System architectures capable of maintaining data integrity under IoE-driven data diversity.
- Quantum-resistant cryptographic techniques adapted to the security demands of SCM.

Future research in these areas should not only follow technological trends but also align with evolving systemic demands to enhance blockchain's strategic contribution to secure and resilient supply chains [3,27].

7.10. A Holistic Outlook

To conclude, this section provides a holistic perspective that integrates the diverse insights presented throughout the paper, aiming to guide future developments in blockchain-based SCM.

Blockchain is not a standalone solution for the digital transformation of supply chains. However, when effectively integrated with complementary technologies, such as the IoT, AI, digital twins, edge computing, and cloud infrastructure, it can contribute to building transparent, resilient, and adaptive supply chain ecosystems.

Emerging technologies, particularly the IoE, quantum computing, and autonomous decision systems, are reshaping the requirements for data security, traceability, and integrity. These developments introduce both opportunities and new vulnerabilities. In this regard, the future role of blockchain will extend beyond enabling trust and move toward supporting resilience, adaptability, and responsiveness to evolving systemic demands.

8. Conclusions

This review has comprehensively examined the role of blockchain in enhancing security, traceability, and data integrity within SCM systems. The findings suggest that while blockchain offers significant potential in these three core dimensions, its real-world application faces several structural, technical, and organizational challenges.

Blockchain can enable end-to-end transparency, immutable data recording, and reduced reliance on intermediaries in supply chains. However, to ensure the sustainable realization of these benefits, further efforts are needed in integrating blockchain with existing systems, developing data-sharing standards, and adapting smart contract mechanisms to legal and operational requirements.

Moreover, blockchain adoption is not merely a technological shift, it also demands changes in organizational culture, collaboration frameworks, and human capital strategies. Balancing technical innovation with socio-organizational dynamics is essential for meaningful transformation.

Notably, emerging technologies, such as the IoE, AI, quantum computing, and edge computing, are introducing new expectations and complexities in how data are generated, validated, and secured. In this context, ensuring trust, traceability, and integrity is no longer a static challenge, but a dynamic and forward-looking requirement.

Thus, future efforts should go beyond integration and emphasize the development of socio-technical models aligned with evolving systemic demands.

This review aims to provide both researchers and practitioners with a clear perspective on the current state and developmental directions of blockchain-enabled supply chain systems. It concludes that building more secure, traceable, and trustworthy supply chains is not solely a matter of technological implementation, but also a product of shared vision, open data culture, and sustainable design principles.

Despite the promising potential of blockchain in securing supply chain systems, several limitations still hinder its seamless adoption. These include the rigidity of smart contracts, legal enforceability issues, the dependency on external data sources (oracles), and the lack of cross-chain standardization, all of which limit flexibility, legal certainty, and system interoperability. While there are emerging examples of integrated and collaborative blockchain applications in supply chains, many current implementations still face challenges of fragmentation and limited interoperability. These issues often stem from het-

erogeneous infrastructures, a lack of standardization, and the absence of well-established integration pathways, particularly in multi-stakeholder environments.

As shown in Sections 7.4 and 7.7, interoperability remains a critical bottleneck. Without common data policies and standardized protocols, cross-chain platforms cannot achieve full synchronization across networks. Similarly, while privacy-enhancing techniques like ZKP offer solutions, their real-world integration into supply chains is still underexplored.

On the technological frontier, quantum computing poses an existential risk to classical cryptographic primitives. Without the rapid development and adoption of post-quantum cryptographic schemes, the long-term sustainability of blockchain security cannot be guaranteed.

In terms of organizational readiness, the human factor is equally important. Resistance to change, a lack of blockchain expertise, and misalignment between blockchain principles and traditional ERP systems complicate integration efforts.

Looking forward, several research directions should be prioritized: the development of lightweight blockchain architectures tailored for SCM environments; legally adaptable smart contract models; AI-assisted anomaly detection; and system architectures that can adapt to the high-volume, high-velocity data streams of IoE-based logistics systems. These pathways will not only address the limitations discussed but also ensure the long-term strategic value of blockchain in resilient, transparent, and intelligent supply chains.

Author Contributions: The research conceptualization and the definition of the research scope: G.G. and Ö.K. The analysis and classification of security threats in traditional and blockchain-enabled supply chains: G.G. and Ö.K. The evaluation of blockchain security mechanisms, including immutability, smart contracts, cryptographic signatures, and decentralization: G.G. The comparative security analysis between traditional and blockchain-based supply chain systems: Ö.K. The examination of smart contract vulnerabilities and blockchain attack vectors: G.G. The mathematical modeling and structured analysis of zero-knowledge proofs: Ö.K. The design and development of performance comparison tables and mathematical metrics: Ö.K. The design of cross-chain architecture and the analysis of its implications on STI principles: Ö.K. The development and explanation of functional pseudocode for supply chain automation and validation processes: G.G. and Ö.K. The sectoral analyses and industry-specific blockchain applications in SCM: G.G. and Ö.K. The investigation of humanitarian logistics and blockchain-based identity management use cases: Ö.K. The identification of research gaps and the formulation of future directions: G.G. and Ö.K. Writing: original draft preparation: G.G. and Ö.K. Writing: review and editing: G.G. and Ö.K. Supervision, coordination, and final approval: Ö.K. All authors have read and agreed to the published version of the manuscript.

Funding: This study is supported by the Institution of Firat University Scientific Research Projects (FUBAP) under project number SHY.24.18, with the APC funded by FUBAP.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created.

Acknowledgments: The authors acknowledge the CHIST-ERA Di4SPDS project (CHIST-ERA-22-SPiDDS-01) and its national partner project, TUBITAK 223N142, conducted under the TUBITAK 1071 International Collaboration Program. Additionally, this study has been carried out within the scope of a master's thesis titled "Afetlerde Yardım Malzemelerinin Blockchain Teknolojisi Kullanılarak Güvenli Şekilde Ulaştırılması (Secure Delivery of Relief Supplies using Blockchain Technology in Disasters)" by Gülsena Gülhas, under the supervision of Özgür Karaduman, at Fırat University, the Department of Software Engineering.

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

References

1. Dudczyk, P.; Dunston, J.K.; Crosby, G.V. Blockchain technology for global supply chain management: A survey of applications, challenges, opportunities and implications. *IEEE Access* **2024**, *12*, 70065–70088. [CrossRef]
2. Aggarwal, M.; Rani, P.; Rani, P.; Sharma, P. Revolutionizing agri-food supply chain management with blockchain-based traceability and navigation integration. *Clust. Comput.* **2024**, *27*, 12919–12942. [CrossRef]
3. Mangala, N.; Naveen, D.R.; Reddy, B.E.; Buyya, R.; Venugopal, K.R.; Iyengar, S.S.; Patnaik, L.M. Secure pharmaceutical supply chain using blockchain in IoT cloud systems. *Internet Things* **2024**, *26*, 101215.
4. Islam, M.D. A survey on the use of blockchains to achieve supply chain security. *Inf. Syst.* **2023**, *117*, 102232. [CrossRef]
5. Tan, Z.; Parambath, S.P.; Anagnostopoulos, C.; Singer, J.; Marnerides, A.K. Advanced persistent threats based on supply chain vulnerabilities: Challenges, solutions and future directions. *IEEE Internet Things J.* **2025**, *12*, 6371–6395. [CrossRef]
6. Roumeliotis, C.; Dasygenis, M.; Lazaridis, V.; Dossis, M. Blockchain and digital twins in smart industry 4.0: The use case of supply chain-a review of integration techniques and applications. *Designs* **2024**, *8*, 105. [CrossRef]
7. Agrawal, B.P.; Aronkar, P.; Palav, M.R.; Badre, S.; Karumuri, V.; Bagale, G.S. Optimizing supply chain management with IoE and AI. In *Interdisciplinary Approaches to AI, Internet of Everything, and Machine Learning*; IGI Global Scientific Publishing: Hershey, PA, USA, 2025; pp. 423–436.
8. Wu, H.; Jiang, S.; Cao, J. High-efficiency blockchain-based supply chain traceability. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 3748–3758. [CrossRef]
9. Shoomal, A.; Jahanbakht, M.; Componation, P.J.; Ozay, D. Enhancing supply chain resilience and efficiency through internet of things integration: Challenges and opportunities. *Internet Things* **2024**, *27*, 101324. [CrossRef]
10. Singh, G.K.; Dadhich, M. Supply chain management growth with the adoption of blockchain technology (BoT) and internet of things (IoT). In Proceedings of the 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 12–13 May 2023; pp. 321–325.
11. Chaker, B.; Damak, C. Integrating blockchain technology for enhanced transparency and security in supply chains. In *Strategic Innovations for Dynamic Supply Chains*; IGI Global Scientific Publishing: Hershey, PA, USA, 2024; pp. 147–169.
12. Maurya, V.; Rishiwal, V.; Yadav, M.; Shiblee, M.; Yadav, P.; Agarwal, U.; Chaudhry, R. Blockchain-driven security for IoT networks: State-of-the-art, challenges and future directions. *Peer-to-Peer Netw. Appl.* **2025**, *18*, 1–35. [CrossRef]
13. Shen, Y.; Gao, X.; Sun, H.; Guo, Y. Understanding vulnerabilities in software supply chains. *Empir. Softw. Eng.* **2025**, *30*, 1–38. [CrossRef]
14. Berry, H.S. The importance of cybersecurity in supply chain. In Proceedings of the 11th International Symposium on Digital Forensics and Security (ISDFS), Chattanooga, TN, USA, 11–12 May 2023; pp. 1–5.
15. Hammi, B.; Zeadally, S. Software supply-chain security: Issues and countermeasures. *Computer* **2023**, *56*, 54–66. [CrossRef]
16. Möller, D.P. Ransomware attacks and scenarios: Cost factors and loss of reputation. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices*; Springer Nature: Cham, Switzerland, 2023; pp. 273–303.
17. Cartwright, A.; Cartwright, E. The economics of ransomware attacks on integrated supply chain networks. *Digit. Threat. Res. Pract.* **2023**, *4*, 1–14. [CrossRef]
18. Manning, L.; Kowalsk, A. The threat of ransomware in the food supply chain: A challenge for food defence. *Trends Organ. Crime* **2023**, *26*, 1–29. [CrossRef]
19. Hammi, B.; Zeadally, S.; Jamel, N. Security threats, countermeasures, and challenges of digital supply chains. *ACM Comput. Surv.* **2023**, *55*, 1–40. [CrossRef]
20. Mohamed, A.A.; Al-Saleh, A.; Sharma, S.K.; Tejani, G.G. Zero-day exploits detection with adaptive WavePCA-Autoencoder (AWPA) adaptive hybrid exploit detection network (AHEDNet). *Sci. Rep.* **2025**, *15*, 4036. [CrossRef] [PubMed]
21. Zhou, S.; Li, H.; Fu, X.; Jiao, Y. A novel malware detection model in the software supply chain based on LSTM and SVMs. *Appl. Sci.* **2024**, *14*, 6678. [CrossRef]
22. Kandasamy, V.; Roseline, A.A. Harnessing advanced hybrid deep learning model for real-time detection and prevention of man-in-the-middle cyber attacks. *Sci. Rep.* **2025**, *15*, 1697. [CrossRef]
23. Fereidouni, H.; Fadeitcheva, O.; Zalai, M. IoT and Man-in-the-Middle attacks. *Secur. Priv.* **2025**, *8*, e70016. [CrossRef]
24. Siadati, H.; Jafarikhah, S.; Sahin, E.; Hernandez, T.; Tripp, E.; Khryashchev, D.; Kharraz, A. DevPhish: Exploring social engineering in software supply chain attacks on developers. In Proceedings of the IEEE 15th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), Yorktown Heights, NY, USA, 17–19 October 2024; pp. 517–523.
25. Lin, I.C.; Kuo, Y.H.; Chang, C.C.; Liu, J.C.; Chang, C.C. Symmetry in blockchain-powered secure decentralized data storage: Mitigating risks and ensuring confidentiality. *Symmetry* **2024**, *16*, 147. [CrossRef]
26. Eghmazi, A.; Ataei, M.; Landry, R.J.; Chevrette, G. Enhancing IoT data security: Using the blockchain to boost data integrity and privacy. *IoT* **2024**, *5*, 20–34. [CrossRef]
27. Chandol, M.K.; Kameswara Rao, M. Blockchain-based cryptographic approach for privacy enabled data integrity model for IoT healthcare. *J. Exp. Theor. Artif. Intell.* **2025**, *37*, 53–74. [CrossRef]

28. Hossain, M.I.; Steigner, T.; Hussain, M.I.; Akther, A. Enhancing data integrity and traceability in industry cyber physical systems (icps) through blockchain technology: A comprehensive approach. *arXiv* **2024**, arXiv:2405.04837. [CrossRef]
29. Yavaprabhas, K.; Kurnia, S.; Seyedghorban, Z.; Samson, D. Demystifying the impact of blockchain on trust in emerging and established relationships: A case of organic food supply chains. In Proceedings of the 57th Hawaii International Conference on System Sciences (HICSS), Honolulu, HI, USA, 3–6 January 2024; pp. 5898–5907.
30. Li, J.; Han, D.; Weng, T.H.; Wu, H.; Li, K.C.; Castiglione, A. A secure data storage and sharing scheme for port supply chain based on blockchain and dynamic searchable encryption. *Comput. Stand. Interfaces* **2025**, *91*, 103887. [CrossRef]
31. Naqvi, F.H.; Ali, S.; Haseeb, B.; Khan, N.; Qureshi, S.; Sajid, T.; Aslam, M.I. Design and implementation of smart contract in supply chain management using blockchain and internet of things. *Eng. Proc.* **2023**, *32*, 15. [CrossRef]
32. Jain, Y.K.; Rathore, C.D.S.; Shukla, A.N.; Sing, J.; Gupta, M.; Garg, N. Analyzing the influence of blockchain technology adoption on the supply chain management of the logistics industry. In Proceedings of the International Conference on Communication, Computer Sciences and Engineering (IC3SE), Gautam Buddha Nagar, India, 9–11 May 2024; pp. 948–953.
33. Sakib, S.N. Blockchain technology for smart contracts: Enhancing trust, transparency, and efficiency in supply chain management. In *Achieving Secure and Transparent Supply Chains with Blockchain Technology*; IGI Global Scientific Publishing: Hershey, PA, USA, 2024; pp. 246–266.
34. Raj, P.V.R.P.; Jauhar, S.K.; Ramkumar, M.; Pratap, S. Procurement, traceability and advance cash credit payment transactions in supply chain using blockchain smart contracts. *Comput. Ind. Eng.* **2022**, *167*, 108038. [CrossRef]
35. Muthamilselvan, S.; Shobana, R.; Sujitha, J.; Varsha, K. Ethereum smart contract in supply chain management. In Proceedings of the IEEE International Conference on Power, Energy, Control and Transmission Systems (ICPECTS), Chennai, India, 8–9 October 2024; pp. 1–6.
36. Yigit, E.; Dag, T. Improving supply chain management processes using smart contracts in the ethereum network written in solidity. *Appl. Sci.* **2024**, *14*, 4738. [CrossRef]
37. Nalayini, C.; Jeevaakatiravan; Imogen, P.V.; Sahana, J. A study on digital signature in blockchain technology. In Proceedings of the Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2–4 February 2023; pp. 398–403.
38. Jasim, L.H.; Mishra, A.; Joshi, S.K.; Sapaev, I.B.; DR, P.; Babu, A.N. Analysing blockchain-based cryptography: Enhancing security, transparency, and practical implementations. In Proceedings of the International Conference for Technological Engineering and its Applications in Sustainable Development (ICTEASD), Necef, Irak, 14–15 November 2023; pp. 39–44.
39. Mahajan, H.; Reddy, K.T.V. Secure gene profile data processing using lightweight cryptography and blockchain. *Clust. Comput.* **2024**, *27*, 2785–2803. [CrossRef]
40. Qatbi, M.R.S.A.; Rathinam, G. Enhancing supply chain management: A blockchain-based approach for data privacy and transparency in the IoT era. In Proceedings of the 10th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Palembang, Indonesia, 20–21 September 2023; pp. 667–671.
41. Savadatti, S.G.; Krishnamoorthy, S.; Delhibabu, R. Survey of distributed ledger technology (dlt) for secure and scalable computing. *IEEE Access* **2025**, *13*, 8393–8415. [CrossRef]
42. Yadav, A.S.; Agrawal, S.; Kushwaha, D.S. Distributed ledger technology-based land transaction system with trusted nodes consensus mechanism. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 6414–6424. [CrossRef]
43. Sharabati, A.A.A.; Jreisat, E.R. Blockchain technology implementation in supply chain management: A literature review. *Sustainability* **2024**, *16*, 2823. [CrossRef]
44. Jahani, M.; Raji, F.; Zojaji, Z. Securing supply chain through blockchain-integrated algorithmic system: Ensuring product quality and counterfeiting tags detection. *Clust. Comput.* **2025**, *28*, 1–23. [CrossRef]
45. Gayialis, S.P.; Kechagias, E.P.; Papadopoulos, G.A.; Masouras, D. A review and classification framework of traceability approaches for identifying product supply chain counterfeiting. *Sustainability* **2022**, *14*, 6666. [CrossRef]
46. Liu, B.; Si, X.; Kang, H. A literature review of blockchain-based applications in supply chain. *Sustainability* **2022**, *14*, 15210. [CrossRef]
47. Santhi, A.R.; Muthuswamy, P. Influence of blockchain technology in manufacturing supply chain and logistics. *Logistics* **2022**, *6*, 15. [CrossRef]
48. Agarwal, U.; Rishiwal, V.; Yadav, M.; Alshammari, M.; Yadav, P.; Singh, O. Exploring blockchain and supply chain integration: State-of-the-art, security issues, and emerging directions. *IEEE Access* **2024**, *12*, 143945–143974. [CrossRef]
49. Hasan, A.S.M.T.; Sabah, S.; Haque, R.U.; Daria, A.; Rasool, A.; Jiang, Q. Towards convergence of IoT and blockchain for secure supply chain transaction. *Symmetry* **2022**, *14*, 64. [CrossRef]
50. Njualem, L.A. Leveraging blockchain technology in supply chain sustainability: A provenance perspective. *Sustainability* **2022**, *14*, 10533. [CrossRef]
51. Gong, Y.; Zhang, Y.; Alharithi, M. Supply chain finance and blockchain in operations management: A literature review. *Sustainability* **2022**, *14*, 13450. [CrossRef]

52. Gokkaya, B.; Karafili, E.; Aniello, L.; Halak, B. Global supply chains security: A comparative analysis of emerging threats and traceability solutions. *Benchmarking Int. J.* **2025**, *32*, 917–942. [CrossRef]
53. Rajchandar, K.; Shameem, A.; Biswas, P.; Geetha, B.T.; Arunkumar, J.R.; Lakineni, P.K. Supply chain management using blockchain: Opportunities, challenges, and future directions. In Proceedings of the Second International Conference on Informatics (ICI), Noida, India, 23 November 2023; pp. 1–6.
54. Chang, A.J.; El-Rayes, N.; Nesreen; Shi, J. Blockchain technology for supply chain management: A comprehensive review. *FinTech* **2022**, *1*, 191–205. [CrossRef]
55. Ahmadjee, S.; Mera-Gómez, C.; Farshidi, S.; Bahsoon, R.; Kazman, R. Decision Support Model for Selecting the Optimal Blockchain Oracle Platform: An Evaluation of Key Factors. *ACM Trans. Softw. Eng. Methodol.* **2025**, *34*, 1–35. [CrossRef]
56. Hassan, A.; Makhdoom, I.; Iqbal, W.; Ahmad, A.; Raza, A. From trust to truth: Advancements in mitigating the Blockchain Oracle problem. *J. Netw. Comput. Appl.* **2023**, *217*, 103672. [CrossRef]
57. Caldarelli, G. Overview of blockchain oracle research. *Future Internet* **2022**, *14*, 175. [CrossRef]
58. Caldarelli, G. Formalizing oracle trust models for blockchain-based business applications. An Example from the supply chain sector. *arXiv* **2022**, arXiv:2202.13930.
59. Cao, Y.; Guan, S.; Wang, D.; Wang, Z. BE-AC: Reliable blockchain-based anti-counterfeiting traceability solution for pharmaceutical industry. *Clust. Comput.* **2024**, *27*, 8119–8139. [CrossRef]
60. Kang, Y.; Shi, X.; Yue, X.; Zhang, W.; Liu, S.S. Enhancing traceability in wine supply chains through blockchain: A stackelberg game-theoretical analysis. *J. Theor. Appl. Electron. Commer. Res.* **2023**, *18*, 2142–2162. [CrossRef]
61. Crossland, V.; Dellwo, C.; Bashar, G.; Dagher, G.G. Janus: Toward preventing counterfeits in supply chains utilizing a multi-quorum blockchain. *Blockchain Res. Appl.* **2023**, *4*, 100157. [CrossRef]
62. Sugandh, U.; Nigam, S.; Khari, M.; Misra, S. An approach for risk traceability using blockchain technology for tracking, tracing, and authenticating food products. *Information* **2023**, *14*, 613. [CrossRef]
63. Chen, C.L.; Zhan, W.B.; Huang, D.C.; Liu, L.C.; Deng, Y.Y.; Kuo, C.G. Hyperledger fabric-based tea supply chain production data traceable scheme. *Sustainability* **2023**, *15*, 13738. [CrossRef]
64. Eren, H.; Karaduman, Ö.; Gençoğlu, M.T. Security challenges and performance trade-offs in on-chain and off-chain blockchain storage: A comprehensive review. *Appl. Sci.* **2025**, *15*, 3225. [CrossRef]
65. Darvishi, I.; Asare, B.T.; Musa, A.; Yeboah-Ofori, A.; Oseni, W.; Ganiyu, A. Blockchain technology and vulnerability exploits on smart contracts. In Proceedings of the 2024 11th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 19–21 August 2024; pp. 160–167.
66. Chaganti, R.; Boppana, R.V.; Ravi, V.; Munir, K.; Almutairi, M.; Rustam, F. A comprehensive review of denial of service attacks in blockchain ecosystem and open challenges. *IEEE Access* **2022**, *10*, 96538–96555. [CrossRef]
67. Sun, T.; Yu, W. A formal verification framework for security issues of blockchain smart contracts. *Electronics* **2020**, *9*, 255. [CrossRef]
68. Dimitrijević, N.; Zdravković, N. A review on security vulnerabilities of smart contracts written in solidity. In Proceedings of the Information Society of Serbia—ISOS, Kopaonik, Serbia, 10–13 March 2024; pp. 89–99.
69. Dhillon, D.; Diksha; Mehrotra, D. Smart contract vulnerabilities: Exploring the technical and economic aspects. In *Blockchain Transformations*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 81–91.
70. Endurthi, A.; Khare, A. Smart contracts resilient against malicious attacks in permission-less blockchain. In Proceedings of the 10th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 15–17 March 2023; pp. 1201–1206.
71. Kannengießer, N.; Lins, S.; Sander, C.; Winter, K.; Frey, H.; Sunyaev, A. Challenges and common solutions in smart contract development. *IEEE Trans. Softw. Eng.* **2022**, *48*, 4291–4318. [CrossRef]
72. Roelink, O. Benchmarking the zk-Snark, zk-Stark, and Bulletproof Non-Interactive Zero-Knowledge Proof Protocols in an Equivalent Practical Application. Master's Thesis, University of Twente, Enschede, The Netherlands, June 2024. Available online: https://essay.utwente.nl/100612 (accessed on 28 March 2025).
73. El-Hajj, M.; Roelink, B.O. Evaluating the efficiency of zk-snark, zk-stark, and bulletproof in real-world scenarios: A benchmark study. *Information* **2024**, *15*, 463. [CrossRef]
74. Imtiaz, N.; Wahid, A.; Abideen, S.Z.U.; Kamal, M.M.; Sehito, N.; Khan, S.; Virdee Bal, S.; Kouhalvandi, L.; Alibakhshikenari, M. A deep learning-based approach for the detection of various Internet of Things intrusion attacks through optical networks. *Photonics* **2025**, *12*, 1–39. [CrossRef]
75. Srhir, A.; Mazri, T.; Benbrahim, M. Towards secure smart campus: Security requirements, attacks and counter measures. *Indones. J. Electr. Eng. Comput. Sci.* **2023**, *32*, 900–914. [CrossRef]
76. Shukla, P.; Krishna, C.R.; Patil, N.V. IoT traffic-based DDoS attacks detection mechanisms: A comprehensive review. *J. Supercomput.* **2024**, *80*, 9986–10043. [CrossRef]

77. Krishna, R.R.; Priyadarshini, A.; Jha, A.V.; Appasani, B.; Srinivasulu, A.; Bizon, N. State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions. *Sustainability* **2021**, *13*, 9463. [CrossRef]
78. Vats, G.; Sharma, P.K. An exhaustive analysis on security issues concerning IoT using blockchain. In Proceedings of the International Conference on Disruptive Technologies (ICDT), Greater Noida, India, 11–12 May 2023; pp. 1–7.
79. Ahmad, R.W.; Ko, K.M.; Rashid, A.; Rodrigues, J.J.P.C. Blockchain for food industry: Opportunities, requirements, case studies, and research challenges. *IEEE Access* **2024**, *12*, 117363–117378. [CrossRef]
80. Alhussayen, A.A.; Jambi, K.; Khemakhem, M.; Eassa, F.E. A Blockchain oracle interoperability technique for permissioned blockchain. *IEEE Access* **2024**, *12*, 68130–68148. [CrossRef]
81. Nasir, N.M.; Hassan, S.; Zaini, K.M. Securing permissioned blockchain-based systems: An analysis on the significance of consensus mechanisms. *IEEE Access* **2024**, *12*, 138211–138238. [CrossRef]
82. Ucbas, Y.; Eleyan, A.; Hammoudeh, M.; Alohaly, M. Performance and scalability analysis of Ethereum and Hyperledger Fabric. *IEEE Access* **2023**, *11*, 67156–67167. [CrossRef]
83. Byers, B.; Hunhevicz, J.J.; Honic-Eser, M.; De Wolf, C. Exploring tokenized product passports for circular construction supply chains. In Proceedings of the European Conference on Computing in Construction, Chania, Crete, Greece, 14–17 July 2024; pp. 34–41.
84. Honar Pajooh, H.; Rashid, M.; Alam, F.; Demidenko, S. Hyperledger fabric blockchain for securing the edge ınternet of things. *Sensors* **2021**, *21*, 359. [CrossRef] [PubMed]
85. Ravi, D.; Ramachandran, S.; Vignesh, R.; Falmari, V.R.; Brindha, M. Privacy preserving transparent supply chain management through Hyperledger Fabric. *Blockchain Res. Appl.* **2022**, *3*, 100072. [CrossRef]
86. Mitani, T.; Otsuka, A. Traceability in permissioned blockchain. *IEEE Access* **2020**, *8*, 21573–21588. [CrossRef]
87. Xue, Y.; Wang, J. Design of a blockchain-based traceability system with a privacy-preserving scheme of zero-knowledge proof. *Secur. Commun. Netw.* **2022**, *2022*, 5842371. [CrossRef]
88. Ishii, D. Mathematical definiton of zero-knowledge proofs: Concepts and examples. *Res. Propos.* **2025**. [CrossRef]
89. Prasad, S.; Tiwari, N. Zero-knowledge proofs in blockchain-enabled supply chain management. In *Sustainable Security Practices Using Blockchain, Quantum and Post-Quantum Technologies for Real Time Applications*; Springer Nature: Singapore, 2024; pp. 47–70.
90. Guo, H.; Yu, X. A survey on blockchain technology and its security. *Blockchain Res. Appl.* **2022**, *3*, 100067. [CrossRef]
91. Samantray, B.S.; Reddy, K.H.K. A novel secure supply chain for smart healthcare systems: An approach to leverage blockchain, Keccak-256, and ZKP for drug safety assurance. *Peer-to-Peer Netw. Appl.* **2025**, *18*, 16. [CrossRef]
92. Zhang, B.; Xu, J.; Wang, X.; Zhao, Z.; Chen, S.; Zhang, X. Research on the construction of grain food multi-chain blockchain based on zero-knowledge proof. *Foods* **2023**, *12*, 1600. [CrossRef]
93. Nithin, G.N.; Pradhan, A.K.; Swain, G. zkHealthChain-blockchain enabled supply chain in healthcare using zero knowledge. In *IFIP International Internet of Things Conference*; Springer: Cham, Switzerland, 2023; pp. 133–148.
94. Anita, N.; Vijayalakshmi, M.; Shalinie, S.M. Blockchain-based anonymous anti-counterfeit supply chain framework. *Sādhanā* **2022**, *47*, 208. [CrossRef]
95. Daraghmi, E.Y.; Jayousi, S.; Daraghmi, Y.A.; Daraghma, R.S.M.; Fouchal, H. Smart contracts for managing the agricultural supply chain: A practical case study. *IEEE Access* **2024**, *12*, 125462–125479. [CrossRef]
96. Agostinelli, S.; Arman, A.; De Luzi, F.; Monti, F.; Manglaviti, M.; Mecella, M. Supporting business confidentiality in coopetitive scenarios: The B-CONFIDENT approach in blockchain-based supply chains. *J. Ind. Inf. Integr.* **2024**, *42*, 100730. [CrossRef]
97. Al-Rakhami, M.; Al-Mashari, M. Interoperability approaches of blockchain technology for supply chain systems. *Bus. Process Manag. J.* **2022**, *28*, 1251–1276. [CrossRef]
98. Mao, H.; Nie, T.; Sun, H.; Shen, D.; Yu, G. A survey on cross-chain technology: Challenges, development, and prospect. *IEEE Access* **2022**, *11*, 45527–45546. [CrossRef]
99. Duan, L.; Sun, Y.; Ni, W.; Ding, W.; Liu, J.; Wang, W. Attacks against cross-chain systems and defense approaches: A contemporary survey. *IEEE/CAA J. Autom. Sin.* **2023**, *10*, 1647–1667. [CrossRef]
100. Peng, X.; Zhang, X.; Wang, X.; Li, H.; Xu, J.; Zhao, Z.; Wang, Y. Research on the cross-chain model of rice supply chain supervision based on parallel blockchain and smart contracts. *Foods* **2022**, *11*, 1269. [CrossRef]
101. Wang, Y.; Cheng, T.; Xi, J. SCT-CC: A supply chain traceability system based on cross-chain technology of blockchain. In Proceedings of the Intelligent Computing and Block Chain: First BenchCouncil International Federated Conferences, Qingdao, China, 30 October–3 November 2021; pp. 281–293.
102. Seven Key Cross-Chain Bridge Vulnerabilities Explained. Available online: https://chain.link/education-hub/cross-chain-bridge-vulnerabilities (accessed on 2 April 2025).
103. Polkadot Platform: Whitepaper. Available online: https://polkadot.com/papers (accessed on 2 April 2025).
104. Cosmos Platform. IBC Versus Other Interoperability Solutions. Available online: https://ibcprotocol.dev/interoperability-solution-comparison (accessed on 2 April 2025).

105. Tortola, D.; Lisi, A.; Mori, P.; Ricci, L. Tethering Layer 2 solutions to the blockchain: A survey on proving schemes. *Comput. Commun.* **2024**, *225*, 289–310. [CrossRef]
106. Augusto, A.; Belchior, R.; Correia, M.; Vasconcelos, A.; Zhang, L.; Hardjono, T. SoK: Security and privacy of blockchain interoperability. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2024.
107. Durán, C.; Yazdi, A.K.; Derpich, I.; Tan, Y. Leveraging blockchain for maritime port supply chain management through multicriteria decision making. *Mathematics* **2024**, *12*, 1511. [CrossRef]
108. Tan, B.Q.; Wang, F.; Kang, J.L.K.; Costa, F. A blockchain-based framework for green logistics in supply chains. *Sustainability* **2020**, *12*, 4656. [CrossRef]
109. Alqarni, M.A.; Alkatheiri, M.S.; Chauhdary, S.H.; Saleem, S. Use of blockchain-based smart contracts in logistics and supply chains. *Electronics* **2023**, *12*, 1340. [CrossRef]
110. Zhang, G.; Zhang, Z. An evolutionary game model of a regional logistics service supply chain complex network in a blockchain environment. *Systems* **2025**, *13*, 32. [CrossRef]
111. Alkhodair, M.; Alkhudhayr, H. Harnessing industry 4.0 for SMEs: Advancing smart manufacturing and logistics for sustainable supply chains. *Sustainability* **2025**, *17*, 813. [CrossRef]
112. Panigrahi, A.; Pati, A.; Dash, B.; Sahoo, G.; Singh, D.; Dash, M. ASBlock: An agricultural based supply chain management using blockchain technology. *Procedia Comput. Sci.* **2024**, *235*, 1943–1952. [CrossRef]
113. Mokgomola, F.; Telukdarie, A.; Munien, I.; Onkonkwo, U.; Vermeulen, A. Blockchain and smart contracts based agricultural supply chain. *Procedia Comput. Sci.* **2024**, *237*, 637–644. [CrossRef]
114. Chen, F.; Zhao, C.; Yang, X.; Luo, N.; Sun, C. A lightweight accountable parallel blockchain architecture based on redactable blockchain for agri-food traceability. *Foods* **2025**, *14*, 623. [CrossRef]
115. Wang, L.; Sun, W.; Zhao, J.; Zhang, X.; Lu, C.; Luo, H. A non-fungible token and blockchain-based cotton lint traceability solution. *Appl. Sci.* **2024**, *14*, 1610. [CrossRef]
116. Morais, R.; Rosado da Cruz, A.M.; Cruz, E.F. Fruit and vegetables blockchain-based traceability platform. *Computers* **2024**, *13*, 112. [CrossRef]
117. Ahuja, R.; Chugh, S.; Singh, R. SeedChain: A secure and transparent blockchain-driven framework to revolutionize the seed supply chain. *Future Internet* **2024**, *16*, 132. [CrossRef]
118. Farooq, M.S.; Riaz, S.; Rehman, I.U.; Khan, M.A.; Hassan, B. A blockchain-based framework to make the rice crop supply chain transparent and reliable in agriculture. *Systems* **2023**, *11*, 476. [CrossRef]
119. Rizzardi, A.; Sicari, S.; Cevallos, M.J.F.; Coen-Porisini, A. IoT-driven blockchain to manage the healthcare supply chain and protect medical records. *Future Gener. Comput. Syst.* **2024**, *161*, 415–431. [CrossRef]
120. Shah, D.; Rani, S.; Shoukat, K.; Kalsoom, H.; Shoukat, M.U.; Almujibah, H.; Liao, S. Blockchain factors in the design of smart-media for e-healthcare management. *Sensors* **2024**, *24*, 6835. [CrossRef] [PubMed]
121. Arvizo, A.I.M.; Sosa, L.A.; Alcaraz, J.L.G.; Cruz-Mejía, O. Beneficiary contracts on a lightweight blockchain architecture using smart contracts: A smart healthcare system for medical records. *Appl. Sci.* **2024**, *13*, 6694. [CrossRef]
122. Abutaleb, R.A.; Alqahtany, S.S.; Syed, T.A. Integrity and privacy-aware, patient-centric health record access control framework using a blockchain. *Appl. Sci.* **2023**, *13*, 1028. [CrossRef]
123. Perumalsamy, S.; Kaliyamurthy, V. Blockchain non-fungible token for effective drug traceability system with optimal deep learning on pharmaceutical supply chain management. *Eng. Technol. Appl. Sci. Res.* **2025**, *15*, 19261–19266. [CrossRef]
124. Azzaoui, A.E.; 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]
125. Aslam, M.; Jabbar, S.; Abbas, Q.; Albathan, M.; Hussain, A.; Raza, U. Leveraging Ethereum platform for development of efficient tractability system in pharmaceutical supply chain. *Systems* **2023**, *11*, 202. [CrossRef]
126. Mishra, R.; Ramesh, D.; Edla, D.R.; Qi, L. VaccineChain: A checkpoint assisted scalable blockchain based secure vaccine supply chain with selective revocation. *J. Ind. Inf. Integr.* **2023**, *34*, 100485. [CrossRef]
127. Mezquita, Y.; Podgorelec, B.; Gil-González, A.B.; Corchado, J.M. Blockchain-based supply chain systems, interoperability model in a pharmaceutical case study. *Sensors* **2023**, *23*, 1962. [CrossRef]
128. Humayun, M.; Jhanjhi, N.Z.; Niazi, M.; Amsaad, F.; Masoo, I. Securing drug distribution systems from tampering using blockchain. *Electronics* **2022**, *11*, 1195. [CrossRef]
129. Chandrasekaran, S. Isogency hosmer–lemeshow logistic regression-based secured information sharing for pharma supply chain. *Electronics* **2022**, *11*, 3170. [CrossRef]
130. Islam, I.; Islam, M.N. A blockchain based medicine production and distribution framework to prevent medicine counterfeit. *J. King Saud Univ.-Comput. Inf. Sci.* **2024**, *36*, 101851. [CrossRef]
131. Arsheen, S.; Ahmad, K. ImmuneChain: A blockchain-based secure and transparent vaccine supply chain. *SN Comput. Sci.* **2025**, *6*, 40. [CrossRef]

132. Mishra, R.; Ramesh, D.; Mohamm, N.; Mondal, B. Blockchain enabled secure pharmaceutical supply chain framework with traceability: An efficient searchable pharmachain approach. *Clust. Comput.* **2024**, *27*, 13621–13641. [CrossRef]
133. Vitaskos, V.; Demestichas, K.; Karetsos, S.; Costopoulou, C. Blockchain and Internet of Things technologies for food traceability in olive oil supply chains. *Sensors* **2024**, *24*, 8189. [CrossRef] [PubMed]
134. Sharma, I.; Kaur, G.; Dey, B.K.; Majumder, A. Leveraging blockchain and consignment contracts to optimize food supply chains under uncertainty. *Appl. Sci.* **2024**, *14*, 11735. [CrossRef]
135. Adamashvili, N.; Zhizhilashvili, N.; Tricase, C. The integration of the internet of things, artificial intelligence, and blockchain technology for advancing the wine supply chain. *Computers* **2024**, *13*, 72. [CrossRef]
136. Toader, D.C.; Rădulescu, C.M.; Toader, C. Investigating the adoption of blockchain technology in agri-food supply chains: Analysis of an extended UTAUT model. *Agriculture* **2024**, *14*, 614. [CrossRef]
137. Cao, S.; Xu, H.; Bryceson, K.P. Blockchain traceability for sustainability communication in food supply chains: An architectural framework, design pathway and considerations. *Sustainability* **2023**, *15*, 13486. [CrossRef]
138. Ahamed, N.N.; Karthikeyan, P. FLBlock: A sustainable food supply chain approach through federated learning and blockchain. *Procedia Comput. Sci.* **2024**, *235*, 3065–3074. [CrossRef]
139. Zhang, Y.; Wu, X.; Ge, H.; Jiang, Y.; Sun, Z.; Ji, X.; Jia, Z.; Cui, G. A blockchain-based traceability model for grain and oil food supply chain. *Foods* **2023**, *12*, 3235. [CrossRef] [PubMed]
140. Kechagias, E.P.; Gayialis, S.P.; Papadopoulos, G.A.; Papoutsis, G. An Ethereum-based distributed application for enhancing food supply chain traceability. *Foods* **2023**, *12*, 1220. [CrossRef]
141. Agarwal, U.; Rishiwal, V.; Shiblee, M.; Yadav, M.; Tanwar, S. Blockchain-based intelligent tracing of food grain crops from production to delivery. *Peer-to-Peer Netw. Appl.* **2024**, *17*, 3722–3749. [CrossRef]
142. Arvana, M.; Rocha, A.D.; Barata, J. Agri-food value chain traceability using blockchain technology: Portuguese hams' production scenario. *Foods* **2023**, *12*, 4246. [CrossRef]
143. Nazir, H.; Fan, J. Revolutionizing retail: Examining the influence of blockchain-enabled IoT capabilities on sustainable firm performance. *Sustainability* **2024**, *16*, 3534. [CrossRef]
144. Yu, T.; Guan, Z.; Zhan, J.; Dong, J. Blockchain adoption and contract coordination of poverty alleviation supply chain considering altruistic preference. *Comput. Ind. Eng.* **2024**, *188*, 109879. [CrossRef]
145. Ekinci, E.; Sezer, M.D.; Mangla, S.K.; Kazancoglu, Y. Building sustainable resilient supply chain in retail sector under disruption. *J. Clean. Prod.* **2024**, *434*, 139980. [CrossRef]
146. Rajagopal, M.; Ramkumar, S.; Thimmiaraja, J.; Gobinath, R.; Kumar, K.S. Blockchain-based model for disaster relief supply chain management. In *The Role of Blockchain in Disaster Management*; Academic Press: Cambridge, MA, USA, 2025; pp. 33–49.
147. Roushan, A.; Das, A.; Dutta, A.; Bera, U.K. A multi-objective supply chain model for disaster relief optimization using neutrosophic programming and blockchain-based smart contracts. *Supply Chain. Anal.* **2025**, *10*, 100107. [CrossRef]
148. Gao, X.; Chen, Z.; Huang, G.; Hezam, I.M. Blockchain-enabled safeguard mechanism in SCP-based relief supply chain designs in response to long-term disasters. *IEEE Access* **2024**, *12*, 133054–133066. [CrossRef]
149. Inayatulloh; Susanto, B.H.; Setiabudiarto, N.; Teguh, W.; Jariyah, A. Blockchain technology model to increase transparency in the distribution of aid to disaster victims. In Proceedings of the IEEE 2nd International Conference on Electrical Engineering, Computer and Information Technology (ICEECIT), Jember, Indonesia, 22–23 November 2024; pp. 222–226.
150. Darmawan, B.; Okitasarı, H.; Dwiyanti, V.; Pratama, P.Y.; Haritman, E. Preliminary research: Blockchain system design for post-disaster management in Indonesia. *J. Eng. Sci. Technol.* **2024**, *19*, 1268–1279.
151. Ankit, K.C. Blockchain based donation management in disaster response. *J. Innov. Inf. Technol. Appl. (JINITA)* **2024**, *6*, 45–59.
152. Lotfi, R.; Nasrabadi, A.M.; Ali, S.S.; Mardani, N.; Davoodi, S.M.R.; Aghakhani, S. A viable relief supply chain network design by considering risk and robustness for disaster and crisis management. *Cent. Eur. J. Oper. Res.* **2024**, 1–36. [CrossRef]
153. Kolhatkar, D.; Jain, O.; Patil, S.; Shelke, P.; Mirajkar, R.; Wawage, P. Blockchain applications in disaster management systems. In Proceedings of the 2023 4th International Conference for Emerging Technology (INCET), Belgaum, India, 26–28 May 2023; pp. 1–7.
154. Mandal, S.; Kar, A.K.; Gupta, S.; Sivarajah, U. Achieving food supply chain resilience during natural disasters through industry 5.0 enablers-empirical insights based on an FsQCA approach. *Inf. Syst. Front.* **2023**, 1–24. [CrossRef]
155. Rai, H.; Srivastava, A.K.; Rai, S.; Pattanashetti, D. Blockchain-powered transparency: Tracking and disseminating donations for disaster-stricken regions. In *Futuristic Trends in Artificial Intelligence*; IIP Series: Chikkamagaluru, India, 2024; pp. 1–15.
156. Mosallanezhad, B.; Hajiaghaei-Keshteli, M.; Cornejo, N.R.S.; Calvo, E.Z.R. An IoMT platform for an integrated sustainable energy-efficient disaster relief supply chain to prevent severity-driven disruptions during pandemics. *J. Ind. Inf. Integr.* **2023**, *35*, 100502. [CrossRef]
157. Zachariah, M.; Avanesh, N.M.; Raghupathi, K. Application of blockchain technology in disaster risk management. In *The Role of Blockchain in Disaster Management*; Academic Press: Cambridge, MA, USA, 2025; pp. 87–110.
158. Das, N.; Basu, S.; Bit, S.D. ReliefChain: A blockchain leveraged post disaster relief allocation system over smartphone-based DTN. *Peer-to-Peer Netw. Appl.* **2022**, *15*, 2603–2618. [CrossRef] [PubMed]

159. Khairuddin, I.E.; Zaini, M.K.; Ghazali, A.K. Decentralized distribution of humanitarian aid for natural disaster relief. *Environ. Behav. Proc. J.* **2022**, *7*, 233–239. [CrossRef]
160. Garazha, A.; Merz, C.; Schwabe, G.; Zavolokina, L. Resilience in times of crisis: Empowering refugees with self-sovereign identity. In Proceedings of the International Conference on Information Systems (ICIS), Bangkok, Thailand, 15–18 December 2024; p. 3135.
161. Harini, S.; Suraj, K.; Kumar, M.V. Blockchain-based certificate generation and validation system for refugees. In Proceedings of the International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bangalore, India, 16–17 January 2025; pp. 1–5.
162. Abraha, D.T. Blockchain-based solution for addressing refugee management in the Global South: Transparent and accessible resource sharing in humanitarian organizations. *Front. Hum. Dyn.* **2025**, *6*, 1391163. [CrossRef]
163. Ungar, M.; Seymour, A. Access without borders: A scoping review to identify solutions to creating portable identity, education and health records for refugee children. *J. Int. Migr. Integr.* **2024**, *25*, 1989–2017. [CrossRef]
164. Cheesman, M. Conjuring a blockchain pilot: Ignorance and innovation in humanitarian aid. *Geopolitics* **2024**, *30*, 1073–1100. [CrossRef]
165. Yang, Y.; Ma, C.; Zhou, J.; Dong, S.; Ling, G.; Li, J. A multi-dimensional robust optimization approach for cold-chain emergency medical materials dispatch under COVID-19: A case study of hubei province. *J. Traffic Transp. Eng.* **2022**, *9*, 1–20. [CrossRef]
166. Zeng, W.; Wang, Y.; Liang, K.; Li, J.; Niu, X. Advancing emergency supplies management: A blockchain-based traceability system for cold-chain medicine logistics. *Adv. Theory Simul.* **2024**, *7*, 2300704. [CrossRef]
167. Shivale, N.; Patwal, P.S.; Mahalle, P. Enhanced traceability and transparency in medical supply chain management using blockchain-based customized smart contracts. *J. Inf. Syst. Eng. Manag.* **2025**, *10*, 478–489.
168. Kumar, P.; Singh, R.K.; Shahgholian, A. Learnings from COVID-19 for managing humanitarian supply chains: Systematic literature review and future research directions. *Ann. Oper. Res.* **2024**, *335*, 899–935. [CrossRef]
169. Kumar, V.V.; Sahoo, A.; Balasubramanian, S.K.; Gholston, S. Mitigating healthcare supply chain challenges under disaster conditions: A holistic AI-based analysis of social media data. *Int. J. Prod. Res.* **2025**, *63*, 779–797. [CrossRef]
170. Lathkar, M.; Deshmukh, P.; Patil, A.; Shelke, P. Increasing donation transparency in disaster relief: A Blockchain-based solution. In Proceedings of the ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS), Manama, Bahrain, 28–29 January 2024; pp. 1527–1532.
171. Sangeetha, V.; Dargar, A.; Jariwala, J.; Rai, R.H.; Agarwala, S. Unified blockchain platform for charitable donations, crowdfunding and CSR. In Proceedings of the International Conference on Distributed Computing and Optimization Techniques (ICDCOT), Bengaluru, India, 15–16 March 2024; pp. 1–6.
172. Chen, C.L.; Zhan, W.B.; Tsaur, W.J.; Huang, D.C.; Liu, L.C. Constructing a secure charity NFT auction platform using fisco bcos blockchain for enhancing transparency and traceability. *IEEE Access* **2024**, *12*, 36924–36941. [CrossRef]
173. Raipurkar, A.R.; Chandak, M.B.; Sorathia, A.; Mankar, I.; Tapkire, P.; Pophali, P. Blockchain based genuine and transparent charity application. *J. Theor. Appl. Inf. Technol.* **2024**, *102*, 1240–1249.
174. Yang, C.; Lin, C.; Zhao, W.; Cui, J. A novel blockchain-based charitable model combined with insurance. *Geneva Pap. Risk Insur.-Issues Pract.* **2025**, *50*, 185–202. [CrossRef]
175. Migliorini, S.; Gambini, M.; Belussi, A. A blockchain-based platform for ensuring provenance and traceability of donations for cultural heritage. *Blockchain Res. Appl.* **2025**, 100278. [CrossRef]
176. Novak, M. Crypto altruism: Applying blockchain to charitable and humanitarian activities. *Chin. Public Adm. Rev.* **2023**, *15*, 11–23. [CrossRef]
177. Ellahi, R.M.; Wood, L.C.; Bekhit, A.E.D.A. Blockchain-driven food supply chains: A systematic review for unexplored opportunities. *Appl. Sci.* **2024**, *14*, 8944. [CrossRef]
178. Guixia, X.; Samian, N.; Faizal, M.F.M.; As'ad, M.A.Z.M.; Fadzil, M.F.M.; Abdullah, A.; Seah, W.K.G.; Ishak, M.; Hermadi, I. A framework for blockchain and internet of things integration in improving food security in the food supply chain. *J. Adv. Res. Appl. Sci. Eng. Technol.* **2024**, *34*, 24–37. [CrossRef]
179. Gupta, R.; Shankar, R. Managing food security using blockchain-enabled traceability system. *Benchmarking Int. J.* **2024**, *31*, 53–74. [CrossRef]
180. Hamidoğlu, A.; Gül, Ö.M.; Kadry, S.N. A game-theoretical approach for the adoption of government-supported blockchain application in the IoT-enabled agricultural supply chain. *Internet Things* **2024**, *26*, 101163. [CrossRef]
181. Sharma, R.; Samad, T.A.; Jabbour, C.J.C.; de Queiroz, M.J. Leveraging blockchain technology for circularity in agricultural supply chains: Evidence from a fast-growing economy. *J. Enterp. Inf. Manag.* **2025**, *38*, 32–67. [CrossRef]
182. Wang, S.; Ghadge, A.; Aktas, E. Digital transformation in food supply chains: An implementation framework. *Supply Chain. Manag. Int. J.* **2024**, *29*, 328–350. [CrossRef]
183. Egunjobi, O.O.; Gomes, A.; Egwim, C.N.; Morais, H. A systematic review of blockchain for energy applications. *e-Prime-Adv. Electr. Eng. Electron. Energy* **2024**, *9*, 100751. [CrossRef]

184. Asif, R.; Hassan, S.R. Shaping the future of Ethereum: Exploring energy consumption in Proof-of-Work and Proof-of-Stake consensus. *Front. Blockchain* **2023**, *6*, 1151724. [CrossRef]
185. Pankovska, E.; Sai, A.R.; Vranken, H.; Ransil, A. Electricity consumption of Ethereum and Filecoin: Advances in models and estimates. In Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing, Avila, Spain, 8–12 April 2024; pp. 269–277.