Archives available at journals.mriindia.com

International Journal of Electrical, Electronics and Computer Systems

ISSN: 2347 – 2820
Volume 14 Issue 01, 2025

Leveraging Block chain to Enhance Data Integrity and Cyber security in Supply Chain Operations

[1] Dr.Syed Umar, [2]Jyothinadh nadella, [3]Vinay Chowdary Dabbara, [4]Ramu Mannava, [5] Dr.Ramesh Safare

[1] Professor, Department of CSE, Malla Reddy Engineering College,Hyderabad India.
[2]Software Engineer, Verinon Technology solution's, U.S.A.
[3]Student, Webster University, Master's in Cyber security operations, U.S.A
[4]Senior SAP Functional Consultant, DEVFI INC, U.S.A.
[5]Associate Professor, Faculty of Management Studies, Marwadi University, Rajkot, India.
Email: [1]Umar332@gmail.com , [2]nadellajyothinadh@gmail.com, [3]dabbaravinaychowdary@gmail.com, [4]Ramu.mannava1@gmail.com, [5]ramesh.safare@marwadieducation.edu.in

Peer Review Information

Submission: 17 Feb 2025
Revision: 21 March 2025
Acceptance: 23 April 2025

Keywords

Blockchain Technology, Data Integrity, Cyber security, Supply Chain Operations, Smart Contracts, Distributed Ledger, Cyber Threats, Supply Chain Security.

Abstract

Supply chain operations that include blockchain technology have the potential to improve cybersecurity and data integrity. The complexity and interconnectedness of global supply chains make it imperative to guarantee the security and validity of data for all parties involved. Because blockchain technology is decentralized, transparent, and unchangeable, it offers a perfect solution to common supply chain weaknesses, including fraud, data tampering, and illegal access. The use of blockchain technology to protect important data at each link in the supply chain—from manufacturing and procurement to distribution and delivery—is examined in this article. By leveraging smart contracts, cryptographic security, and distributed ledger systems, blockchain can ensure the traceability of goods, validate transactions, and protect sensitive information from cyber threats. The paper also highlights how blockchain has the potential to completely transform supply chain management security while addressing issues like scalability, integration with current systems, and regulatory considerations. In the end, this study highlights how blockchain technology may improve data integrity, lower cyber threats, and foster trust among supply chain actors.

INTRODUCTION

In the rapidly evolving global economy, supply chains are becoming increasingly intricate, involving multiple stakeholders across various industries, geographic regions, and technological platforms. Throughout the supply chain lifecycle, this complexity creates major obstacles to preserving the security, integrity, and transparency of data [1]. Conventional supply chain data security techniques frequently depend on centralized systems, which are susceptible to fraud, data manipulation, cyber-attacks, and illegal access. As a result, the need for a robust, secure, and transparent approach to managing supply chain data has never been more critical.

Blockchain technology offers a novel way to deal with these issues because of its intrinsic decentralization, immutability, and transparency features. Blockchain creates a distributed ledger that records every transaction in a way that can't be changed or hacked, so data can be checked and tracked in real time across the supply chain network [2]. Smart contracts are an important part of blockchain technology. They make transactions even safer by automating and enforcing rules that have already been set. This

makes sure that everyone follows the terms of the agreement without the need for middlemen.
This study investigates the ways in which supply chain operations can benefit from the use of blockchain technology to improve cyber security and data integrity [3]. It talks about the problems that might stop it from being used, like how to make it work with existing systems, how to make it scalable, and how to make sure it follows the rules. It also looks at how blockchain could help protect data in the supply chain, make it easier to find, and make things more open [4]. The goal of this investigation is to demonstrate how blockchain can transform supply chain management by providing a safe, effective, and reliable framework for data handling, which will ultimately lower risks, stop fraud, and encourage increased cooperation among supply chain participants.

LEVERAGING BLOCKCHAIN TO ENHANCE DATA INTEGRITY AND CYBERSECURITY IN SUPPLY CHAIN OPERATIONS

It has become more challenging to guarantee the confidentiality, transparency, and correctness of data due to the complexity of global supply chains, which involve several stakeholders, procedures, and technology [5]. Conventional supply chain management systems frequently depend on centralized databases, which are susceptible to fraud, data manipulation, hacks, and illegal access. These hazards have the potential to undermine participant trust, interfere with operations, and result in monetary losses and harm to one's reputation. Innovative solutions that can improve data integrity and fortify cyber security are desperately needed as supply chains continue to grow and digitize.
A potent remedy for these issues is provided by blockchain technology, which is decentralized, transparent, and unchangeable [6]. Blockchain can provide accurate, tamper-proof information for all supply chain participants by offering a safe and verifiable way to record transactions. By securely recording each transaction in blocks and connecting them, this technology generates a distributed ledger that makes it nearly impossible to change or tamper with past data [7]. In order to ensure compliance and eliminate the need for middlemen, smart contracts integrated into the blockchain can also automate and enforce the terms of agreements between parties.
The potential of blockchain technology to improve cyber security and data integrity in supply chain operations is examined in this article. From procurement to delivery, it demonstrates how blockchain can enhance openness, accountability, and traceability at several points in the supply chain [8]. The report also tackles issues related to the deployment of blockchain technology, such as scalability, regulatory compliance, and interaction with existing systems. Lastly, it looks at the wider effects of blockchain technology on protecting supply networks from fraud, cyber-attacks, and other weaknesses. to look into the ways that blockchain might guarantee data integrity throughout the supply chain. To investigate how blockchain might improve cyber security and safeguard private information [9]. To evaluate the usefulness of integrating blockchain technology into supply chain management. to solve issues with supply chains' scalability and acceptance of blockchain technology.

LITERATURE SURVEY ANALYSIS

The incorporation of blockchain technology into supply chain management has drawn a lot of interest because it potentially solve enduring issues with cyber security, transparency, and data integrity. This review of the literature looks at different research, methods, and applications that use blockchain technology to increase supply chain data security and dependability. The technological prowess of blockchain, along with its possible advantages, drawbacks, and real-world applications, are important areas of study [10]. An immutable ledger that documents transactions across a network of computers is provided by blockchain technology, which is by its very nature distributed and decentralized. Because of its design, blockchain is impervious to fraud and manipulation. In a blockchain, every block is connected to the one before it, and once a block is created, any changes to its contents would need network consensus, guaranteeing data integrity.
Because a decentralized architecture does not require a central authority, the likelihood of single points of failure is decreased. Blockchain technology ensures the integrity of supply chain transactions by preventing data from being changed after it has been recorded. Consensus techniques like Proof of Stake (PoS) and Proof of Work (PoW) protect data from unwanted access [11]. Studies reveal that blockchain technology offers a revolutionary resolution to a number of supply chain management issues. Supply chains, for example, frequently deal with problems like fraud, counterfeiting, and data transparency. Businesses may use blockchain technology to track the flow of commodities and instantly confirm their legitimacy. By making transactions visible to all supply chain actors, blockchain's distributed ledger improves accountability and transparency. This is essential in sectors like luxury goods, pharmaceuticals, and food safety,

where confirming the provenance and legitimacy of products is critical.

Without the need for middlemen, these self-executing contracts automatically enforce agreed agreements. They are especially useful for protecting and automating intricate supply chain contracts [12]. Blockchain makes guarantees that every transaction is safely and publicly recorded, which lowers the likelihood of fraudulent activities like document fabrication and fake goods. Blockchain's contribution to improving data integrity throughout the supply chain. Blockchain guarantees that data is correct, comprehensive, and verifiable by logging each transaction in an unchangeable ledger. This lowers the possibility of fraud and mistakes that are frequently brought on by manual record-keeping. Blockchain ensures that all data stored is consistent across all participants, reducing the chances of discrepancies [13]. Blockchain allows for the real-time recording of events, which improves decision-making and operational efficiency.

The system's transparent nature means that stakeholders can easily audit the entire history of a product or transaction, providing strong evidence in case of disputes. One of the biggest issues with contemporary supply networks is still cybersecurity. Financial losses, reputational harm, and the theft of private information are all possible outcomes of a cybersecurity breach. Hash functions and public-private key encryption, two of blockchain's cryptographic security features, can be used to keep supply chain data safe [14]. Blockchain uses cutting-edge cryptography methods to protect data. Because each transaction is hashed and connected to the one before it, it is extremely difficult to tamper with. The likelihood of cyber-attacks targeting a single entity is much decreased because there is no central point of control. To improve access control and stop unwanted data modification, blockchain can be used with other technologies like biometrics or multi-factor authentication.

Although blockchain's potential to improve cybersecurity and data integrity is well known, there are a number of obstacles preventing its widespread use. Many blockchain networks face issues related to transaction speed and scalability. The limited processing speed of blockchain systems like Ethereum and Bit coin might cause bottlenecks in supply chains with significant traffic. It can be difficult and expensive to integrate blockchain with current supply chain management systems. Many organizations are hesitant to adopt blockchain due to the significant upfront investment required [15]. Blockchain adoption requires navigating legal and regulatory frameworks, which vary by region and industry. Ensuring that blockchain implementations comply with these regulations remains a key challenge. Future research in blockchain for supply chain management focuses on improving scalability and interoperability between blockchain networks. To increase transaction speed, innovations like Layer 2 solutions (off-chain processing) and sharding (breaking a blockchain into smaller, easier-to-manage pieces) are being investigated. Supply chains may also become smarter and more automated as a result of combining blockchain with other cutting-edge technologies like artificial intelligence (AI) and the internet of things (IoT). Blockchain has the potential to greatly improve cybersecurity and data integrity in supply chain processes, according to the literature. Blockchain solves important issues like fraud, data tampering, and cybersecurity flaws by offering a safe, transparent, and impenetrable way to record transactions. However, before blockchain can be extensively used, issues with scalability, system integration, and regulatory compliance need to be resolved. Further research is needed to refine blockchain solutions, making them more scalable, efficient, and compatible with existing supply chain systems.

EXISTING APPROCHES

There is growing interest in using blockchain technology to improve cybersecurity and data integrity in supply chain operations. Various approaches have been explored by both researchers and practitioners to address issues such as fraud, data manipulation, and unauthorized access in supply chains. The following outlines the main strategies now in use for utilizing blockchain technology to enhance the security, accuracy, and transparency of data in supply chain networks. Offering real-time tracking and traceability of commodities is one of the most popular ways to employ blockchain technology in supply chain operations. With blockchain, every transaction and movement of items is recorded on a decentralized ledger, giving everyone access to the same, unchangeable information on the location and status of assets. This reduces the risk of counterfeiting, diversion, or theft and provides complete visibility of product journeys from production to delivery.

In order to provide openness and traceability, especially in the area of food safety, IBM's Food Trust Network tracks food products from farm to table using blockchain technology. improved supply chain accountability and transparency, which will help verify product origins and stop

fraud and improper handling of items. Smart contracts, self-executing agreements, directly encode the conditions of the agreement into lines of code. These contracts can be carried out using blockchain technology without the need for middlemen. When certain conditions are met, smart contracts automatically enforce and carry out established regulations, guaranteeing that all supply chain participants abide by the agreements that have been agreed upon. This reduces the possibility of human errors or intentional manipulation of agreements.

De Beers, the global diamond company, uses blockchain-powered smart contracts to verify the authenticity of diamonds and manage contracts with suppliers. Payments and shipment deliveries are automatically executed once certain conditions are met. Increased trust between parties, reduced reliance on intermediaries, and minimized fraud or contract breaches. Blockchain's inherent cryptographic features are a key element in enhancing cybersecurity within supply chain operations. By securing data exchanges with encryption and hashing, blockchain ensures that sensitive information cannot be altered or tampered with without being detected. Blockchain technology can enable safe data sharing between numerous parties while preserving confidentiality and integrity, which is essential for sectors like government, healthcare, and finance that handle sensitive data. Blockchain technology is being used in healthcare supply chains to guarantee safe patient data exchange between parties while upholding stringent data privacy laws, like HIPAA compliance.

Improved security for sharing sensitive information, with data integrity assured by the immutability of blockchain records. Supply chains are particularly vulnerable to fraud, such as the falsification of shipment records, misrepresentation of product origins, or diversion of goods. Blockchain's transparent, immutable ledger makes it difficult to alter records without detection, which helps mitigate fraud risks. By monitoring every stage of the supply chain process and making every transaction publicly transparent (or available to authorized parties), blockchain helps guard against record tampering and guarantees that the transaction history can be audited whenever necessary. Luxury goods producers, such as LVMH, utilise blockchain technology to verify the authenticity of expensive goods and prevent product counterfeiting. This approach reduces the opportunities for fraud and counterfeiting, while also enabling quick and accurate audits and verifications of product histories.

In supply chains, privacy and regulatory compliance are major concerns. Public blockchains offer transparency but may not always be appropriate when privacy is crucial. Permissioned blockchains, on the other hand, restrict access to authorized parties and can be used to create more controlled environments that still leverage block chain's strengths in security and data integrity. Businesses like Walmart track items in a private blockchain network using hyper ledger Fabric, an enterprise-grade permissioned blockchain technology that makes sure that only people they can trust can access the data. Adherence to privacy laws (such as GDPR and HIPAA) while continuing to take advantage of block chain's advantages for data integrity and transparency. Blockchain can also enhance data integrity in the financial transactions that occur within supply chains. Blockchain technology can help businesses guarantee the traceability and transparency of financial activities by facilitating supply chain financing and payments. Blockchain-based solutions can help cut down on delays, simplify payments, and remove the fraud risks that come with using traditional financial intermediaries.

TradeLens, a blockchain-based shipping and logistics platform, integrates financial transactions into its supply chain ecosystem, allowing for seamless, transparent payment processes between suppliers, manufacturers, and logistics companies. TradeLens facilitates faster and more transparent payment systems, thereby reducing delays and ensuring financial integrity within the supply chain. Given that supply chains often involve multiple stakeholders across different geographic regions and industries, ensuring interoperability between various blockchain networks is crucial. To enable smooth data sharing and communication between various blockchain systems, multi-chain solutions and bridges are being created. This guarantees the integration of data from many sources, increasing the transparency and security of the supply chain as a whole. The combination of various blockchain networks, such as Ethereum and Hyperledger, in a unified system that enables smooth data exchange across different platforms in a global supply chain.

This results in enhanced collaboration between different stakeholders, with seamless data sharing and integration across blockchain networks. Blockchain technology combined with Internet of Things (IoT) devices offers improved visibility and control over commodities while they are in transit. Temperature, humidity, and location are just a few of the variables that IoT

sensors can monitor in real time. Product quality and integrity can be ensured by recording this data on a blockchain, which offers unchangeable evidence of the storage and transportation circumstances of goods. The use of IoT-enabled sensors to monitor temperature-sensitive products, such as pharmaceuticals or perishable goods, where blockchain records real-time data to ensure that goods have been stored and transported under the required conditions. Improved monitoring and assurance of product quality, with tamper-proof records that can be audited to verify conditions throughout the supply chain.

The existing approaches for leveraging blockchain to enhance data integrity and cybersecurity in supply chains offer diverse and impactful solutions to longstanding problems. The decentralized, irreversible, and transparent nature of blockchain technology offers substantial benefits for protecting supply chain processes, from enhancing traceability and transparency to automating contract execution and guaranteeing secure data sharing. But issues like regulatory compliance, scalability, and integration with older systems still need to be resolved. Further research and development are required to refine these approaches and expand block chain's applicability across different industries.

PROPOSED METHOD

In the context of contemporary supply chain management, utilizing blockchain technology to improve cybersecurity and data integrity is crucial for resolving the many flaws in conventional methods. A unique, multi-layered strategy is put out to accomplish this, enabling a more secure, transparent, and effective supply chain by fusing blockchain's decentralized ledger capabilities with auxiliary technologies like smart contracts, the Internet of Things, and encryption techniques. A hybrid blockchain architecture that strikes a compromise between supply chain actors' privacy needs and transparency requirements is what the suggested approach promotes. This architecture combines both public and permissioned blockchains, where sensitive data (e.g., pricing, contracts, and proprietary business processes) is stored on permissioned blockchains accessible only to authorized parties, while public blockchains are used for verification and tracking purposes.

The system stores verifiable transaction data, such as timestamps, product movements, and basic event logs, making it accessible to all participants for transparency. The system stores sensitive business and financial data, guaranteeing that only verified participants can access or update critical records. This reduces the risks associated with exposing sensitive information to the public while still ensuring the integrity of transactions. This hybrid approach guarantees not only transparency across the supply chain but also privacy, adhering to regulatory standards like GDPR. The suggested approach allows for real-time monitoring and data capture by integrating blockchain technology with Internet of Things (IoT) devices. Numerous supply chain factors, including temperature, humidity, location, and the state of products in transit, can be monitored by IoT sensors. Each IoT device is paired with a blockchain ledger that records the sensor data in real time.

IoT sensors continuously collect environmental and movement data, such as temperature fluctuations for perishable goods or geolocation data for tracking shipments. All permitted supply chain parties can access this transparent and unchangeable record, which is created when this real-time data is hashed and safely stored on the blockchain. If something isn't right (like the temperature going above what's safe), smart contracts can send alerts and take automatic actions (like rerouting shipments or letting the right people know), making sure that problems are dealt with before they happen. By ensuring that the data gathered is unchangeable and verifiable at every point in the supply chain, this approach protects the integrity and quality of the final product. Smart contracts are a key component of the proposed method for enhancing both data integrity and cybersecurity. There is less need for middlemen and human involvement thanks to these self-executing contracts, which automate and enforce adherence to predetermined terms. The smart contracts would be programmed to execute automatically upon the fulfillment of conditions, such as shipment delivery or payment confirmation.

Upon the confirmation of conditions (e.g., goods delivered to a specific location), the smart contract executes automatically, ensuring that payments are processed and invoices are generated without delay. By incorporating compliance checks into the contract code, smart contracts can also be used to guarantee that all parties involved adhere to legal obligations. For example, blockchain can be used to verify that certain standards (e.g., quality certifications, origin of goods) have been met before allowing a transaction to proceed. Through the elimination of errors and the reduction of fraud opportunities, smart contracts greatly improve the efficiency and security of supply chain

transactions. Multi-layered encryption and authentication procedures are used in the suggested approach to further improve cybersecurity and safeguard private information kept on both public and permissioned blockchains. These safeguards are intended to stop illegal access, guarantee data integrity, and protect against online threats. Blockchain transactions would require multi-factor authentication from participants, ensuring that only authorized entities can make changes to the blockchain ledger. MFA can include biometrics, password authentication, and cryptographic keys. Data transmitted between stakeholders in the supply chain will be encrypted using advanced encryption standards (AES-256) to ensure that sensitive information remains confidential. Data security is further strengthened by blockchain's intrinsic use of cryptographic hashing, both in transit and at rest. Blockchain uses PKI to securely handle keys and provide digital signatures, ensuring the authenticity and verifiability of every transaction. Supply chain data is protected and impenetrable because to these cryptographic methods and the intrinsic immutability of blockchain technology.

In the suggested method, blockchain would also have real-time auditing features to make sure that everyone in the supply chain has access to a record of every event and transaction that can't be changed and is time-stamped. This feature would greatly increase transparency and confidence among all parties. A transparent and auditable supply chain is made possible by the time stamping and linking of every transaction in the blockchain network to the one before it. To ensure complete supply chain visibility, authorized stakeholders (suppliers, manufacturers, logistics providers, and customers) can examine product statuses, invoices, and contracts at any time. Utilizing blockchain analytics tools can improve the capacity to monitor trends, spot inefficiencies, and evaluate supply chain risk concerns. Not only does this transparency increase confidence between supply chain partners, but it also facilitates the detection and mitigation of possible fraud, theft, and data manipulation problems.

Scalability is one of the main drawbacks of blockchain technology. The suggested approach uses Layer 2 technologies (like Lightning Network) to deal with large transaction volumes and lessen the strain on the primary blockchain network. We also propose cross-chain interoperability frameworks like blockchain bridges to facilitate communication among various blockchain systems within the supply chain ecosystem. These technologies greatly improve the network's speed and scalability by processing transactions off-chain and settling them on the main blockchain. Interoperability solutions will make it possible for data to flow smoothly between different blockchains in global supply chains. This way, all stakeholders can access the same, accurate data, no matter which platform they use.

These scalability solutions will ensure that the blockchain-based supply chain system can handle increasing transaction volumes while maintaining security and efficiency. Designing the system with compliance in mind is crucial to guaranteeing that the suggested approach is both safe and complies with international laws (such as GDPR and HIPAA). Blockchain networks will implement privacy-by-design principles, ensuring that personally identifiable information (PII) is encrypted and that only authorized entities can access or process it. Additionally, supply chain participants will need to be trained in the best practices for blockchain implementation to ensure smooth adoption. We will utilise permitted blockchains to adhere to privacy requirements and guarantee that only authorised parties can access sensitive data. By automating compliance checks, smart contracts can ensure that goods fulfil legal requirements before they are offered for sale or distribution.

The suggested approach of using blockchain to improve cybersecurity and data integrity in supply chain operations offers a complete answer to the fundamental problems of privacy, data security, transparency, and fraud prevention. This method creates a safe, effective, and expandable framework for modern supply chains by combining hybrid blockchain architecture, IoT, smart contracts, and advanced encryption methods. This method not only enhances operational efficiency but also builds trust among supply chain participants, enabling more resilient and secure supply chains.

RESULT

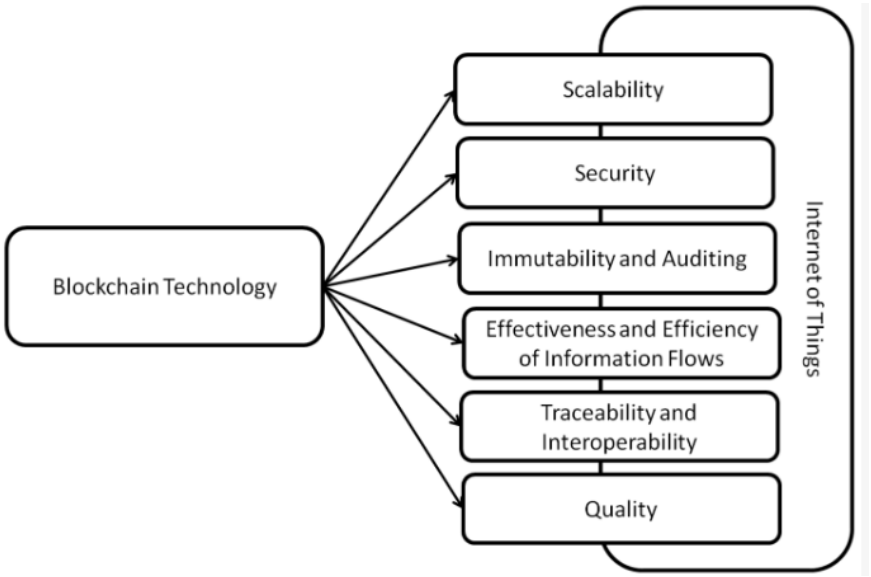

Fig 1. The way blockchain technology affects IoT features

In Figure 1 Blockchains make it possible to aggregate large volumes of data produced by IoT devices in a decentralized manner and guarantee that the advantages are distributed more fairly among supply chain exchange participants. In the sections that follow, we address the primary research topics at the nexus of IoT and Blockchain technology, such as scalability, security, immutability and auditing, information flow effectiveness and efficiency, traceability and interoperability, and quality. We conclude each section with a research question.

Fig. 2. Using blockchain technology to combat food fraud.

The process of recognizing the risk of food fraud, putting innovative blockchain solutions into practice, and the teamwork required to overcome these obstacles are all shown in Fig. 2. This acts as a guide for interested parties who want to comprehend and negotiate the challenges of applying blockchain technology to stop food theft.

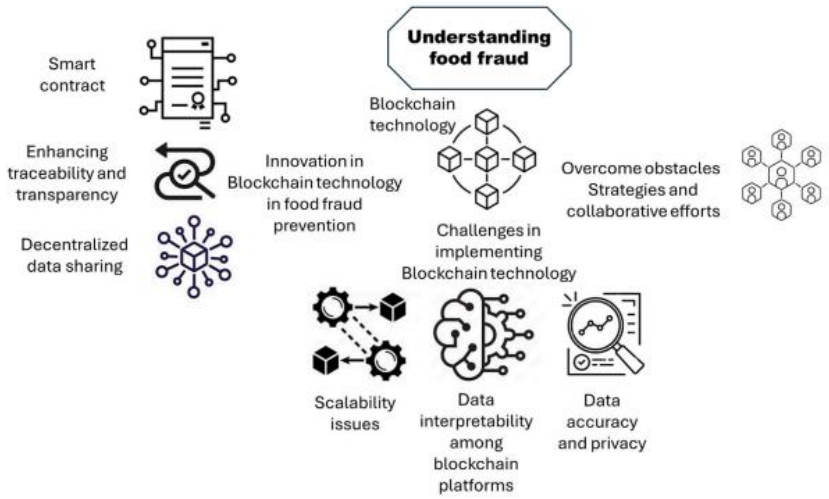

Fig. 3. An outline of the use of blockchain technology to stop food fraud is shown in this flowchart.

A flow chart demonstrating the use of blockchain technology to stop food fraud is shown in Fig. 3 below. It provides an overview of the developments, difficulties, and barriers in applying blockchain technology to stop food fraud.

Table 1 Blockchain technology advancements for preventing food fraud

Blockchain innovations in food fraud prevention.

Innovation	Description	Examples	Impact
Transparency and traceability	Utilizes immutable ledgers to securely track food products from their origin to the consumer.	JD.com's partnership with Kerchin for beef traceability; Bumble Bee Foods' seafood traceability system.	Enhances the ability of stakeholders to verify the history, quality, and safety of food products, thereby enhancing consumer trust.
Smart contracts and decentralized data sharing	Automates the execution of contracts based on predefined conditions, removing the need for intermediaries.	Blockchain-centered platform for the Indian dairy industry [47]; "FarMarketplace" [28].	Reduce costs, improves safety and traceability, and aids in resolving conflicts among stakeholders.

Table 2 Key Industrial 4.0 technologies are compared.

Comparison of key industrial 4.0 technologies.

Technologies	Key features	Strengths in the management of FSC	Limitations
Blockchain (BLC)	- Decentralization; - Shared database structure; - Immutability of records	- Ensure privacy, establishing trust and security;- Promote transparency; Achieve remarkable efficiency and speed- Reduce cost	- Scalability issues; - Interoperability issues; - Data accuracy issues
Internet of Things (IoT)	- Monitoring sensors for precision; - Facilitate connection and coordination	- Digital identification marks for food products; - Increased traceability	- Significant unresolved technical issues; Lacks creativity;- Privacy concerns
Artificial intelligence (AI) and Machine learning (ML)	- Stimulates human intelligence;- Automatic decision making	- Automatic quality control; - Improves predictability and automation; - Improves predictability and automation	- Data security concerns; Great complexity; Compatibility issues; Extensive energy use
Virtual Reality (VR)	- Creates a computer-generated simulation of three-dimensional environments or images	- Allows users to interact with the virtual world in a realistic and tangible way	- Requires specialized equipment
3D printing	- Revolutionizes the creation of devices aimed at monitoring food quality,	- Allows for the production of intelligent components that integrate smoothly into standard food packaging	- Speed and scalability; - Material limitations; - Resolution and surface finish

By providing legitimacy of origin and accountable authority, blockchain technology has the potential to enhance the global food supply chain's safety and quality. Before it can reach its full potential, though, important problems including scalability, compatibility, accuracy, and security must be resolved. In order to improve a safe food supply chain and the health of consumers, this necessitates the development of solutions through inventions and cross-stakeholder interactions to embrace cutting-edge technologies like the Internet of Things and artificial intelligence and execute the necessary changes in the food supply chain. The main conclusions of this study highlight the advantages of blockchain technology in terms of accountability and traceability, which may be used as a lever to raise the standard and safety of the food supply chain. Nonetheless, the accuracy of the data entered into the system determines how well blockchain works. Finding ways to increase data credibility and system efficiency requires coming up with more innovative solutions because inaccurate or insufficient data can also jeopardize the system's overall credibility.

CONCLUSION

A revolutionary solution to persistent issues with data integrity, transparency, and cybersecurity is provided by the use of blockchain technology into supply chain processes. Businesses can be sure that every transaction and piece of data in the supply chain is safely documented, verifiable, and impenetrable by utilizing the decentralized and unchangeable nature of blockchain technology. Using a hybrid blockchain architecture, smart contract automation, real-time data monitoring through IoT, and advanced cryptographic security is what is suggested as a strong way to protect the privacy and integrity of supply chain data. Blockchain lowers the risk of fraud, mistakes, and unauthorized access by facilitating transparent tracking of commodities, automating contract enforcement, and improving data privacy and security. This increases stakeholder trust.

Supply chains stay scalable, effective, and flexible in response to the always changing nature of international trade when blockchain is used for real-time auditing and cross-chain interoperability. Blockchain can assist businesses in meeting legal and operational needs by providing scalability solutions and a regulatory compliance emphasis, providing a solution that is future-proof for contemporary supply chains. In the end, implementing blockchain in supply chain operations improves operational efficiency, lowers costs, and fortifies the overall resilience of supply chain systems in addition to improving data security and integrity. Blockchain's ability to transform supply chain management will only increase as more companies realize how valuable it is for protecting their operations. This will spur innovation and provide businesses in an increasingly linked world with sustainable solutions.

REFERENCES:

Cakici, M., Alkan, F., & Yılmaz, H. (2020). Blockchain technology and its applications in supply chain management: A review. Journal of Industrial Engineering and Management, 13(2), 303-320.

Kamilaris, A., Fonts, A., & Prenafeta-Boldú, F. X. (2019). The rise of blockchain technology in the supply chain. International Journal of Production Research, 57(7), 2111-2129.

Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind bitcoin and other crypto currencies is changing the world. Penguin Random House.

Xie, X., Zhang, L., & Wei, K. (2021). Blockchain-based supply chain traceability: A comprehensive review. Computers & Industrial Engineering, 156, 107272.

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology in supply chain management: A review of the literature and applications. International Journal of Production Research, 57(7), 2119-2134.

Zhang, Y., Sun, W., & Li, J. (2021). Blockchain-based smart contracts in supply chain management: A survey. Journal of Manufacturing Systems, 58, 296-308.

Mougouei, M., Pahlevan, M., & Khajeh, E. (2020). Blockchain-based solutions for enhancing transparency and security in supply chain management: A review. Computers, Materials & Continua, 66(1), 29-45.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Shacham, H. (2016). Bit coin and crypto currency technologies. Princeton University Press.

Pilkington, M. (2016). Blockchain technology: Principles and applications. In Research Handbook on Digital Transformations (pp. 225-253). Edward Elgar Publishing.

Gurtu, A., & Johny, J. (2019). Blockchain applications in supply chain management: A

survey. Journal of Enterprise Information Management, 32(5), 731-748.

Dinh, T. T. A., & Nguyen, D. T. (2020). A blockchain-based solution for ensuring security and privacy in supply chain systems. International Journal of Computer Science and Network Security, 20(5), 78-85.

Xu, X., Weber, I., & Staples, M. (2019). Architecture for blockchain applications. Springer.
Zhang, L., & Sun, Y. (2020). Blockchain-based logistics and supply chain management: A survey and future directions. Journal of Industrial Information Integration, 18, 100123.

Li, J., Chen, L., & Wang, J. (2021). Blockchain and the supply chain: A comprehensive review of applications and future research directions. Computers & Industrial Engineering, 161, 107591.

Ribeiro, F., & Mota, A. (2020). Blockchain applications for secure supply chain management: A review and future research. IEEE Access, 8, 203267-203281.