STM JOURNALS

Recent Trends in
Sensor Research & Technology

ISSN: 2393-8765
Volume 11, Issue 2, 2024
May–August
DOI (Journal): 10.37591/RTSRT

https://journals.stmjournals.com/rtsrt

Research RTSRT

Avvanhi[1,*], Haneesh Hasan[2], Mohammad Musthafa[3], Mohammad Niyaz[4], Yashwin Y Puthran[5]

Abstract

In recent years, blockchain technology has emerged as a transformative force capable of enhancing transparency, security, and efficiency across various industries. Supply chain management is one area where blockchain integration has a lot to offer. This article explores the application of blockchain technology within supply chain systems, focusing on its potential to streamline operations, reduce fraud, and enhance traceability. By leveraging the decentralized and immutable nature of blockchain, stakeholders can achieve greater visibility into the lifecycle of products, from origin to consumer. This study reviews current blockchain implementations in supply chains, analyzes their impact on operational workflows, and discusses the challenges and opportunities associated with their adoption. According to the research, blockchain technology can significantly enhance supply chain operations, but its effective application necessitates navigating organizational, legal, and technological obstacles. The ultimate goal of this article is to present a thorough knowledge of how blockchain technology may transform supply chain management and open the door to supply chains that are more transparent and robust.

***Author for Correspondence**
Avvanhi
E-mail: avnichaki@gmail.com

[1–5]Students, Department of Computer Science and Engineering, P A College of Engineering, Mangalore, Karnataka, India

Received Date: July 06, 2024
Accepted Date: July 15, 2024
Published Date: July 25, 2024

Avvanhi, Haneesh Hasan, Mohammad Musthafa, Mohammad Niyaz, Yashwin Y Puthran. Smart Contracts in Supply Chain Management: A Blockchain Perspective. Recent Trends in Sensor Research & Technology. 2024; 11(2): 10–18p.

Keywords: Supply chain, block chain, stake holders, bitcoin, data storage ecosystem

INTRODUCTION

In the modern supply chain, suppliers, manufacturers, distributors, and retailers are only a few of the many parties involved in a complicated web of procedures. Ensuring the efficiency, transparency, and security of these processes is paramount for maintaining the integrity and reliability of the supply chain. On the other hand, traditional supply chain management systems frequently include problems like data silos, fraud susceptibility, inefficiencies, and a lack of transparency [1–4]. The aforementioned issues highlight the necessity for inventive approaches to improve supply chain functions.

With the rise in popularity of cryptocurrencies like Bitcoin, blockchain technology has become a viable way to deal with these issues. Fundamentally, blockchain is a decentralized ledger that immutably and transparently records transactions over a network of computers. This unique capability positions blockchain as a powerful tool to revolutionize supply chain management by providing end-to-end visibility, enhancing data integrity, and fostering trust among stakeholders [5].

The incorporation of blockchain technology into supply chain management systems is examined in this article. We begin by outlining the fundamental principles of blockchain and its relevance to supply chain operations. Next, to demonstrate the useful advantages and constraints of blockchain in actual supply chains, we look at case studies and contemporary implementations. We also go over the organizational, legal, and technological obstacles that need to be overcome in order to enable the broad implementation of blockchain-based supply chains. The objective of this study is to provide a comprehensive analysis of how blockchain technology can enhance supply chain management. By doing so, we aim to offer insights into the potential of blockchain to create more efficient, transparent, and secure supply chains, ultimately leading to improved business outcomes and customer satisfaction [6].

LITERATURE SURVEY

Tian F. et al., [7] in their article, have explored the use of blockchain technology to enhance traceability in agri-food supply chains. They implemented a blockchain-based system to track the entire lifecycle of agricultural products from farm to table. Their study demonstrated that blockchain could significantly improve transparency and traceability, thereby reducing food fraud and enhancing consumer trust products from farm to table. Their study demonstrated that blockchain could significantly improve transparency and traceability, thereby reducing food fraud and enhancing consumer trust.

In their study, Kouhizadeh M. et al. [8] examined how blockchain technology affects sustainable supply chain management. They conducted a systematic literature review to identify key areas where blockchain can contribute to sustainability. Their findings indicate that blockchain can enhance sustainability by improving supply chain transparency, reducing waste, and enabling better resource management.

In their research, Saberi S. et al. [9] looked into how blockchain technology might improve supply chain resilience. They suggested a methodology for controlling supply chain risks and disruptions based on blockchain technology. The framework was tested through simulations, showing that blockchain could enhance supply chain resilience by providing real-time visibility and facilitating quicker response to disruptions.

In their article, Casino F. et al. [10] examined a number of blockchain applications for supply chain management in a variety of industries.

They provided a comprehensive analysis of existing case studies and identified key benefits such as enhanced transparency, improved security, and reduced costs their analysis also emphasized the difficulties and potential avenues for further blockchain research in supply chain management.

Zhao G. et al., [11] in their research, examined the potential of blockchain to address counterfeit issues in pharmaceutical supply chains. They created a prototype blockchain-based system to trace the origin of pharmaceuticals. Their findings demonstrated that the method may successfully lower the possibility of fake medications getting into the supply chain, guaranteeing the safety and authenticity of the goods.

EXISTING SYSTEM

The existing supply chain management system is based on antiquated techniques like paper records and centralized computer systems. While these systems function to some extent, they are often slow and prone to errors. Information is typically siloed in separate locations, hindering a comprehensive view of product movement throughout the supply chain. This fragmentation makes it challenging to identify and address issues when they arise. Traditional supply chain systems suffer from inefficiency due to their reliance on manual processes for record-keeping and communication, leading to delays in order fulfillment and issue resolution. A significant lack of transparency exists as information is segregated within different enterprises, complicating collaboration and decision-making. These systems are also mistake-prone, with centralized databases susceptible to manipulation and human error, jeopardizing the accuracy and reliability of supply chain information. Limited traceability further complicates the tracking of items across the supply chain, making it difficult to identify the origins of problems such as defects or contamination. Additionally, centralized supply chain systems are vulnerable to disruption from cyberattacks, natural disasters, and geopolitical events. Existing system is shown in Figure 1.

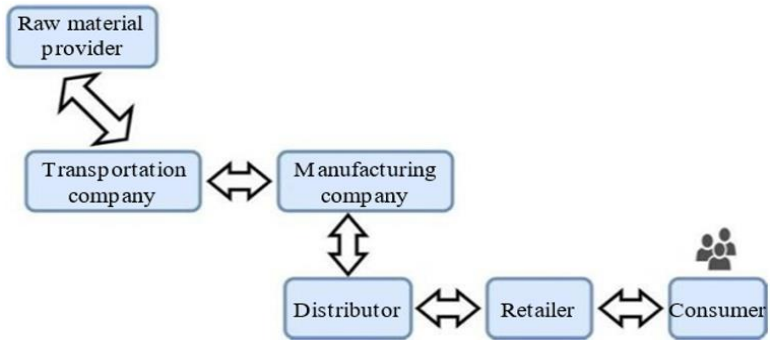

Figure 1. Existing system.

PROPOSED SYSTEM

The proposed system aims to integrate blockchain technology into supply chain management to address the limitations of the existing system. Blockchain functions similarly to a digital ledger, securely and transparently storing data across a network of computers. We can manage supply chains in a more effective, dependable, and traceable manner by utilizing blockchain.

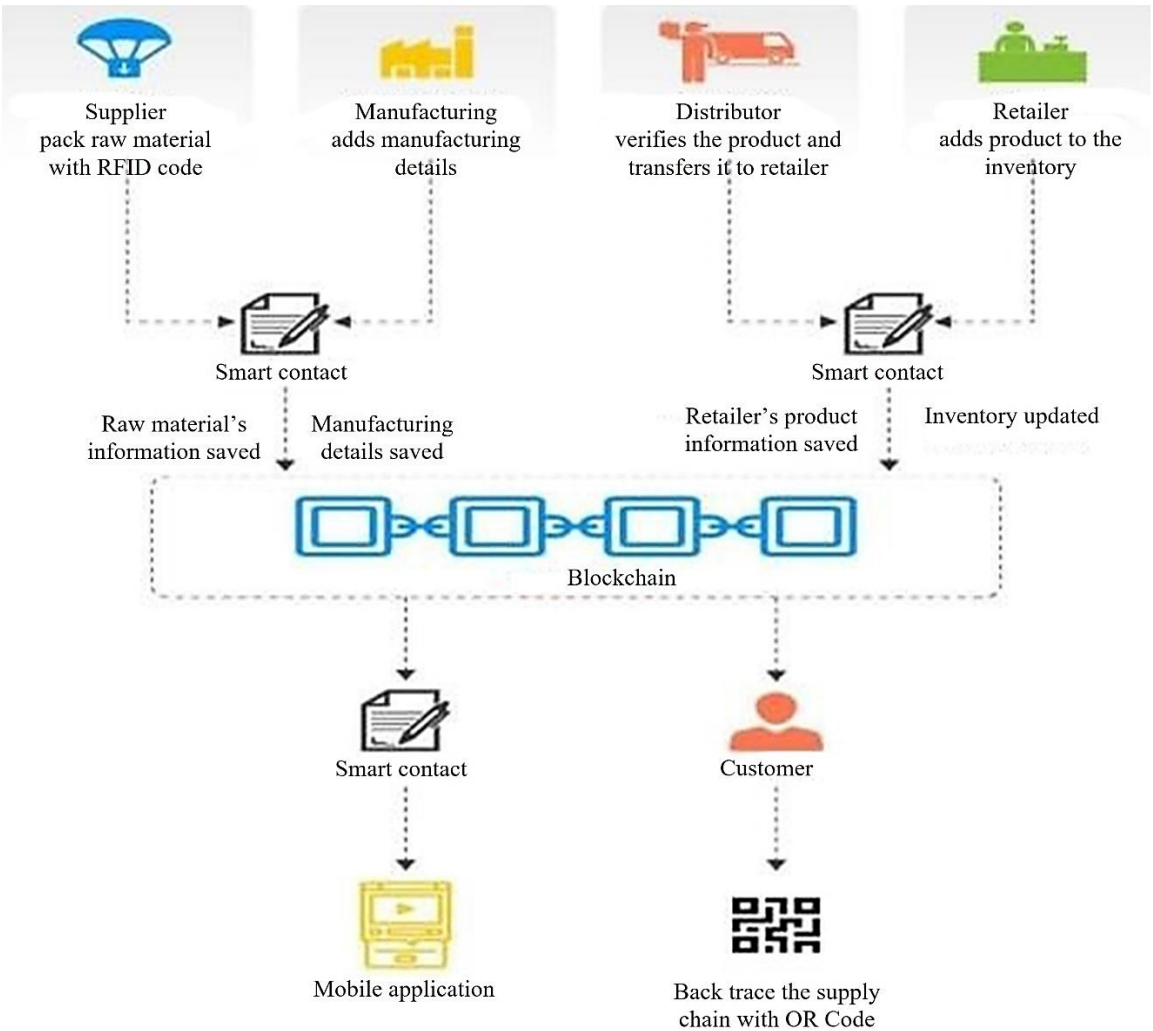

Figure 2. Proposed system.

In the proposed system, each step of the supply chain process, from production to delivery, is recorded on the blockchain in a secure and tamper-proof manner. This guarantees that, in real time, all parties

participating in the supply chain have access to the same precise information. The utilization of smart contracts, which are self-executing contracts with the conditions of the agreement directly encoded into code, is a crucial component of the suggested system. Automation of supply chain procedures including payments, shipments, and quality control inspections is possible with smart contracts.

Operations are streamlined, and less manual involvement is required.

DESIGN

System Architecture

The decentralized framework of the blockchain-based supply chain management solution's system architecture is designed to improve efficiency, security, and transparency across the whole supply chain network. Fundamentally, a blockchain network functions as a distributed ledger, storing and recording transactions in a way that is impervious to tampering. Individual nodes allow network participants—suppliers, manufacturers, distributors, retailers, and customers—to communicate with the system. Every node has a copy of the blockchain ledger and takes part in the consensus-building and validation steps to add new transactions. Using blockchain technology, smart contracts automate and enforce supply chain regulations that control things like product identification, inventory control, and payment settlements. Off-chain data sources, such as Internet of Things sensors and external databases, supplement on-chain transaction data, while user interfaces, such as mobile applications and web-based dashboards, offer straightforward access to the system. Digital signatures and cryptographic encryption are examples of security techniques that guarantee data integrity and authenticity [12]. Sensitive information is protected by privacy-enhancing technology. In order to foster cooperation and interoperability throughout the supply chain ecosystem, the architecture facilitates smooth connections with external applications and current supply chain systems. The system architecture as a whole aims to promote efficiency, trust, and teamwork among stakeholders, resulting in real advantages for the whole supply chain network. The proposed system is shown in Figure 2, and the system architecture of blockchain is shown in Figure 3.

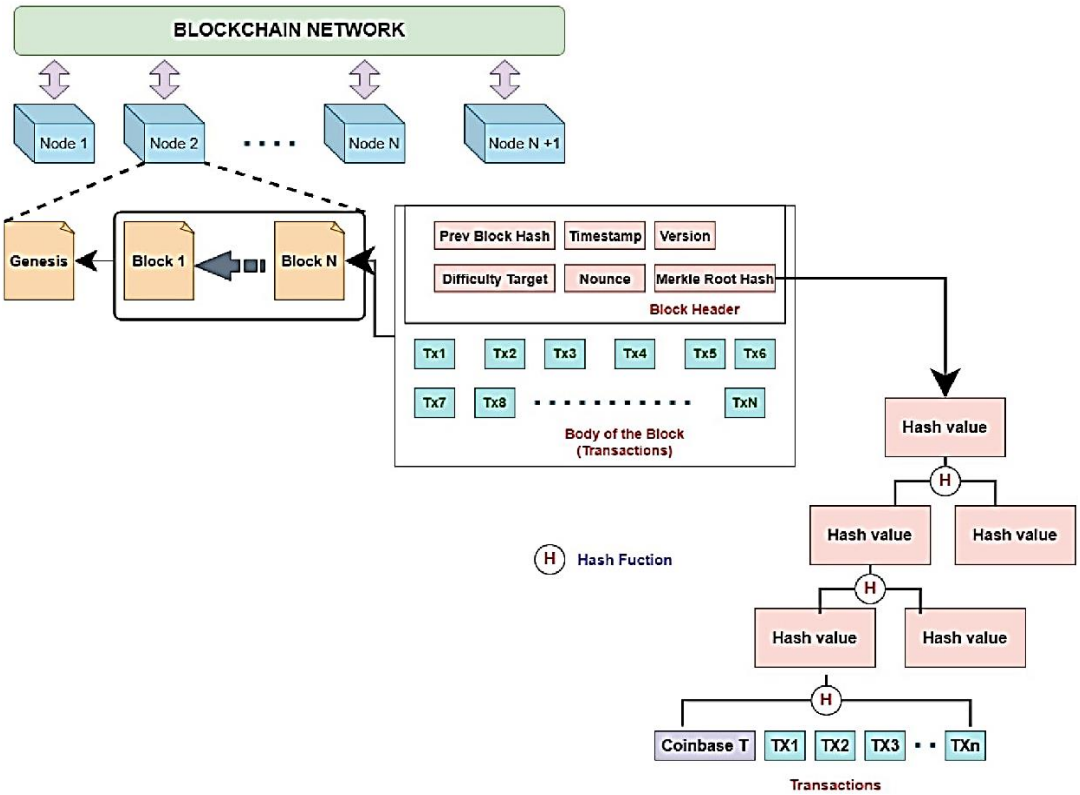

Figure 3. System architecture of blockchain.

Data Storage Ecosystem

Establishing a strong "Data Storage Ecosystem" for a supply chain management system based on blockchain requires careful consideration of a number of important factors. First off, the method used to store supply chain data is greatly influenced by the blockchain platform selected. Different blockchain platforms provide different methods of storing data, depending on things like scalability, privacy needs, and consensus procedures. As an illustration, Ethereum employs a distributed ledger architecture in which each node keeps a copy of the complete blockchain, providing redundancy and resilience but possibly posing scalability issues as data volume rises. However, permissioned blockchains, such as Hyperledger Fabric, provide increasingly fine-grained control over access permissions and data privacy through channels and private data collections, enabling customized storage solutions inside a consortium.

Second, for effective data management and retrieval, the blockchain system's storage architecture and data schema design are essential. To do this, the structure of data records or transactions kept on the blockchain must be defined. This includes details about participants, supply chain events, timestamps, and product identifiers. Appropriate data architectures and encoding methods can maximize storage effectiveness and speed up query processing, guaranteeing prompt access to vital supply chain data.

In addition, taking into account off-chain data storage and integrating with external databases or systems is crucial for handling massive data volumes and fulfilling intricate reporting and analytics needs. When on-chain storage isn't suited for storing extra data or historical records because of size or performance issues, off-chain storage options like distributed file systems, cloud storage services, or conventional databases can be used. To ensure data consistency and integrity throughout the ecosystem, safe and dependable data pipelines must be established for syncing data between off-chain storage repositories and the blockchain.

To further ensure confidentiality, integrity, and regulatory compliance, key elements of the data storage ecosystem include data encryption, access control methods, and data governance standards.

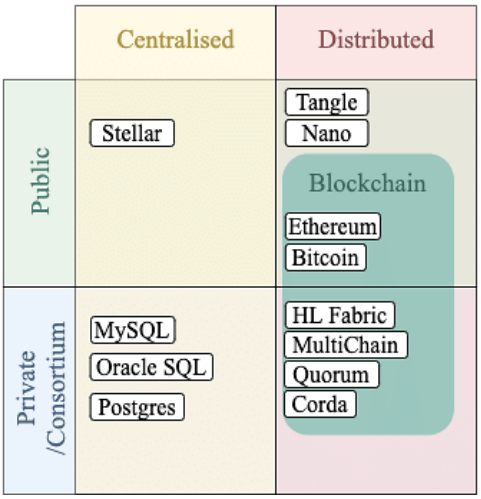

Figure 4. Data storage ecosystem.

Ethereum employs a distributed ledger architecture in which each node keeps a copy of the complete blockchain, providing redundancy and resilience but possibly posing scalability issues as data volume rises. However, permissioned blockchains, such as Hyperledger Fabric, provide increasingly fine-grained control over access permissions and data privacy through channels and private data collections, enabling customized storage solutions inside a consortium. Data storage ecosystem is shown in Figure 4.

Second, for effective data management and retrieval, the blockchain system's storage architecture and data schema design are essential. In order to do this, the structure of data records or transactions kept on the blockchain must be defined. This includes details about participants, supply chain events, timestamps, and product identifications.

Appropriate data architectures and encoding methods can maximize storage effectiveness and speed up query processing, guaranteeing prompt access to vital supply chain data.

In addition, taking into account off-chain data storage and integrating with external databases or systems is crucial for handling massive data volumes and fulfilling intricate reporting and analytics needs. When on-chain storage isn't suited for storing extra data or historical records because of size or performance issues, off-chain storage options like distributed file systems, cloud storage services, or conventional databases can be used. To ensure data consistency and integrity throughout the ecosystem, safe and dependable data pipelines must be established for syncing data between off-chain storage repositories and the blockchain.

To further ensure confidentiality, integrity, and regulatory compliance, key elements of the data storage ecosystem include data encryption, access control methods, and data governance standards.

BLOCKCHAIN TECHNICAL COMPONENTS

A number of core strategies in blockchain technology are essential to maintaining the ledger's integrity and security. These methods include consensus processes, digital signatures, asymmetric cryptography, hash functions, and Merkle trees. Collectively, they serve as the framework for blockchain architecture, enabling decentralized administration and building network trust. Every block in the blockchain consists of two main components: the block header and the block body. The real data, on the other hand, is kept in the block body and usually consists of transaction records or other confidential data.

Hash Function

A crucial method in blockchain technology is the hash function, which is employed for consensus, address generation, and digital signatures, among other things. Using a hash function, it is easy to convert data of any size to fixed-size values. On the other hand, deriving the original data from its hash value is challenging. For instance, the irreversible hash function Hash(x) can be used to get the associated hash value for a given big data set, x. The hash result Hash(x 0) differs entirely from Hash(x) if x is accidentally changed to x 0. Depending on the complexity of the data, message digest 5 (MD5) and SHA256 are the two most often used hash algorithms in blockchain. Data integrity can be checked during network transmission using a cryptographic hash approach. Let's say Alice sends Bob data x, for illustration. Encrypt(Hash(x)), the encrypted hash value, is surrounded with data x. Bob can confirm data integrity once he receives the information by computing the hash value from the received data, Hash(x 0), and contrasting it with the anticipated hash results decoded from the received Encrypt(Hash(x)). Data is correctly transferred if Hash(x 0) = Hash(x), where x 0 = x. Alternatively, if Hash(x 0) 6= Hash(x), then data integrity has been.

Asymmetric cryptography technology is used in conjunction with a hash function to enforce a digital signature mechanism in order to establish verifiable transactions in distributed systems. Every user in asymmetric cryptography possesses a pair of keys, which are the public key K and the private key K. While the public key may be known by others, the private key is kept secret and known only by the owner. Although the private key can be used to calculate the public key, the private key cannot be acquired in reverse using the public key that is provided. Data in pairs can be encrypted and decrypted using the public key K and the private key k. As demonstrated by Equation 1, for instance, data x encrypted with public key K can be decoded using the matching private key K. Conversely, data x that has been encrypted using private key K can likewise be unlocked using the matching public key K.

Decryptk (EncryptK (x)) = DecryptK (Encryptk (x))
= x (1)

Applied with flexibility, asymmetric cryptography can target varying security requirements. Assume once more that Alice is sending Bob data x and that they each have a pair of asymmetric keys. It should be noted that although Bob and Alice only know each other's private keys, they are aware of each other's public keys. Alice can use Bob's public key, EncryptKB (x), to encrypt data x in order to maintain confidentiality. As a result, only Bob can use his private key to decrypt the data. Alice, on the other hand, should transmit data x encrypted by her own private key, EncryptkA (x), to provide authentication and non-repudiation. In this instance, Bob can try to decode the data using Alice's public key after receiving it. If it works, Alice will be unable to retract the fact that she supplied this data.

Digital Signature

To prevent an issued transaction from being changed or rejected, a digital signature is needed for every blockchain transaction. In theory, a digital signature is a combined method that makes use of asymmetric cryptography and hash functions. A legitimate digital signature guarantees that unaltered data is provided by a known sender and cannot be revoked, just like a signature on paper papers. The file is first hashed to a certain length for this purpose, after which it is encrypted using the sender's private key. The outcome is this sender's digital signature. Because each designated sender is in possession of a unique private key, the asymmetric cryptography method guarantees are compromised, and Bob might ask Alice to give the information again.

Asymmetric Cross-over

Verification and unquestioning acceptance of this signature. In the meantime, anyone can confirm the integrity of the signature by computing the hash value from the data and comparing it with the hash value decoded from the signature, as long as they have access to the sender's public key. Additionally, the data can be encrypted using the designated recipient's public key if confidentiality is also needed.

Merkle Tree

As transaction volume increases, downloading all of the older transactions from the blockchain to perform verification uses a significant amount of storage space. The Merkle Tree approach is used to minimize the storage data without compromising the block hash in order to overcome this problem. A leaf hash node, an intermediate hash node, and a root hash node make up the binary tree known as the Merkle Tree. Individual transaction hash values are stored in leaf hash nodes within each block. Let's take an example where a block containing the transaction data TA, TB, TC, and TD exists. A Markle tree with four leaves—Hash(TA), Hash(TB), Hash(TC), and Hash—is about to appear (TD). Two intermediary hash nodes, HashAB and HashCD, are computed as the parents of these leaves. HashAB = Hash(TA) + Hash(TB)), and HashCD = Hash(TC) + Hash(TD)). Last, the value of intermediate nodes is hashed to determine the value of the root hash, which is contained in the block header.

Distributed Consensus Schemes

In distributed systems, the byzantine general problem has been brought up as a trust concern. In the context of blockchain, it refers to data tampering induced by some dishonest nodes. In order to address the issue and safeguard the data from minority attacks, a consensus mechanism is suggested, which assigns random candidates chosen from among all the nodes the task of updating data blocks. Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPOS), Practical Byzantine Fault Tolerance (PBFT), and Proof of Elapse Time (PoET) are some of the commonly used consensus procedures. The initial Bitcoin plan to reach consensus in peer-to-peer management is called proof of work (PoW) [7]. With little incentives, the nodes in the network compete with one another to solve a cryptographic problem so that the next block can be added to the blockchain. "Mining" is the term used for this in blockchain-based cryptocurrencies. Even though the plan is.

It takes a lot of time and work to defend the blockchain system against hostile attacks, which is astounding.

As a result, the systems that employ this approach have low on-chain speed (transactions per second). PoS is a way to update the blocks using validators rather than miners. By adding a specific number of coins to the system, the nodes must demonstrate their stakes. The substantial decrease in processing power is the main benefit of PoS over PoW. The primary problem, though, is that the nodes with the largest stakes are more likely to end up serving as the block validators. A better variation of proof of stake, known as delegate proof of stake (DPoS), limits the number of validators in order to increase the blockchain's scalability. All users who have a certain amount of votes determined by their network stakes cast votes for block producers. If two-thirds of the producers agree, a block is created. The Byzantine general problem was the original goal of the Practical Byzantine Fault Tolerance (PBFT) method. It emphasizes that in the event f nodes in the network are defective or dishonest, the PBFT needs 3f+1 nodes to decide correctly. The method has been implemented as a substitute consensus mechanism in a blockchain system.

According to the plan, a block proposer is first chosen in a round-robin fashion. After that, the proposer will broadcast and gather 3f+1 network nodes.

CONCLUSION

The advent of a blockchain-based supply chain management system marks a transformative era in the management and operation of supply chains across industries.

One of the key strengths of this system lies in its ability to enhance transparency and traceability throughout the supply chain. By recording every transaction and movement of goods on an immutable blockchain ledger, stakeholders gain unprecedented visibility into the entire lifecycle of products, from raw material sourcing to final delivery.

REFERENCES

Omar IA, Jayaraman R, Debe MS, Hasan HR, Salah K, Omar M. Supply chain inventory sharing using Ethereum blockchain and smart contracts. IEEE Access. 2022; 10: 2345–2356.

Du M, Chen Q, Chen J, Ma X. An optimized consortium blockchain for medical information sharing. IEEE Trans Eng Manag. 2021; 68 (6): 1677–1689.

Guggenberger T, Schweizer A, Urbach N. Improving interorganizational information sharing for vendor managed inventory: Toward a decentralized information hub using blockchain technology. IEEE Trans Eng Manag. 2020; 67 (4): 1074–1085.

Xiao H, Zhang W, Li W, Chronopoulos AT, Zhang Z. Joint clustering and blockchain for real-time information security transmission at the crossroads in C-V2X networks. IEEE Internet Things J. 2021; 8 (18): 13926–13938.

Lee D, Song M. Exchange: A privacy-preserving blockchain-based framework for health information exchange using ring signature and stealth address. IEEE Access. 2021; 9: 158122–158139.

Yang X, Li M, Yu H, Wang M, Xu D, Sun C. A trusted blockchain-based traceability system for fruit and vegetable agricultural products. IEEE Access. 2021; 9: 36282–36293.

