BLOCK CHAIN BASED SUPPLY CHAIN MANAGEMENT

Avvanhi[1], Haneesh Hassan[1], Mohammad Musthafa[1], Mohammad Niyaz[1],Yashwin Y. Puthran[1]

[1]*Department of Computer Science and Engineering, P A College of Engineering, Mangalore*

*Corresponding Author: Avvanhi E-mail: avvanhi.cse@pace.edu.in

Abstract:

In recent years, blockchain technology has emerged as a transformative force capable of enhancing transparency, security, and efficiency across various industries. One area that stands to benefit significantly from blockchain integration is supply chain management. This paper 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. The findings suggest that while blockchain technology offers substantial improvements in supply chain processes, successful implementation requires overcoming technical, regulatory, and organizational hurdles. Ultimately, this paper aims to provide a comprehensive understanding of how blockchain can revolutionize supply chain management, paving the way for more resilient and transparent supply chains.

Key Words: Blockchain Technology, Blockchain Adoption, Transparency, Security, Efficiency.

1. Introduction

The modern supply chain is a complex network of processes involving multiple stakeholders, including suppliers, manufacturers, distributors, and retailers. Ensuring the efficiency,

ISBN-978-81-19905-39-3

transparency, and security of these processes is paramount for maintaining the integrity and reliability of the supply chain. However, traditional supply chain management systems often suffer from issues such as lack of transparency, data silos, inefficiencies, and susceptibility to fraud. These challenges underscore the need for innovative solutions to enhance supply chain operations.

Blockchain technology, initially popularized by crypto currencies like Bitcoin, has emerged as a promising solution to address these challenges. At its core, blockchain is a decentralized ledger that records transactions across a network of computers in an immutable and transparent manner. 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.

This paper explores the integration of blockchain technology into supply chain management systems. We begin by outlining the fundamental principles of blockchain and its relevance to supply chain operations. We then examine current implementations and case studies to illustrate the practical benefits and limitations of blockchain in real-world supply chains. Additionally, we discuss the technical, regulatory, and organizational challenges that must be addressed to facilitate widespread adoption 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.

2. LITERATURE SURVEY

Tian, F. et al., [1] in their paper, 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

ISBN-978-81-19905-39-3

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.

Kouhizadeh, M. et al., [2] in their research, analyzed the impact of blockchain technology on 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.

Saberi, S. et al., [3] in their study, investigated the role of blockchain in enhancing supply chain resilience. They proposed a blockchain-based framework for managing supply chain risks and disruptions. 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.

Casino, F. et al., [4] in their paper, reviewed various blockchain applications in supply chain management across different industries. They provided a comprehensive analysis of existing case studies and identified key benefits such as enhanced transparency, improved security, and reduced costs. Their review also highlighted the challenges and future research directions for blockchain in supply chain management.

Jims et al., [5] in their research, examined the potential of blockchain to address counterfeit issues in pharmaceutical supply chains. They developed a blockchain-based prototype system to track the provenance of pharmaceutical products. Their results showed that the system could effectively reduce the risk of counterfeit drugs entering the supply chain, ensuring product authenticity and safety.

3. EXISTING SYSTEM

ISBN-978-81-19905-39-3

The current system for managing supply chains relies on traditional methods such as paper records and centralized computer databases. 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 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 disruptions from cyber-attacks, natural disasters, and geopolitical events.

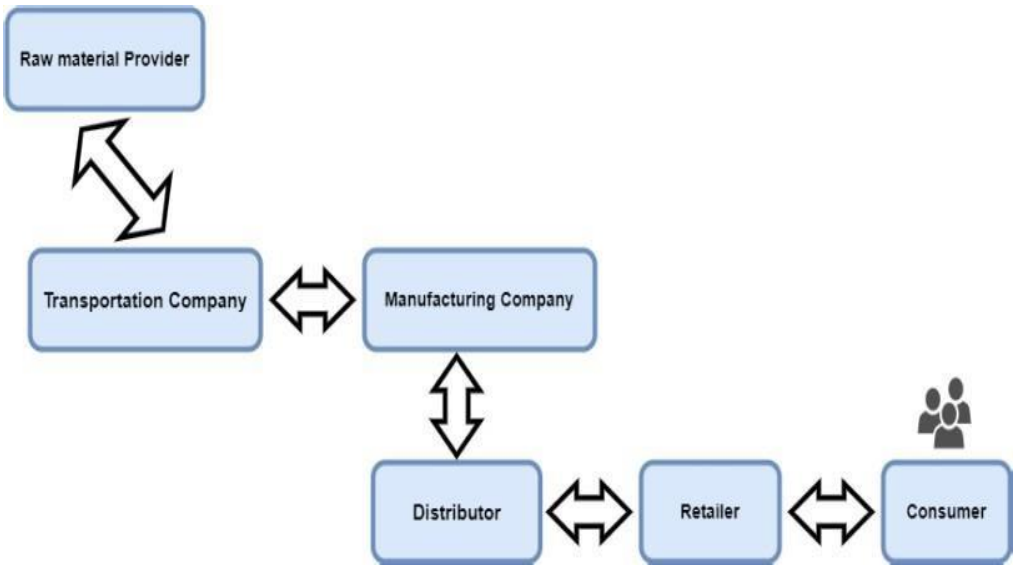

Figure 1: Existing System

ISBN-978-81-19905-39-3

4. PROPOSED SYSTEM

The proposed system aims to integrate blockchain technology into supply chain management to address the limitations of the existing system. Blockchain is like a digital ledger that stores information across a network of computers, making it secure and transparent. By using blockchain, we can create a more efficient, reliable, and traceable way of managing supply chains.

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 ensures that everyone involved in the supply chain has access to the same accurate information in real- time. One key feature of the proposed system is the use of smart contracts, which are self- executing contracts with the terms of the agreement directly written into code. Smart contracts can automate various processes in the supply chain, such as payments, shipments, and quality control checks, reducing the need for manual intervention and streamlining operations.

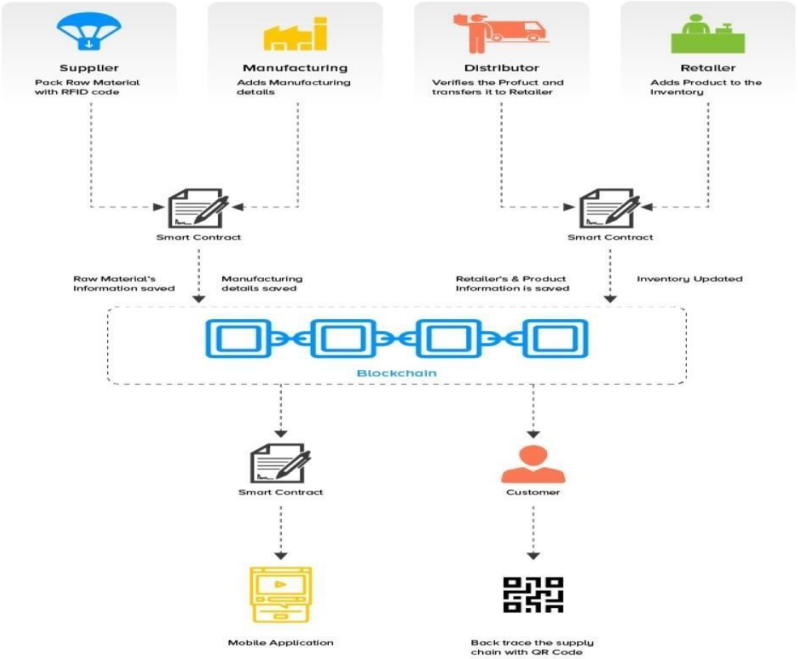

Figure 2: Proposed System

ISBN-978-81-19905-39-3

5. DESIGN

i. 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. Sensitive information is protected by privacy-enhancing technology.

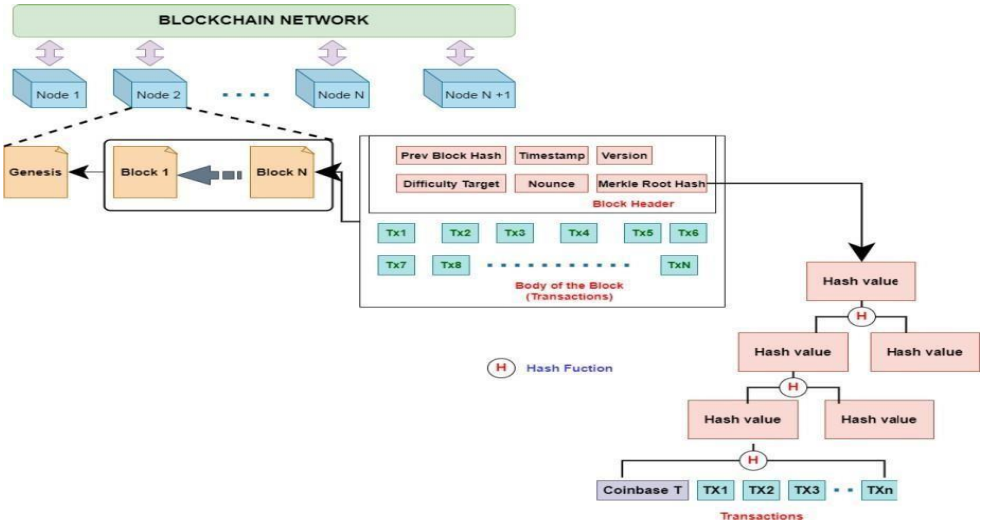

Figure 3: System Architecture of Blockchain

ISBN-978-81-19905-39-3

ii. 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 Hyper ledger 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. 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 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.

ISBN-978-81-19905-39-3

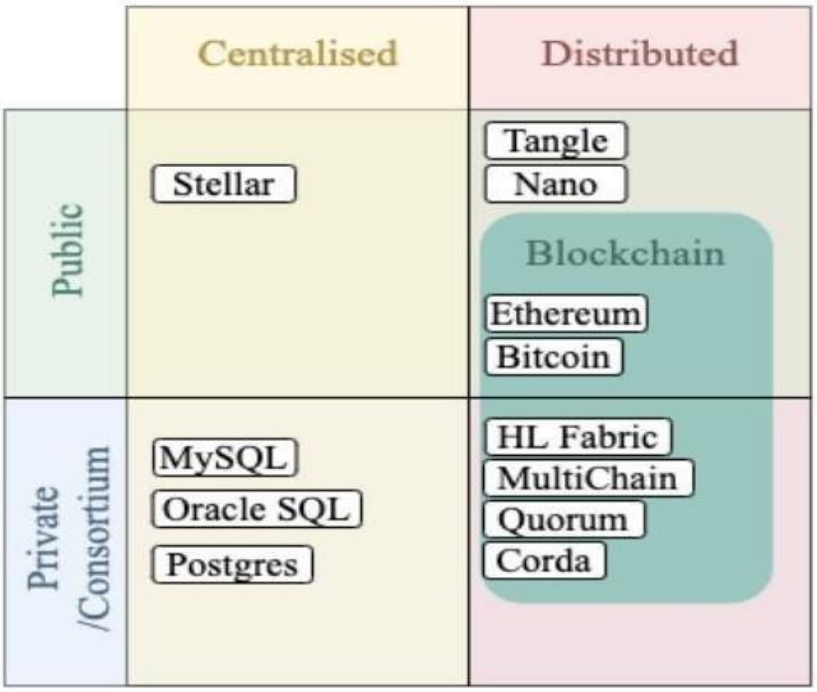

Figure. 4: Data Storage Ecosystem

6. 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. The block header and the block body are the two primary parts of every block in the blockchain. The real data, on the other hand, is kept in the block body and usually consists of transaction records or other confidential data.

I. 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. It is simple to convert arbitrary size

ISBN-978-81-19905-39-3

data to fixed-size values using a hash function. 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).To implement verifiable transaction in distributed system, asymmetric cryptography technique [30] is used along with hash function to enforce digital signature technique. In asymmetric cryptography, each user has a pair of keys, i.e. private key k and public key K. The private key is kept confidentially and known only by the owner, while the public key could be known by the others. The public key can be calculated from the private key, but with given public key, private key cannot be obtained in reverse. The public key K and the private key k can encrypt and decrypt data in pairs. For example, as shown in Eqn. 1, data x encrypted by public key K can be decrypted by corresponding private key k. On the other hand, data x encrypted by private key k can also be decrypted by corresponding public key K. Decryptk (EncryptK (x)) = DecryptK (Encryptk (x)) = x (1) Targeting different security requirements, asymmetric cryptography can be flexibily applied. Again, assume Alice is sending data x to Bob, and both of them have a pair of asymmetric key. Note, Alice and Bob know each other's public key whereas their private keys are only known by themselves, individually. To ensure confidentiality, Alice can encrypt data x through Bob's public key, EncryptKB (x). Hence, only Bob can decrypt the data by using his private key. On the other hand, to ensure authentication and non- repudiation, Alice should send data x encrypted by her own private key, EncryptkA (x). In this case, after receiving the transmitted data, Bob can attempt to decrypt it by Alice's public key. If successful, these data are indeed sent by Alice and she cannot deny it.

ISBN-978-81-19905-39-3

II. ASYMMETRIC CRYPTOGRAPHY

Authentication and non-repudiation of this signature. Meanwhile, because anyone can obtain the sender's public key, the integrity of signature can be verified by anyone through calculating the hash value from the data and comparing it with the hash value decrypted from the signature. Moreover, if confidentiality is also required, the data can also be encrypted by the public key of nominated receiver.

III. DIGITAL SIGNATURE

For each blockchain transaction, digital signature is required to avoid issued transaction being modified or denied. Technically, digital signature is an integrated technique utilizing both hash function and asymmetric cryptography. Like the signature for paper documents, a valid digital signature ensures that an unaltered data is sent by a known sender, which cannot be repudiated. For this purpose, the file is firstly hashed to a fixed length and then encrypted by sender's private key, and the result refers to the digital signature of this sender.

IV. MERKLE TREE

Once the number of transactions becomes larger, doing verification by downloading all the antiquated transactions in blockchain consumes a large amount of storage resource. To address this issue, Merkle Tree technique is used to reduce the storage data without breaking the block's hash. Merkle Tree is a binary tree consisting of leaf hash nodes, intermediate hash nodes and a root hash node. In each block, leaf hash nodes are the hash values of individual transactions. For example, assume there is a block with transaction data TA, TB, TC and TD. Here comes a Markle Tree with 4 leaves, i.e. Hash(TA), Hash(TB), Hash(TC) and Hash(TD). As the parents of these leaves, two intermediate hash nodes, HashAB and HashCD, are calculated as follows. HashAB = Hash(Hash(TA) + Hash(TB)) HashCD = Hash(Hash(TC) + Hash(TD)) .

V. DISTRIBUTED CONSESUS SCHEMES

Byzantine general problem has been raised as a trust issue in distributed systems. It refers to the data tamper caused by some dishonest nodes under the blockchain context. The consensus

ISBN-978-81-19905-39-3

mechanism is proposed to solve the problem and protect the data from minority attacks by allocating the responsibility of updating data blocks to random candidates selected from all the nodes. The popular consensus mechanisms include Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPOS), Practical Byzantine Fault Tolerance (PBFT), and Proof of Elapse Time (PoET). PoW is the first proposed scheme in the bitcoin to achieve consensus in peer to peer management [1]. The nodes across the network compete with each other to solve a cryptographic puzzle to add the next block into the blockchain with a small amount of incentives. This is called "mining" in blockchain based crypto currency. Although the scheme is remarkable to protect the blockchain system from malicious attacks, it is a time-consuming and energy consumption process.

Therefore, the on-chain speed (transactions per second) is low in the systems by using this scheme. PoS is a mechanism to use validators instead of miners to update the blocks. The nodes must prove their stakes by depositing certain amount of coins in the system. The key advantage of the PoS over PoW is the significant reduction of the computational power. However, the main issue is that the nodes who have large proportion of stakes are more likely to become the validators of the blocks. Delegate Proof of Stake (DPoS) is an improved version of PoS by restricting the number of validators to further improve the scalability of the blockchain. Block producers are voted by all the users who have a number of votes calculated based on their stakes on the network. A block is generated if two third of producers reach an agreement. Practical Byzantine Fault Tolerance (PBFT) algorithm was initially proposed to target on the Byzantine general problem. It highlights that the PBFT requires 3f+1 nodes to make a correct decision if f nodes are faulty/dishonest nodes in the network. The algorithm has been adopted into a blockchain system as one alternative consensus scheme.

7. 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. This innovative solution

ISBN-978-81-19905-39-3

addresses longstanding challenges in traditional supply chain management by introducing a decentralized, transparent, and secure framework powered by blockchain technology.

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. This transparency not only mitigates the risk of counterfeit products but also enables companies to ensure compliance with regulatory standards and ethical sourcing practices.

Moreover, the implementation of smart contracts within the blockchain ecosystem revolutionizes the execution of contractual agreements and business processes. Smart contracts automate and enforce the terms of agreements in a trustless manner, reducing the reliance on intermediaries and minimizing the potential for disputes or delays.

REFERENCES

[1]. Tian, Feng. "An agri-food supply chain traceability system for China based on RFID & blockchain technology." 2016 13th international conference on service systems and service management (ICSSSM). IEEE, 2016.

[2]. Kouhizadeh, Mahtab, Sara Saberi, and Joseph Sarkis. "Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers." International journal of production economics 231 (2021): 107831.

[3]. Saberi, Sara, et al. "Blockchain technology and its relationships to sustainable supply chain management." International journal of production research 57.7 (2019): 2117-2135.

[4]. Dasaklis, T. K., Voutsinas, T. G., Tsoulfas, G. T., & Casino, F. (2022). A systematic literature review of blockchain-enabled supply chain traceability implementations. Sustainability, 14(4), 2439.

[5]. Zoughalian, Kavyan, Jims Marchang, and Bogdan Ghita. "A blockchain secured pharmaceutical distribution system to fight counterfeiting." International Journal of Environmental Research and Public Health 19.7 (2022): 4091.

ISBN-978-81-19905-39-3