International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

IoT Supply Chain Management using Customized Blockchain Implementation

[1]Mr. Harshad D. Markad, [2]Dr. Sachin R. Sakhare

Submitted: 23/10/2023 **Revised**: 17/12/2023 **Accepted**: 24/12/2023

Abstract: The combination of blockchain technology with the Internet of Things (IoT) has opened up new possibilities for supply chain management, disrupting several sectors in the process. Conventional supply chain systems often face difficulties with privacy, security, and data integrity. On the other hand, the decentralized and tamper-proof characteristics of blockchain provide a safe, verifiable, and easily understood documentation of product movement across the supply chain. By using the unchangeable characteristics of blockchain, the system improves the capacity to track products, verify their validity, and ensure responsibility, all while greatly decreasing operating expenses. IoT devices are susceptible to attack owing to their limited computing power, storage capacity, and other factors. The integration of blockchain and IoT offers a solution to the challenges encountered by many businesses. Blockchains and smart contracts have garnered significant interest in the field of technology. Blockchain integration effectively overcomes these deficiencies by offering strong data security and integrity, hence reducing the likelihood of illegal access or modification. This study introduces a system that enables industrialists to access agricultural data and provide farmers with information on crop availability. The provided method represents a major advancement in the exchange of agricultural information, contributing to a more efficient and secure future as sectors increasingly adopt digitalization and networking. This solution will efficiently facilitate supply chain management for reliable delivery.

Keywords- *Hash generation; Smart Contract; Consensus; IoT; Supply Shain; Proof-of-Work; Proof-of-Stake.*

1. Introduction

The supply chain is a complex process due to the continuous alterations that impact the systems. These supply chains are essential since they transport data pertaining to the companies. The supply chain encompasses information on the company's next endeavours, necessitating safeguarding due to the presence of sensitive data. Integrating IoT (Internet of Things) into these supply chains is crucial since it substantially reduces the labor costs associated with data collection and processing. By ensuring that enterprises adhere to the manufacturing process to the point of sales, the supply chain may be enhanced for greater efficiency [1]. Furthermore, logistics plays a crucial role in maintaining the connection between the manufacturer, supplier, and customer. These supply chains use both business-to-business and business-to-consumer linkages. Given the advancements and competitive nature of the business environment, it is essential to ensure that products or commodities are effectively safeguarded along the whole supply chain, from their origin to their final destination [2]. The adoption of IoT devices presents itself as a feasible solution for automatically monitoring and tracking processes, eliminating the need for human interventions. This is in response to the issues that come from safeguarding the security and integrity of the supply chain model, which have been intensified by the fast expansion of globalization [3].

[1]*Research Scholar: SKN COE, Pune 411041, Maharashtra, India*
[2]*Prof: Computer Engineering Department Vishwakarma Institute of Information Technology, Pune 411048, MH, India*
Corresponding author. E-mail: harshad.markad@gmail.com

Although IoT devices are often used in supply chain management, the current business community has difficulties in using them due to their advanced approaches and algorithms. Many illicit IoT devices use unlawful means to get access to resources. Ensuring the security of IoT devices is a major concern, and one effective approach is to use the Blockchain network to enhance security in the supply chain management of IoT devices [4][8]. Compatibility of IoT devices with Due to their ability to authenticate and verify data in an environment where trust is not required, blockchain networks play a vital role in many applications, making them an essential component in supply chain management [10]. Blockchain is an emerging technology that gained widespread notice in recent years. By using innovative approaches and leveraging the three fundamental characteristics of distributed ledgers, namely transparency and immutability, it revolutionized the operational tactics of several firms and created enhanced opportunities. The use of blockchain has escalated due to the implementation of immutable transactions [11].

IoT devices generate vast amounts of data that exist inside IIoT networks. The use of IoT vulnerabilities might lead to a variety of security concerns when dealing with confidential and private information. Decentralized methods provide a possible remedy to enhance the security and reliability of existing IIoT systems. It mitigates the risk of system failure and allows for prolonged operation of IoT devices and networks [12]. High-end computing is essential for modern centralized systems that provide data processing, security, and privacy services. Third-party entities often provide these services. Users must possess unwavering trust in this solution for data management and preservation. Nevertheless, this data might potentially be misused and, in the most severe scenario, it could even be revealed to unauthorized individuals [15]. The blockchain enables direct and safe interchange and storage of data from IIoT system components, eliminating the need for intermediaries. The inherent security of blockchain technology will enhance the trustworthiness and safety of IIoT systems, perhaps leading to changes in the way IIoT manages data [4]. These blockchain systems may be evaluated based on factors such as energy consumption, CPU and memory use, block size, and so on.

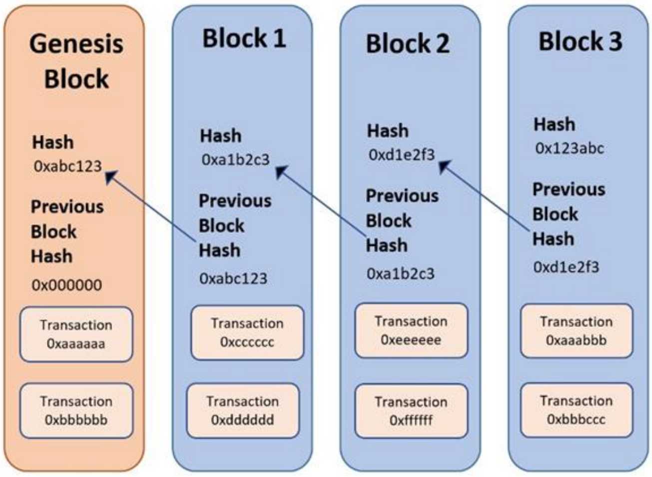

Fig 1: Blockchain architecture

Blockchains are often regarded as decentralized ledgers that possess both public and, more recently, private attributes. They are comprised of a series of linked blocks that hold transactional data. Asymmetric cryptography and consensus approaches are used to provide consistency, data integrity, non-repudiation, and authentication [6]. Once blockchain transactions have been authenticated by network peers and added to the chain, they become tamper-proof owing to their immutable nature. Reliability and resilience are essential characteristics that distinguish blockchains as extremely trustworthy systems operating on peer networks characterized by a lack of trust. The ledger will be replicated in an identical manner on every node inside the network. The ledgers in the database are synchronized with all other copies at preset intervals.

This ledger is very exact and secure as a result of using cryptographic methods such as the hash function and digital signature. Consensus, which refers to a collective accord, regulates this modification or advancement [7].The text is presented in the form of a numbered reference [11]. Consensus algorithms are used in blockchain systems to address the absence of a centralized controller. Several consensus techniques may be used based on the need for a distributed consensus. Furthermore, there are several types of blockchain networks.

Open, decentralized, and transparent digital ledgers: Public blockchains are inclusive, granting access to all individuals and enabling their participation as validators or users inside the network. Their extensive participant base ensures the utmost degree of decentralization and security. Notable examples include Bitcoin and Ethereum.

Bitcoin (BTC): Bitcoin, the initial and renowned blockchain, is mostly used for decentralized digital money transactions (cryptocurrencies) amongst individuals. The network utilizes a proof-of-work (PoW) consensus process to verify, validate transactions, and ensure the security of the network.

Ethereum (ETH): Ethereum enables the use of smart contracts, which are self-executing programs that operate in a legally binding manner.The system now employs a comparable Proof of Work (PoW) method, but it is in the process of shifting to a Proof of Stake (PoS) mechanism in collaboration with Ethereum. This move aims to enhance scalability and energy efficiency.

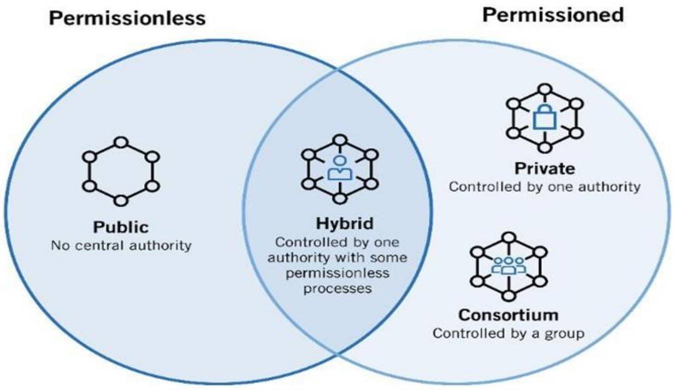

Fig 2 : types of blockchain

Private blockchains are exclusive to a certain set of participants, such as a single corporation or consortia. They provide enhanced network management capabilities and are often used for internal operations.

Hyperledger Fabric: Hyperledger Fabric is specifically tailored for corporate applications and was created by the Linux Foundation. It enables the customisation of consensus procedures and data privacy restrictions. Participants possess different degrees of authorization to access and verify transactions.

Corda: Corda is specifically tailored for financial organizations to systematically document and oversee agreements between several parties. The major emphasis is on privacy, enabling participants to engage in direct transactions while ensuring the confidentiality of data.

Consortium Blockchains: A compromise between public and private blockchains is provided by consortium blockchains. They include many organizations cooperating to keep the network up to date, often for a particular sector or use case..

R3 Corda: Although Corda may be used for private blockchains, it also enables consortium models, in which many parties work together to keep the network up to date..

Quorum: Quorum, a corporate application platform built on Ethereum, facilitates permissioned participation, private transactions, and data privacy.

Hybrid Blockchains: Hybrid blockchains include elements from public as well as private blockchains to target unique requirements.

A smart contract is a piece of computer code that acts as an understanding or mutual agreement between many stakeholder groups without the need for a third party or other controller [22]. It's a legally binding contract between the parties and a program that executes upon the fulfillment of a certain requirement. The blockchain technology's commercial components depend on smart contracts. Typically, you would have to get in touch with, employ, and then wait for the paperwork to be delivered by a lawyer. But you may be able to avoid hiring a lawyer if you use smart contracts to complete the procedure, pay for it, and then get the documentation. the required document [39]. Smart contracts go above and beyond traditional contracts, which just outline the terms and conditions of an agreement, by automatically elaborating on requirements. Transparency and privacy are to be balanced, they hope.

Enforcing the above requirements will greatly lessen the likelihood of fraud and scams. Among the many advantages of smart contracts are their accuracy, speed, transparency, security, paperless trust, and so on. Smart Contracts are computer programs that express an agreement between two parties or organizations in a manner similar to a typical legal contract (on paper). Examples of these programming languages include Solidity, Python, and GoLang. One common use for blockchain technology is smart contracts. An example of purchasing real estate [9].

Assuming that A transfers the property to B, B will then pay the agreed upon sum. or if B makes the agreed-upon payment. Alternatively, Party A will transfer ownership on behalf of Party B upon B's payment of the agreed upon sum. The smart contract may include any term or condition. Additionally, the smart contract won't operate and verify the transaction until all of the prerequisites have been satisfied. Furthermore, since the smart contract is kept in a distributed system, real-time communication between the two parties is possible without the need for outside assistance. This will result in significant time and cost savings. Because they are kept on a decentralized ledger, these encrypted contracts are impervious to deletion [8]. Applications in the fields of supply chain management, real estate, healthcare, and insurance are all possible.

2. Literature Survey

A blockchain system was suggested by Pinchen Cui et al. [1] to help monitor and trace every chip as it travels through the supply chain. The proposed structure is based on a permissioned blockchain. Hyperledger is utilized to construct the framework, and a comprehensive analysis is conducted to show that the recommended approach is viable.

A method that integrates the unique applications of blockchain and IoT technologies into a comprehensive traceability was proposed by Yung Po Stang et al. [2]. An IoT-based blockchain-based food traceability system called Bifts has been developed to control the expiration date of perishable food items. Lightweight and vaporized features are added to the blockchain in order to satisfy food traceability requirements, and an integrated consensus mechanism that accounts for shipment transit time, stakeholder evaluation, and shipment volume is built.

Supply chain management (SCM), a crucial business function responsible for moving products and services between many stakeholders and locations, was covered by U Agrawal et al. [3]. conducts a detailed analysis of the literature on the features, business consequences, and BC implementations in different SCM cycles.

With an emphasis on transportation, M. Nasir et al. [4] presented a model that updates the quality of perishables in tandem with supply chain management. It was recommended to develop a safe Internet of Things-based monitoring and reporting system.

A hybrid and delegated proof-of-stake consensus approach is proposed by B. Wang et al. [5]. The nodes use the Delegated Proof-of-Stake consensus method and the modified Proof-of-Probability consensus algorithm, respectively, to carry out the tasks of block production and validation. The system broadcasts a number of target hash values to the whole network each time a transaction takes place. Because each customized Proof-of-Probability node utilizes a separate sorting algorithm, each node has a unique mining priority.

Decentralized arbitration is made possible by the innovative Proof of Vote (PoV) consensus approach, which was presented by Kelao Li et al. [6]. It enables scattered nodes controlled by consortium members to reach an agreement by voting. PoV divides the accounting and voting powers based on the core idea of establishing unique security identities for network nodes.

A comprehensive study of blockchain-based technology is provided by S. Tanwar et al. [7], particularly for Industry 4.0-based applications. The benefits and drawbacks of several cutting-edge techniques are examined. Interoperability and governance are emphasized in order to provide professionals and academics with a comprehensive understanding of the blockchain's problems.

An extensive examination of contemporary blockchain-based technologies, particularly those used for different Industry 4.0 applications, was covered by S. Tanwar et al. [8]. The benefits and drawbacks of several cutting-edge techniques are examined. Interoperability and governance are emphasized in order to provide professionals and academics with a comprehensive understanding of the blockchain's problems.

Oscar Nova et al. [9] discussed the benefits and challenges of decentralizing blockchain technology. Furthermore discussed were the concepts of different distributed consensus, how consensus algorithms work with a permissionless protocol, and a thorough case study on decentralized supply chain management with a blockchain. a structure for choosing IoT permissions and responsibilities.

According to Jaime Chan et al. [10], The new architecture is a fully distributed IoT access control system built on blockchain technology. The idea is backed by a proof-of-concept implementation and has been tested in real-world IoT environments.

The Access Control Lists (ACL), Role-based Access Control (RBAC), and Attribute-based Access Control (ABAC) methods that Yu Chen et al. [11] presented—all of which relied on a Traditional AC approach—cannot provide an efficient, scalable, and controllable solution to satisfy the demands of IoT systems. Employing both more potent computing devices (like laptops) and resource-constrained devices (like Raspberry PI nodes), a proof-of-concept prototype has been created and tested on a local private blockchain network. The results of the experiment demonstrate that the Blend CAC can provide a fine-grained, scalable, decentralized, and lightweight AC solution to an Internet of Things system.

In order to provide a scalable, decentralized management solution and safe access to IoT data, Hamda et al. [12] suggested a decentralized IoT data access control system that combines blockchain and trusted oracles with blockchain and smart contract capabilities. Additionally, Oracle provides uniform, trustworthy, and decentralized source flows for IoT data by acting as a gateway between the blockchain, IoT data servers, and distant users. The architectural design, interfaces, logic flows, algorithms, implementation specifics, cost, computation, and security evaluations are all included in this paper.

As previously noted, S. Tanwar et al. [13] explored how using blockchain in the supply chain might increase transparency and traceability while reducing administrative costs. Because blockchain supply chains store sensitive data like price, date, location, quality, certification, and more, they may help participants manage supply chains. The data's accessibility via the blockchain may improve the supply chain's traceability for raw materials, reduce market loss and counterfeiting, boost compliance and visibility, and enable contract manufacturing.

Rejeb et al. [14] spoke about how supply chains may be modernized and value chain networks enhanced by combining Blockchain technology with IoT infrastructure. The use of Blockchain technology may provide the foundation for future research endeavors by impacting critical IoT aspects including scalability, security, immutability and auditability, information flow, traceability, and interoperability, among others.

A traceability-based methodology was presented by Mabrook S. et al. [15] to address the issues raised by supply chain mechanism security considerations. The distributed ledger system maintains the scalability, costs, and quantum robustness. The system achieved high tractability, security, and traceability; nevertheless, power and computing capacity need to be further optimized.

Majid et al.'s discussion [16] Prochain, a provenance-aware traceability framework for Internet of Things-based supply chain systems, which provided a full framework of all the data gathered by the sensors and the whole collection of provenance data, was brought forward in connection to these concerns. An extensive simulation of the proposed framework on the IoT device Raspberry PI 3B also looked at Prochain's performance in local and cloud simulation scenarios. Prochain demonstrated traceability, transparency, and complex security.

Peer-to-peer backup methods, access control systems, and internal data separation and transmission strategies were recommended by Qun Song et al. [17]. The access control system consists of both an inspection and a registration module. According to a registration policy, all firms in the supply chain must register information, and the registration module is primarily in responsibility of achieving this. To preserve the system's resilience, this approach is fully considered for fault tolerance and network stability.

In addition to providing a digital ledger for accessing information about the goods, Muhammad Nasir et al. [18] maintained supply chain management systems by continuously monitoring and reporting information to the networks that greatly guaranteed the privacy and security of the system. This strategy, while improving the supply chain, is primarily centered on agriculture and may be used universally.

A cross-disciplinary study on distributed ledger technology and supply chain management in business was given by Yaou Qian et al. [19]. Following testing and debate, three major benefits that blockchain implementation may provide to contemporary supply chain management were highlighted. Additionally, we've found a few problems that the blockchain program as it stands is unable to resolve.

Proof of work(PoW) : Bitcoin and many other groundbreaking blockchain platforms were the first to use the consensus technique known as PoW. Nodes, also known as miners, compete in Proof of Work (PoW) by trying to solve a difficult mathematical puzzle. The first miner to solve the problem correctly wins the opportunity to add the next block of transactions to the blockchain and get money for transaction fees. To keep the pace of block formation constant, the puzzle's complexity is gradually changed. It takes a lot of energy for miners to use their computing power to obtain a hash value that satisfies certain requirements. The chain that is the longest and requires the most total computing effort is deemed legitimate, with the other chains being eliminated. Because it takes a lot of computing power to build blocks, it has the benefit of high security. Because the network is maintained by a number of people, it is decentralized. High energy usage is one of its drawbacks. Possible centralization as resource-rich miners eventually acquire an edge.

Proof of stake(PoS) : An alternative consensus method called PoS seeks to solve the problems of PoW's centralization and energy consumption. The amount of bitcoin that participants (validators) "stake," or lock up as collateral, determines which blocks they get to generate in a proof of stake. Essentially, a participant's chances of getting chosen to validate transactions and add new blocks increase with the amount of bitcoin they own and are prepared to lock up. Validators are motivated to take action. Mechanisms to randomly choose validators and avoid power concentration are common components of PoS systems.

Delegated Proof of Stake(DPoS) : a PoS variant in which token owners cast ballots for a select group of delegates to approve transactions. Blocks are created by delegates in shifts. Compared to PoS, faster block confirmation and lower centralization risk.

Proof of Authority (PoA) : Rather than computing power, validators are chosen based on their reputation and identification. Appropriate for blockchains in consortiums or private settings where users are recognized entities. less centralized yet lowers the possibility of malevolent behavior.

Proof of Space (PoSpace) ::Miners demonstrate that they have set aside a certain quantity of disk space. used to build blocks when used with Proof of Time. Resource-intensive yet less energy-intensive at times.

Proof of Burn (PoB) : In order to mine new cryptocurrency, users destroy (burn) old coin. Participants get the opportunity to mine more blocks in proportion to the quantity burnt. Used in some experimental systems, with the intention of demonstrating dedication to the network.

Hybrid Concensus Algorithm: To counteract each consensus mechanism's drawbacks, combine them. For instance, combining PoW with PoS to provide energy efficiency and security.

3. Supply Chain Management

One of the newest blockchain-related technologies is supply chain management. Blockchain is a digital record system designed for cryptocurrency networks that, by generating a history of data and financial movements in a transparent transaction, may assist supply chain users in overcoming some of their obstacles. openness and prevention of counterfeiting [13][21]. Businesses may transact directly thanks to blockchain, which increases the effectiveness of the global supply chain. By providing logistical and financial service integration, it enables data cooperation amongst several stakeholders. Using blockchain supply chains, stakeholders may document price, date, location, quality, certification, and other relevant information to enhance supply chain management. Data integration into the blockchain may prevent loss from counterfeiting, increase contract manufacturing visibility and compliance, and improve material supply chain traceability. The growing use of blockchain technology in supply chain management is not unexpected. As of April 2018, a number of international organizations have used Blockchain technology, as seen in Figure 3 of Statista. In fact, over 53% of respondents agree that their company conducts use case research to give chain [37].

Accurate and transparent product tracking in the supply chain is made possible by blockchain technology. Businesses may digitize their actual goods and build an unchangeable, decentralized record of each transaction, tracking goods from manufacturing to delivery throughout the whole supply chain. finally, to the client [22]. Supply chain management is a crucial tactic for handling food insecurity and public health concerns. Relationships of dynamic collaboration are established between suppliers, manufacturers, retailers, and end users via supply chain management. Information, money, logistics, and commerce are also involved. Supply chain models are getting more complicated and automated in today's environment, and they have several advantages. Because of this, SCM agro-food products place a high priority on technological advancements that enable notable losses to be reduced as well as improved health and safety management. Due to the need for food safety, SCM has put in place quality control and traceability systems that are especially strict for the food sector [19]. Furthermore, globalization and reallocation increase the allure of the culinary scene by including several suppliers and businesses.

There are a number of possible advantages and applications for integrating blockchain technology with the Internet of Things (IoT), but it's important to remember that the choice to combine these two technologies should be made in light of the specific requirements and objectives of a given project or application. The following are some justifications for why blockchain integration with IoT can be beneficial:

Security and Integrity of Data: Data security and integrity are improved when blockchain is used in combination with IoT, which is one of the key benefits. Massive amounts of data are generated and sent by IoT devices, and this data may be subject to manipulation or illegal access. Because blockchain is decentralized and unchangeable, it is a good choice for protecting the integrity of Internet of Things data. It is almost hard to change or modify data once it is stored on the blockchain without the network's members' agreement.

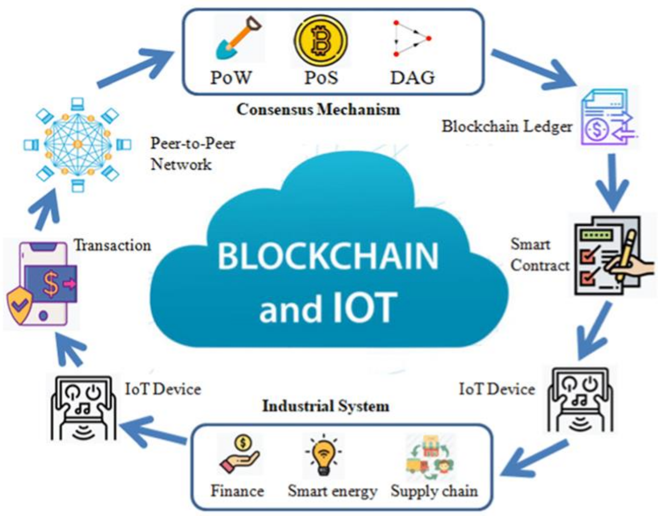

Fig 3. Integrating IoT with Blockchain

Transparency and Trust: In IoT environments, blockchain's transparent and impervious to tampering nature adds a trust layer. There is less need to depend on centralized intermediaries for data validation when all parties involved can verify the validity and provenance of the data. As a result, there may be an increase in trust between manufacturers, suppliers, consumers, and regulators involved in IoT networks.

Smart Contracts: Smart contracts are self-executing sets of rules and conditions that are often supported by blockchain systems. Automated actions based on preset triggers may be made possible by integrating smart contracts with Internet of Things devices. For example, when certain circumstances are satisfied—like a shipment of products being received and confirmed by IoT sensors—a smart contract may automatically carry out a payment.

Supply Chain Management: Blockchain technology and IoT may be used together to improve supply chain traceability and transparency. Through the use of IoT sensors and blockchain technology, businesses are able to monitor items and verify their authenticity. This is especially beneficial for sectors like luxury products, medicines, and agriculture.

Data Monetization: IoT device owners may share or sell their data to interested parties in a transparent and safe manner with the help of blockchain technology. By enabling direct data flow between data suppliers and customers, smart contracts may eliminate the need for middlemen.

Decentralization: Decentralization is a concept that is supported by both blockchain and IoT. By combining the two, a network's control and decision-making may be distributed even more, decreasing the number of single points of failure and increasing system resilience.

Regulatory Compliance: Regulations are stringent in certain areas, such as healthcare and banking. Organizations may prove compliance with data management and privacy rules by using blockchain's unchangeable audit trail feature.

Energy and Resource Management: Environmental conditions, resource utilization, and energy consumption may all be tracked and managed using IoT devices. These systems can be made more effective, transparent, and responsible by incorporating blockchain, which will allow for improved resource management.

4. Proposed System Architecture

The primary objective of this research is to furnish crucial agricultural knowledge to individuals in the farming industry, specifically pertaining to agricultural techniques and other relevant information. This will be accomplished efficiently through the utilization of Blockchain-enabled IoT systems within the agricultural sector. Initially, the industrialist would send a request to the agricultural industry sector in order to get information about the crops. The agricultural industry may be either a government entity or an organization that encompasses comprehensive information pertaining to the agricultural sector.

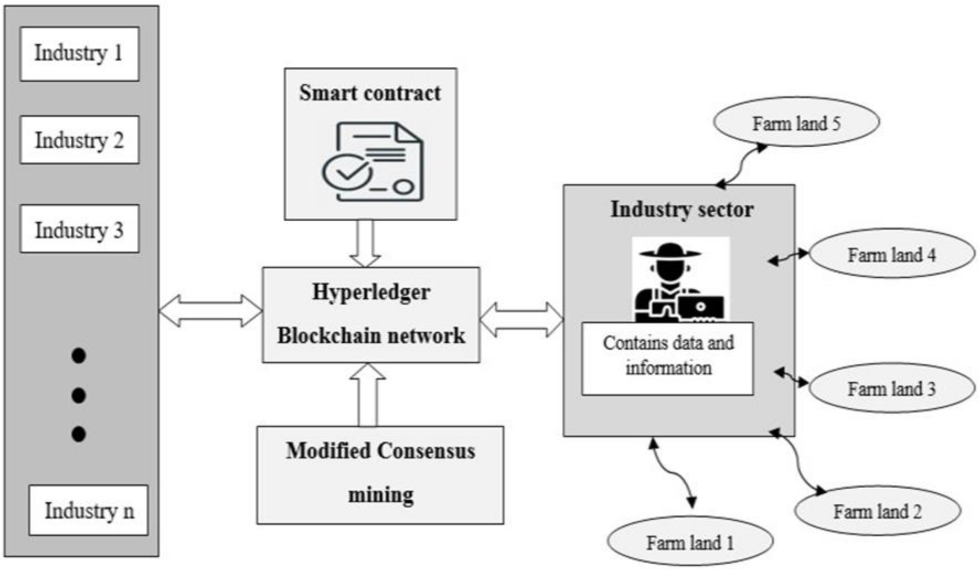

Fig: proposed system architecture of supply chain with IoT blockchain

The request will be sent over the Blockchain network to improve the confidentiality and integrity of the data, while also using smart contract functionality. The Blockchain integrates a consensus mechanism to maintain authentic records of transmitted data. The consensus mechanism serves as an agreement between farmers and agriculture sector authorities over the distribution of resources. The consensus method enhances the velocity and security of transactions, while the smart contract monitors the data transit between the owner and the user to prevent any legal duties in the future. Authorized users may easily get data from the source over the Blockchain network whenever it is required, without encountering any complications. The research's relevance will be shown by using the Crop Recommendation Dataset [46] in the Python programming language. The research is visually shown in the figures below. Two distinct datasets are used in the Crop Recommendation system: one including crop production statistics categorized by year and state, and the other containing the annual cost of cultivating certain crops categorized by state. A DAPP has been constructed to showcase the system's efficacy. It includes detailed information about crop requests, utilizing two separate databases, along with transaction and account details. Ganache is used as the platform for this development.

Algorithm Design :

TransEvaluator

Input: Smart Contract SMC[], Previous_Hash[], Current_Hash[], Current Transaction Minor TM [id]

Output: Authenticated valid previous hash for mining current transaction

Step 1: Read previous hash from current blockchain from any random server for TM [id] and SMC

$$Prev\_Hash[] = \sum_{n=1}^{m}(Commited\_hash[Trans[m]])$$

Step 2: To validate the $Prev\_Hash$[] or Genesis_block after validation with SMC [] and TM [id]

Step 3: SMC generate XOR for previous $Prev\_Hash$[] using below function

X_key← XOR($Prev\_Hash$[])

Step 4 : SMC selects random text or number called ***Rand_Text*** and encrypt **using** X_key

Encode_cipher ← cipher($Prev\_Hash$[]),X_key)

And send ***Encode_cipher*** **to** TM [id]

Step 4: TM [id]generate XOR for previous $Prev\_Hash$[] using below function

Y_key← XOR($Prev\_Hash$[])

Dencode_cipher ← docipher($Prev\_Hash$[]),Y_key)

Step 5 : if (*Encode_cipher* == *Dencode_cipher*)

Authenticated TM

Else

Malicious TM

End if

5. Results and Discussions

An open-source environment was used for the implementation, which included a CPU clocked at 3.0 GHz and 16GB of RAM. The JDK 1.8 environment was used for the implementation. It has been proposed to utilize a custom blockchain inside a Java environment. Building a variable number of virtual nodes—between four and one hundred at most—requires a distributed method. Below is an overview of the conclusions drawn from the in-depth experimental examination. In academic research and publishing, tables and figures are often used to provide data and information in a visual style. These graphic aids improve comprehension and interpretation of all the data that were gathered.

Table 1: Performance evaluation of Hash generation and transaction mining algorithm with different data sizes

Data Size	Hash Generation	Mining
1 MB	25	50
2 MB	40	90
3 MB	61	128
4 MB	95	145
5 MB	110	198
10 MB	203	201

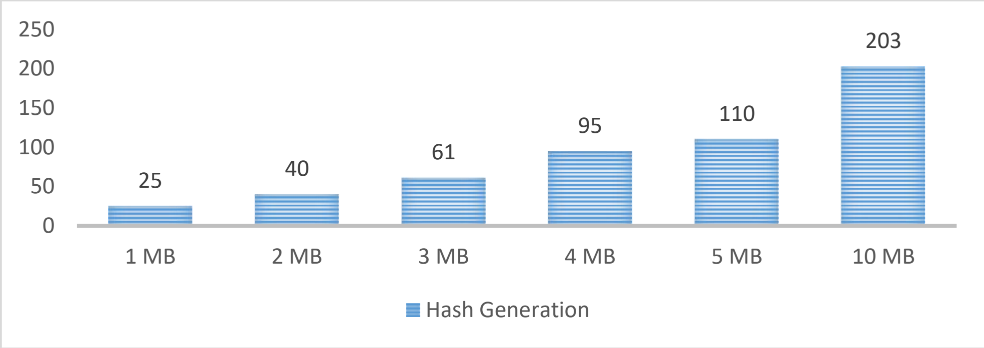

Fig 5: Time (no of seconds) required for hash generation with different data size

The link between the volume of data and the equivalent time required for hash production is shown in Figure 5. Transactional data is subjected to one-way hashes using the SHA family of algorithms. The above chart shows that the increase in data size and the accompanying increase in time needed are positively correlated.

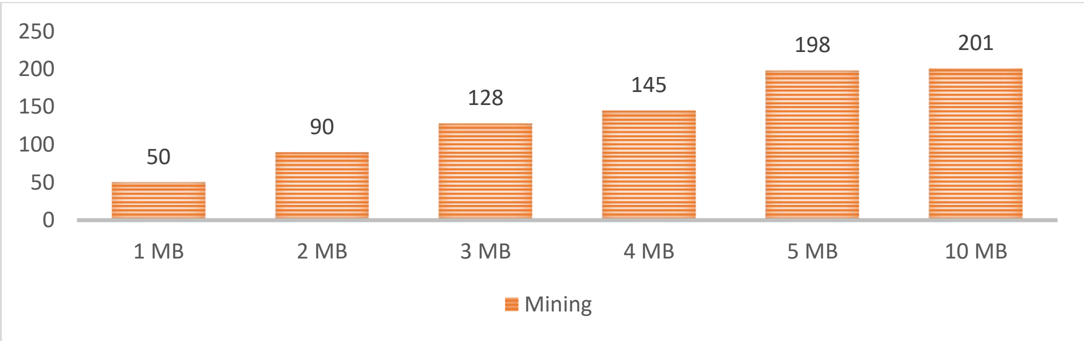

Fig 6: Time (no of seconds) required for transaction mining with different data size

The time of transaction mining across different data volumes is shown in Figure 6. Transaction mining is carried out based on the algorithmic difficulty that is set in the smart contract.

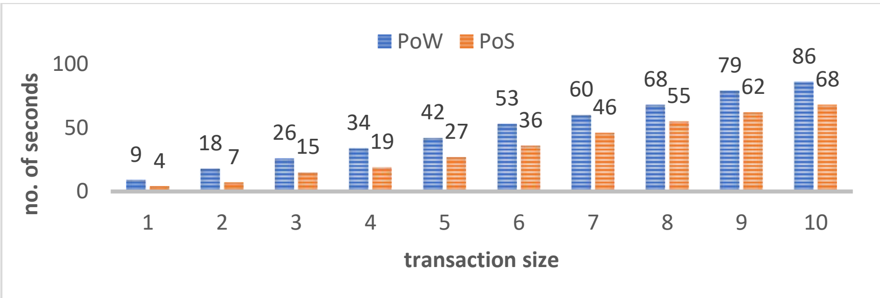

Fig 7: Time required (in seconds) for PoW and PoS for transaction mining

A comparison of PoW and PoS for transaction mining based on necessary time is shown in Figure 7 above. Whereas the PoS algorithm chooses a single miner for transaction mining based on a predetermined strategy, the PoW algorithm uses the largest number of miners to solve the algorithm's difficulty. Throughout the whole mining process, the PoS lowers time and power usage while improving system efficiency.

6. Conclusion

This study explores the use of blockchain and IoT in the supply chain model, specifically focusing on how it might benefit farmers and industrialists by ensuring a consistent supply of crops and providing detailed information on crop production and costs. The suggested technique delineates a systematic procedure that starts with a data requisition from an industrialist, which is thereafter transferred securely over the Blockchain network. Implementing a consensus process improves the security and secrecy of transactions, strengthening the fault-tolerant characteristics of distributed and multi-agent systems. This approach, in conjunction with the inherent capabilities of Blockchain, establishes the foundation for a dependable and impervious record of data transfers including the crop suggestion dataset. Additionally, the introduced system plays a role in the continuous digitalization of the agricultural sector, promoting effective and protected sharing of data that is in line with current requirements.

References

[1] P. Cui, J. Dixon, U. Guin and D. Dimase, "A Blockchain-Based Framework for Supply Chain Provenance," in IEEE Access, vol. 7, pp. 157113-157125, 2019, doi: 10.1109/ACCESS.2019.

[2] Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho and H. Y. Lam, "Blockchain-Driven IoT for Food Traceability with an Integrated Consensus Mechanism," in IEEE Access, vol. 7, pp. 129000-129017, 2019, doi: 10.1109/ACCESS.2019.

[3] U. Agarwal et al., "Blockchain Technology for Secure Supply Chain Management: A Comprehensive Review," in IEEE Access, vol. 10, pp. 85493-85517, 2022, doi: 10.1109/ACCESS.2022.

[4] M. N. M. Bhutta and M. Ahmad, "Secure Identification, Traceability and Real-Time Tracking of Agricultural Food Supply During Transportation Using Internet of Things," in IEEE Access, vol. 9, pp. 65660-65675, 2021, doi: 10.1109/ACCESS.2021.

[5] Wang, Baocheng & Li, Zetao & Li, Haibin. (2020). Hybrid Consensus Algorithm Based on Modified Proof-of-Probability and DPoS. Future Internet. 12. 122. 10.

[6] Li, Kejiao & Li, Hui & Wang, Han & An, Huiyao & Lu, Ping & Yi, Peng & Zhu, Fusheng. (2020). PoV: An Efficient Voting- Based Consensus Algorithm for Consortium Blockchains. Frontiers in Blockchain.

[7] Shaik, Vaseem Akram & Malik, Praveen & Singh, Rajesh & Gehlot, Anita & Tanwar, Sudeep. (2020). Adoption of blockchain technology in various realms: Opportunities and challenges. Security and Privacy.

[8] Tanwar, Sudeep. (2022). Decentralization and Architecture of Blockchain Technology. 10.1007/978-981-19-1488-1_3.

[9] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," in IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184-1195, April 2018, doi: 10.1109/JIOT.2018.2812239.

[10] Reyna, Ana & Martín, Cristian & Chen, Jaime & Soler, Enrique & Díaz, Manuel. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems. 88. 173-190. 10.1016/j.future.2018.

[11] Antonina A. Filimonova, Andrey A. Chichirov, Alexander V. Pechenkin, Artem S. Vinogradov. (2023). Technological Scheme of a Solid Oxide Fuel Cell – Microturbine Hybrid Power Plant for Electricity Production. International Journal of Intelligent Systems and Applications in Engineering, 11(3s), 301–306. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2694

[12] Ronghua Xu; Yu Chen; Erik Blasch, "Decentralized Access Control for IoT Based on Blockchain and Smart Contract," in Modeling and Design of Secure Internet of Things, IEEE, 2020, pp.505-528, doi: 10.1002/9781119593386.

[13] H. Al Breiki, L. Al Qassem, K. Salah, M. Habib Ur Rehman and D. Sevtinovic, "Decentralized Access Control for IoT Data Using Blockchain and Trusted Oracles," 2019 IEEE International Conference on Industrial Internet (ICII), 2019, pp. 248-257, doi: 10.1109/ICII.2019.

[14] Tanwar, Sudeep. (2022). Blockchain for Supply Chain Management. 10.1007/978-981-19-1488-1_12.

[15] Rejeb, Abderahman & Keogh, John & Treiblmaier, Horst. (2019). Leveraging the Internet of Things and Blockchain Technology in Supply Chain Management. Future Internet. 11.

[16] Mabrook Al-Rahmani "A Blockchain based Trust Model for Internet of Things Supply chain Management" MDPI 2021.

[17] M. S. Al-Rakhami and M. Al-Mashari, "ProChain: Provenance- Aware Traceability Framework for IoT-Based Supply Chain Systems," in IEEE Access, vol. 10, pp. 3631-3642, 2022

[18] [18Mr. Kaustubh Patil. (2013). Optimization of Classified Satellite Images using DWT and Fuzzy Logic. International Journal of New Practices in Management and Engineering, 2(02), 08 - 12. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/15

[19] Song, Qun, Yuhao Chen, Yan Zhong, Kun Lan, Simon Fong, and Rui Tang. "A supply-chain system framework based on internet of things using blockchain technology." ACM Transactions on Internet Technology (TOIT) 21, no. 1 (2021): 1-24.

[20] M. N. M. Bhutta et al., "A Survey on Blockchain Technology: Evolution, Architecture and Security," in IEEE Access, vol. 9, pp. 61048-61073, 2021

[21] Qian, Yaou & Meng, Mark Huasong. (2018). The Blockchain Application in Supply Chain Management: Opportunities, Challenges and Outlook. 10.29007

[22] Laaper, S., J. Fitzgerald, E. Quasney, W. Yeh, and M. Basir. "Using blockchain to drive supply chain innovation." In Digit. Supply Chain Manag. Logist. Proc. Hambg. Int. Conf. Logist, vol. 1, p. 2013. 2017.

[23] Alkhader, Walaa & Salah, Khaled & Sleptchenko, Andrei & Jayaraman, Raja & Yaqoob, Ibrar & Omar, Mohammed. (2021). Blockchain-Based Decentralized Digital Manufacturing and Supply for

COVID-19 Medical Devices and Supplies. IEEE Access. PP. 1-1. 10.1109

[24] K. Agrawal, M. Aggarwal, S. Tanwar, G. Sharma, P. N. Bokoro and R. Sharma, "An Extensive Blockchain based Applications Survey: Tools, Frameworks, Opportunities, Challenges and Solutions," in IEEE Access, 2022

[25] G. Subramanian, A. SreekantanThampy, N. Valbosco Ugwuoke and B. Ramnani, "Crypto Pharmacy – Digital Medicine: A Mobile Application Integrated With Hybrid Blockchain to Tackle the Issues in Pharma Supply Chain" in IEEE Open Journal of the Computer Society, vol. 2, no. 01, pp. 26-37, 2021.

[26] F. M. Benčić, P. Skočir and I. P. Žarko, "DL-Tags: DLT and Smart Tags for Decentralized, Privacy-Preserving, and Verifiable Supply Chain Management," in IEEE Access, vol. 7, pp. 46198-46209, 2019

[27] S. Jangirala, A. K. Das and A. V. Vasilakos, "Designing Secure Lightweight Blockchain-Enabled RFID-Based Authentication Protocol for Supply Chains in 5G Mobile Edge Computing Environment," in IEEE Transactions on Industrial Informatics, vol. 16, no. 11, pp. 7081-7093, Nov. 2020

[28] Pourvahab, Mehran, and Gholamhossein Ekbatanifard. "An efficient forensics architecture in IoT using blockchain technology." IEEE Access 7 (2019): 99573-99588.

[29] N. Fotiou, I. Pittaras, V. A. Siris, S. Voulgaris and G. C. Polyzos, "Secure IoT Access at Scale Using Blockchains and Smart Contracts," 2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), 2019, pp. 1-6, doi: 10.1109/WoWMoM.2019.

[30] K. Kataoka, S. Gangwar and P. Podili, "Trust list: Internet-wide and distributed IoT traffic management using blockchain and SDN," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), 2018, pp. 296-301

[31] Juan Garcia, Guðmundsdóttir Anna, Johansson Anna, Maria Jansen, Anna Wagner. Machine Learning for Decision Science in Healthcare and Medical Systems. Kuwait Journal of Machine Learning, 2(4). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/210

[32] Azizi, Neda, Heliyeh Malek Zadeh, Peyman Akhavan, Omid Haass, Shahrzad Saremi, and Seyedali Mirjalili. 2021. "IoT– Blockchain: Harnessing the Power of Internet of Thing and Blockchain for Smart Supply Chain" Sensors 21, no. 18: 6048

[33] Mann, Suruchi, Vidyasagar Potdar, Raj Shekhar Gajavilli, and Anulipt Chandan. "Blockchain technology for supply chain traceability, transparency and data provenance." In Proceedings of the 2018 international conference on blockchain technology and application, pp. 22-26. 2018.

[34] Dong, Yuhong, Zetian Fu, Stevan Stankovski, Siyu Wang, and Xinxing Li. "Nutritional quality and safety traceability system for China's leafy vegetable supply chain based on fault tree analysis and QR code." IEEE Access 8 (2020): 161261-161275.

[35] Cai, Hongming, Li Da Xu, Boyi Xu, Cheng Xie, Shaojun Qin, and Lihong Jiang. "IoT-based configurable information serviceplatform for product lifecycle management." IEEE Transactions on Industrial Informatics 10, no. 2 (2014): 1558-1567.

[36] Ali, Muhammad Salek, Massimo Vecchio, Miguel Pincheira, Koustabh Dolui, Fabio Antonelli, and Mubashir Husain Rehmani. "Applications of blockchains in the Internet of Things: A comprehensive survey." IEEE Communications Surveys & Tutorials 21, no. 2 (2018): 1676-1717.

[37] Maroufi, Mohammad & Abdolee, Reza & Mozaffari Tazehkand, Behzad. (2019). On the Convergence of Blockchain and Internet of Things (IoT) Technologies. Journal of Strategic Innovation and Sustainability. 14. 10.33423

[38] Vadgama, Nikhil, and Paolo Tasca. "An Analysis of BC adoption in supply chains between 2010 and 2020." Frontiers in BC 4 (2021): 8.

[39] Dhablia, A. (2021). Integrated Sentimental Analysis with Machine Learning Model to Evaluate the Review of Viewers. Machine Learning Applications in Engineering Education and Management, 1(2), 07–12. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/12

[40] Gonczol, Peter, et al. "BC implementations and use cases for supply chains-a survey." IEEE Access 8 (2020): 11856-11871.

[41] Prabha, P., Chatterjee, K. Design and implementation of hybrid consensus mechanism for IoT based healthcare system security. Int. j. inf. tecnol., 1381–1396 (2022).

[42] Samy, Hossam & Tammam, Ashraf & Fahmy, Ahmed & Hasan, Bahaa. (2021). Enhancing the performance of the blockchain consensus algorithm using multithreading technology. Ain Shams Engineering Journal. 12. 10.1016/j.asej.2021.01.019.

[43] W. Wang et al., "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," in IEEE Access, vol. 7,

pp. 22328-22370, 2019, doi: 10.1109/ACCESS.2019.2896108.

[44] B. Lashkari and P. Musilek, "A Comprehensive Review of Blockchain Consensus Mechanisms," in IEEE Access, vol. 9, pp. 43620-43652, 2021, doi: 10.1109/ACCESS.2021.3065880.

[45] S. Aich, S. Chakraborty, M. Sain, H. -i. Lee and H. -C. Kim, "A Review on Benefits of IoT Integrated Blockchain based Supply Chain Management Implementations across Different Sectors with Case Study," 2019 21st International Conference on Advanced Communication Technology (ICACT), 2019, pp. 138- 141, doi: 10.23919/ICACT.2019.8701910.

[46] M. P. Caro, M. S. Ali, M. Vecchio and R. Giaffreda, "Blockchain- based traceability in Agri-Food supply chain management: A practical implementation," 2018 IoT Vertical and Topical Summit on Agriculture - Tuscany (IOT Tuscany), 2018, pp. 1-4, doi: 10.1109/IOT-TUSCANY.2018.8373021.

[47] Examples from Blockchain Implementations in Logistics and Supply Chain Management: Exploring the Mindful Use of a New Technology

[48] B. Subashini and D. Hemavathi, "Detecting the Traceability Issues in Supply chain Industries using Blockchain Technology," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), 2022, pp. 1-8

[49] Li Wei, Machine Learning in Fraudulent E-commerce Review Detection , Machine Learning Applications Conference Proceedings, Vol 2 2022.

[50] K. Pundir, J. D. Jagannath, M. Chakraborty and L. Ganpathy, "Technology Integration for Improved Performance: A Case Study in Digitization of Supply Chain with Integration of Internet of Things and Blockchain Technology," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019, pp. 0170-0176

[51] Agriculture crop production in India, “https://www.kaggle.com/datasets/srinivas1/agricuture-crops- production-in-india?select=datafile.csv”.