International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8484
***Article Received:** 27 July 2023 **Revised:** 18 September 2023 **Accepted:** 02 October 2023*

An Effective Supply Chain Model using Blockchain in IoT with Trust Enabled Hybrid Concensus Algorithm

Yassir Farooqui[*1], Dr. Swapnil M. Parikh[2]
[1]Ph.D. Scholar & Assistant Professor
Computer Science & Engineering Department
Parul Institute of Engineering & Technology
Parul University
Vadodara,Gujarat,India
yassir.farooqui270062@paruluniversity.ac.in
[2]Professor & Principal
Computer Science & Engineering Department
Parul Institute of Technology
Parul University
Vadodara,Gujarat, India
swapnil.parikh17761@paruluniversity.ac.in

Abstract— With the rapid growth of multiagent systems, concerns about privacy and security have assumed a position of paramount importance. Blockchain technology has gained a lot of attention since it first appeared because of its benefits in terms of decentralization, accessibility, traceability, and the capacity to be trustless. The increasingly complicated supply chains in today's world face significant issues regarding traceability and integrity. Blockchain technology holds out the possibility of developing a new concept for supply chain traceability, lapping these worries. Thus, in this research, the trust enable hybrid consensus algorithm is proposed for establishing consistency in the network with the irrelevant traders. The authorization is identified by the proposed model for accessing the Blockchain network depending on the accessibility rules. Depending on the various information sources, the authenticity of data is calculated, which makes the interaction between both the agent as well as the resource. The efficiency of the proposed model is determined by three different measures for secure data transfer. The attained minimal transaction time is 0.856 ms, memory usage is 87.684 KB, and responsiveness is 3.599 ms, respectively.

Keywords- Blockchain, Hybrid consensus algorithm, Internet of Things, supply chain.

I. INTRODUCTION

The supply chain is a complex process due to the periodic changes that occur in the systems, and these supply chains are important because it carries information about the organizations. It also consists of information about the upcoming activities of the organization, which initiates a need for protection due to its sensitive information. The incorporation of IoT (Internet of things) plays a crucial role in these supply chains, which highly reduces the labour cost occurred during the data collection and analysis process. The supply chain can be made more efficient if the organizations accompany the process of production to sales [11][5]. In addition, the relationship between the producer and the supplier, logistics, and consumer is maintained through these supply chains by the means of business-to-business relations and business-to-consumer relations. In the process of supply chain management of products or goods, the goods should be delivered with complete protectiveness from the source to the destination due to the advancement and competitiveness in the business field [2]. The rapid rise in globalization initiates difficulties in ensuring the security and integrity of the supply chain and the usage of IoT devices becomes a promising solution to record and trace the process on its own without manual intervention [12][1].Although IoT devices are widely used in supply chain management, due to their enhanced techniques and algorithms current business individuals find difficulties in using IoT devices for supply chain management because multiple unauthorized IoT devices access the resources through illegal access. The security of IoT devices becomes a major dispute and as an effective solution, the Blockchain network is enabled for the enhancing of the supply chain management security that avails in IoT devices [5]. The execution of Blockchain networks in IoT devices highly needs the association of all the members involved in the supply chain

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8484
***Article Received:** 27 July 2023 **Revised:** 18 September 2023 **Accepted:** 02 October 2023*

management to develop collaborative ecosystems [10]. The current performance evaluation of the system with a deeper analysis of data could be performed using the smart supply chain [4][9]. The major problem that occurs in the traditional supply chain is the trust issues between the consumer and the supplier and that can be effectively resolved by enabling the smart contract. The smart contract is a protocol used in will need to create these components, incorporating the applicable criteria that follow.

Blockchain networks for the effective tracking of legal information automatically without the intervention of third parties. The smart contract also makes the supply chain smart by enabling and recording the data available in a trustful way and the data becomes unchangeable with access to only authorized users [13][9].

The researchers preserve that while Blockchain is a useful system for controlling supply chain transparency, it is inadequate on its own to ensure the accuracy of data on the standard of goods and the dependability of supply chain participants. Once registered on the BC, false data produced by supply chain participants become unchangeable. Using the proposed modified consensus algorithm to penalize and reward dishonest and trustworthy participants, respectively, is one method to increase the trust and dependability of the data. These techniques rely on a system of trust management, which we suggest incorporating into a supply chain BC. Data produced by the Internet of Things (IoT) sensors, which are progressively being integrated into different phases of the supply chain lifecycle, may also be useful to such a system

The remaining section involved in this paper is organized as follows: Section 2 reveals the review of the existing works with the challenges. Section 3 reveals the system model and proposed methodology for the hybrid trust-enabled reputed consensus algorithm. Section 4 reveals the results and discussion of the proposed as well as the other existing methods. Finally, section 5 concludes the paper.

II. LITERATURE REVIEW

The review of the various existing methods for the secure transmission of data is as follows,

Mabrook S. Al-Rakhami and Majed Al-Mashari [1], introduced a traceability-based framework that addressed the issues raised by the supply chain mechanism's security considerations. Distributed blockchain technology maintains the scalability, costs, and quantum resilience. The system achieved good tractability, security, and traceability; however, power and computational capacity should still be further optimized.

Muhammad Nasir Mumtaz Bhutta and Muneer Ahmad [2] perpetuated the supply chain management systems through continuous monitoring and reporting of information to the networks that highly ensured the privacy and security of the system, as well as this method, provided a digital blockchain for the availing of the information about the goods. Although the supply chain is enhanced, this method mainly focused on agriculture and can be generalized for overall purposes.

Walaa Alkhader *et al.* [3] dwelled with the medical chain supply especially during the pandemic times, through the decentralized digital environment using the Blockchain network, which enhanced the trustworthiness of the supply chain system. The system needs to be improved in terms of allocating responsibilities, initiating policies, and certain other attributes.

Pinchen Cui *et al.* [4] focused on the traceability characteristics of the supply chain system through the Blockchain network that enabled the suppliers as well as consumers to track the information about the product. This method provided a highly secure and reliable solution, but an extension for the development of the tamper-resistant characteristics is necessary.

Ganesan Subramanian *et al.* [6] integrated and developed a hybridized Blockchain for the supply chain system and provided transparency to the users and every user with valid authentication fetched the details about the product. The interpretability of the system is considerably low acts as a disadvantage of the system.

Qun Song *et al.* [11] innovated an access control mechanism that allows the user to provide their information through a registration module and whenever a mis operation occurs, that information is utilized for the detection of unauthorized access and is attained through the usage of Blockchain-based mechanisms. The stability and the guarantee of the system are provided by this system and the disadvantage of the system is that the demonstration is made using fewer samples.

III. TRUST ENABLED REPUTED CONCESUS ALGORITHM

This ledger is accurate and extremely safe because it makes use of cryptographic techniques like the hash function and digital signature. This modification or development is governed by consensus, or mutual agreement [7][11]. Consensus algorithms are used in blockchain because it lacks a central controller. Depending on when a distributed consensus is required, different consensus algorithms can be used. There are also different kinds of blockchain networks.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8484
Article Received: *27 July 2023* ***Revised:*** *18 September 2023* ***Accepted:*** *02 October 2023*

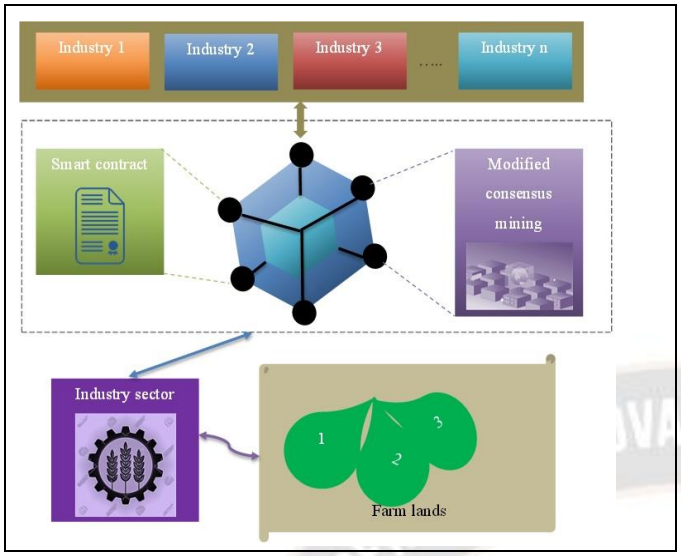

Figure.1 System model for trust enabled reputed consensus mechanism

In a situation when these traders do not trust one another, a consensus algorithm is a process employed to promote all traders into contracts and trust with one another. A hybrid trust-enabled reputed consensus algorithm is developed to establish consistency in a network with many untrustworthy traders [16]. The system model for the trust-enabled reputed consensus algorithm is described in figure 1.

3.1 PROPOSED TRUST ENABLE HYBRID CONCENSUS ALGORITHM

Three major parts make up the proposed model: the authority layer, the IoT layer, the Blockchain layer, and the application layer as revealed in figure 2. The first transceiver includes information gathered by sensors throughout the supply chain and from transactions between its participants. This unprocessed data can be stored in the supply chain's application layer's database, whereas the cryptographically altered data is sent as a transaction from the IoT module to the Blockchain layer. The proposed hybrid trust enabled reputed consensus, which establishes which one has the authority to contribute to and read from the data kept in the Blockchain, so that such transactions are recorded, preserved, and executed at the Blockchain following the set rules for accessibility. The current supply chain is a nonlinear economic approach that meets requirements either directly or indirectly. However, this approach has significant drawbacks, such as the connections between the supply chain's participants or the insufficient information provided to consumers regarding the products' places of origin. In this research, a new blockchain-based supply chain model is proposed by integrating the improved consensus algorithm.

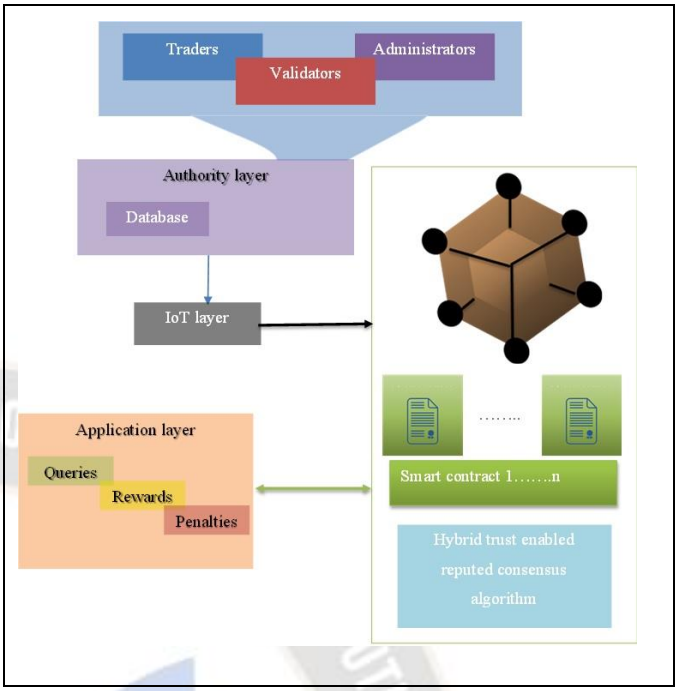

Figure.2 Proposed model for trust enabled reputed consensus system

The proposed trust-enabled reputed consensus technique accomplishes this goal by calculating reputation ratings for transactions and authorized parties at a finer level and assessing the authenticity of the supply chain data. Traders, validators, administrators' inquiries, and transaction requests are mostly handled by the application layer. The application layer implements penalties and incentives depending on the outcomes of the queries and the function of the appropriate authority.

3.1.1 Authority Layer

Depending on the regulatory endorsement data presented in the formation of reports, regulatory ratings $r_{reg}(t)$, are established. Transactions and smart contracts, which are described in the following section, are used to generate all of the ratings. The BC layer receives the generated sensor ratings $r_s(t)$, trader ratings $r_{trader}(t)$, and regulatory rating $r_{reg}(t)$ at a time t.

3.1.2 IoT Layer

The authority layer receives inputs from streams of the sensor, trader, and regulatory ratings, in which the authority layer creates transactions depending on the input ratings for the BC layer. A trade event is defined as a modification in ownership of a commodity in which the BC is annexed with the trader rating $r_{trader}(t)$, which is given by the client for the farmer. The rating is determined by evaluating the commodity that was traded according to pre-arranged terms between the trading parties.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8484
Article Received: *27 July 2023* ***Revised:*** *18 September 2023* ***Accepted:*** *02 October 2023*

3.1.3 Blockchain Layer

The authorization for registering transactions, receiving access to the Blockchain system, altering details, and other operations for supply chain entities are defined by the Blockchain layer. All supply chain participants and farm products have digital profiles that are kept up to date by the BC layer.

3.1.3.1 Transactions

The transactions that are executed at the Blockchain layer are described in this section. These transactions affect the state of the individuals (such as a trader's reputation) and the farm products (such as ownership changes) in the supply chain and are recorded on the smart contract. The generated transaction TN_g, the trader transaction TN_{trader}, the sensory transaction TN_s, the regulator transaction TN_{reg}, and the receipt of product transaction TN_{rc} are among the transactions at the blockchain layer, with the following details.

Starting with a generated transaction TN_g, which is provided by a raw material to validate the existence of a newly created specific product and designate the performance of the smart contract, how this product will be associated with a transaction that contains information about the generation of each specific product. The source of the TN_g is:

$$TN_g = \left[TN_{ID} \left| h_d \right| \mathrm{T}_{ID}^1 \left| C_{ID} \right| \alpha' \left| u' \right| \right] \quad (1)$$

where T_{ID}^1 is the identification of the commodity farmer, TN_{ID} is the identification of the commodity, h_d is the hash of the transaction data, and C_{ID} is the identifier of the quality contract the commodity is connected to. The commodity farmer's signature and public key are α' and u'. A commodity is physically transferred from a farmer to a client as part of the trade transaction:

$$TN_{trader} = \left[tr_{ID} \left| h_d \right| ID_c \left| C_{ID} \right| \alpha_F' \left| u_F' \right| \alpha_c' \left| u_c' \right| \right] \quad (2)$$

where T_{ID}^1 is substituted with ID_c, the client's identification number, and TN_{ID}, h_d are analogous to TN_g. The public keys and signatures of the client and farmer are denoted by α_F', u_F', α_c', and u_c', respectively. IoT devices can use sensory transactions, or TN_s, to log TN_g IoT sensors often have limited processing capabilities, thus the gateway traders that are identifiable by device IDs produce these transactions. Providing a sensory transaction are:

$$TN_S = \left[TN_{ID} \left| h_d \right| \alpha_S' \right] \quad (3)$$

where α_S' is the signature of the gateway trader that is creating the sensory transactions, h_d is the IoT sensor stream hash, and TN_{ID} is the identification of the commodity. The regulator assigns a rating for the farmer, $r_{reg}(t)$, via the regulator transaction TN_{reg} after physically inspecting a storage facility.

$$TN_{reg} = \left[ID_{trader} \left| h_d \right| tr_{type} \right] \quad (4)$$

where the trader's identification is ID_{trader}, the observation evidence's hash is h_d, and the type of the product for which the performance is being given is tr_{type}. The receipt of commodity transactions TN_{rc} is created to log the end of the production chain on BC when a commodity is received at the retailer's end.

$$TN_{rc} = \left[TN_{ID} \left| \alpha_{RC}' \right| u_{RC}' \right] \quad (5)$$

where α_{RC}' and u_{RC}' stand for the receiving distributor's private keys, respectively, and TN_{ID} stands for the commodity's distributor identity. The transaction serves two purposes, initially, it enforces the reliability consensus mechanism and uploads $r_s(t)$. Second, for security reasons, it is necessary to keep the supplies completing the supplier chain as the resources with no dynamic chains may be identified as fakes.

3.3.2 Smart Contracts

When transactions related to a supply chain session are registered on BC, a reputable consensus mechanism for smart contracts in hybrid trust enabled is used to calculate ratings of authorities and farm products. These ratings are computed automatically, transparently, securely, and efficiently using smart contracts, doing away with the requirement for any distribution channels. Supply chain entities are motivated by smart contracts to determine the ratings, in addition to the reward and disciplinary processes at the application layer. The commercial system administrators of distributed blockchain or a division of an organization deploy the smart contracts.

i) Quality contract:

For about every supply chain commodity, a quality contract is installed on a trusted consensus algorithm that supports hybrid trust and lists the quality rating standards. When a primary producer issue TN_g, which ties the newly generated

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8484
Article Received: *27 July 2023* ***Revised:*** *18 September 2023* ***Accepted:*** *02 October 2023*

commodity so then quality contract is instantiated. The rating contract uses the reputation score of the commodity $r_s(t)$, which is invoked as a result of a trading transaction TN_{trader}, to determine the reputation of the farmer. We generate r_s to generate the related commodity reputation ratings when a commodity's supply chain includes n trading transactions.

$$r_s = \left[r_s(t_0), r_s(t_1), ...r_s(t_{n-1}) \right] \quad (6)$$

ii) Rating contract

The rating contract is used to calculate the reputation of the farmer, $r_F(t)$ involving a client and a farmer that occurs at time t using three inputs: Initially, the sensing rate of the trader commodity $r_s(t)$, second, rating for the farmer $r_{reg}(t)$, and third the trader's rating for the farmer $r_{trader}(t)$. A weighted sum can be used to calculate $r_F(t)$, which is formulated as follows,

$$r_F = w_1 \times r_s(t) + w_2 \times r_{trader}(t) + w_3 \times r_{reg}(t) \quad (7)$$

where the reputation constituents' weighting factors are represented as w_1, w_2 and w_3, in addition, the features of the supply chain decide the value of weighting factors.

3.3.3 Trust Enabled Reputed Consensus Algorithm

Whenever a trader first enters the supply chain network at instant t', it lacks any prior reputation from which to derive the trust score $\mathrm{T}_{trader}(t')$. Since each entity must maintain a minimum trust score to continue taking part in the Blockchain network, the initial trust score given to the trader is $\mathrm{T}_{trader}(t') = \mathrm{T}_{\min}$. The reputation and trust module updates the trader's trust score after initialization. Two phases are involved in computing the trust score: first, determining the trader's overall reputation score based on past and present reputation scores; second, determining the overall reputation based on the trust score and other application-specific criteria.

The two main algorithms in the past were proof of work (PoW) and proof of stake (PoS). With PoW, any trader can participate in inserting blocks to the chain by demonstrating that it has completed a labor-intensive computation. Mining is the process of creating new blocks using the PoW algorithm, in which the PoW-based blockchains are also energy-intensive, slow, and very inefficient. However, PoS lacks randomization, which could lead to participants with high stakes consistently winning the consensus and preventing participants with low stakes from revising their trust values. The main goal of PoS is to lower the excessive power consumption of blockchain networks caused by the PoW idea. Therefore, an alternative for avoiding computationally expensive puzzle-solving. Validators act in place of miners in this case,a validator is chosen to publish a block in the blockchain.

The various significant steps involved in the hybrid trust-enabled reputed consensus algorithm are as follows,

1. Read the ordinary traders

The traders involved in every transaction are required to register in the Blockchain network using the trader's ID, and the transaction details for various further transactions.

2. Establish the consensus security bin

i) ID of traders T_{ID}^1

ii) Transaction details T_{tr}^2

iii) Trust score issued by authorities T^3

iv) An overall behavioural score of traders $\mathrm{T}_{\mathrm{B}}^5$

The consensus security bin for the hybrid trust-enabled reputed consensus algorithm is described as follows,

$$\mathrm{M} = \left\{ \mathrm{T}_{ID}^1, \mathrm{T}_{tr}^2, \mathrm{T}^3, \mathrm{T}_{\mathrm{I}}^4, \mathrm{T}_{\mathrm{B}}^5 \right\} \quad (8)$$

3. Generation of access/trading request

A request R from the trader for active trading with the network, which is reached at the verifier premises, who validates the identity and confirms the transaction, as a sign of transaction validation.

$$R_{Trader} = \left\{ \mathrm{T}_{ID}^1, \mathrm{T}_{tr}^2, \mathrm{T}^3, \mathrm{T}_{\mathrm{I}}^4, \mathrm{T}_{\mathrm{B}}^5, d \right\} \quad (9)$$

Trust evaluation

The demand and the traders are authenticated and monitored in the next stage by our proposed consensus mechanism. The network's administrators keep an eye on activity to publicly commend and criticize network participants. Administrators have the option to inquire about the estimated trust scores for the relevant items and authorities. Administrators can publicly promote or penalize the participating parties by removing them from the entire network based on the score they obtain.

When a client requests approvals from nearby traders for a transaction, a trust evaluation is carried out. Before transactions can be fully inserted into the blockchain, the trader must submit transaction proposals to any accessible endorsing participants.

i) Direct trust D

The amount of trust the need for an agent calculates based on its own experiences regarding the target agent is known as a direct trust or local trust. Let $D_n^t(\mathrm{X}, Y)$ stand for the up to n transactions in the t^{th} time interval direct trust that agent X

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8484
Article Received: *27 July 2023* ***Revised:*** *18 September 2023* ***Accepted:*** *02 October 2023*

holds upon agent Y. The satisfaction index has been used to measure direct trust as follows:

$$D_n^t(\mathrm{X},Y) = s_n^t(\mathrm{X},Y) \quad (10)$$

ii) Indirect trust $\mathrm{I_T}$

Indirect trust, which is also known as a request, is calculated using the knowledge of other agents. When making transaction decisions, an agent often draws on the knowledge of other agents in the system, particularly when it has little to no experience with the target agency. An agent does this by asking other agents for recommendations regarding the target agent. The assessing agent then compiles recommendations from other agents and assesses the recommenders' response reliability. Let $\mathrm{I}_{\mathrm{T}n}^{\,t}(\mathrm{X},Y)$ represent the calculated indirect trust between agent X and agent Y. The total set of agents that have once cooperated with agent Y is represented by $w = TF(Y)$ (11)

iii) Historical trust H

Historical trust is a reflection of long-term behavioral patterns and is based on prior experience. By utilizing a logarithmic averaging update function because as time passes, the recent trend turns into a historical trend. Allow $\mathrm{H}_n^t(\mathrm{X},Y)$ to stand in for the historical confidence that an agent X has an agent Y.

$$\mathrm{H}_n^t(\mathrm{X},Y) = \frac{\rho \times \mathrm{H}_{n-1}^t(\mathrm{X},Y) + \mathrm{Re}\,\mathrm{T}_{n-1}^t(\mathrm{X},Y)}{2} \quad (12)$$

iv) Satisfactory trust S

The satisfactory trust involved in the trust evaluation during the trader transactions is formulated as,

$$S = \left(\frac{\mathrm{T}_{\max} - \mathrm{T}_{\min}}{\mathrm{T}_{avg}} \times r \right) \quad (13)$$

where, the maximum score for trust T is denoted as $\mathrm{T}_{\max}$, the minimum score for trust T is denoted as $\mathrm{T}_{\min}$, the average trust score is represented as T_{avg}.

v) Influential trust IF

The influencial trust involved in the trust evaluation during the trader transactions is formulated as,

$$IF = rand \times \mathrm{T} + \frac{1}{2}\alpha(\mathrm{T}_{t-1} - 1) \quad (14)$$

where, the trust score of the node in the previous iteration is denoted as $(t-1)$ and the influential order is expressed as α.

vi) Reputation factor RF

Consumers take into account the reputation scores referring to the present and past supply chain activities to determine the total reputation score $RF(t_n)$ for a trader at a time t_n, in which $r_F(t_0)\ r_F(t_1),\ldots..\ r_F(t_n)$ as,

$$RF(t_n) = \sum_{t=t_0}^{t=t_n} r_F(\mathrm{T}) \times \beta(t_n - t) \quad (15)$$

The proposed formula for trust calculation using the direct, indirect, historical, satisfactory, influencial, and reputation trust are as follows,

$$\mathrm{T} = w_1 \cdot \mathrm{I_T} + w_2 \cdot D + w_3 \cdot \mathrm{H} + w_4 \cdot S + w_5 \cdot IF + w_6 \cdot RF \quad (16)$$

Weights are adjustable as per trader movement in the network, in which the database update with the behavioral score

$$\mathrm{B} = \begin{cases} 1 & ;0 \le \mathrm{T} \le threshold \\ 0 & ;otherwise \end{cases} \quad (17)$$

If the score is 1, the trader is marked for good movement and genuine trading

Trust Enabled Hybrid Consensus algorithm	
1	Register Traders
2	Establish the Consensus Security Bin M $\mathrm{M} = \{\mathrm{T}_{ID}^1, \mathrm{T}_{tr}^2, \mathrm{T}^3, \mathrm{T}_{\mathrm{I}}^4, \mathrm{T}_{\mathrm{B}}^5\}$
3	Generation of access/trading request R_{Trader} $R_{Trader} = \{\mathrm{T}_{ID}^1, \mathrm{T}_{tr}^2, \mathrm{T}^3, \mathrm{T}_{\mathrm{I}}^4, \mathrm{T}_{\mathrm{B}}^5, d\}$
4	Verifier
	Validate trader's identity and transaction $S_v^* = \mathrm{M}^* \otimes \mathrm{E}(\mathrm{T}_{ID}^{'} + \alpha * u)$
5	Evaluate Trust
	Calculate direct trust
	$D_n^t(\mathrm{X},Y)$
	Calculate indirect trust
	$\mathrm{I}_{\mathrm{T}n}^{\,t}(\mathrm{X},Y)$
	Calculate historical trust
	$\mathrm{H}_n^t(\mathrm{X},Y)$
	Calculate satisfactory trust
	S
	Calculate influential trust
	IF
	Calculate reputation factor
	$RF(t_n)$
6	Calculate Overall Trust

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8484
Article Received: *27 July 2023* ***Revised:*** *18 September 2023* ***Accepted:*** *02 October 2023*

	Calculate overall trust using weighted sum of trust components
	$T = w_1 \cdot I_T + w_2 \cdot D + w_3 \cdot H + w_4 \cdot S + w_5 \cdot IF + w_6 \cdot RF$
7	Update Database with Behavioral Score B
8	Mark Trader for Good Movement and Genuine Trading
9	Terminate

IV. RESULTS

The reliability of trust enabled hybrid consensus algorithm depending on the transaction time, memory usage, and responsiveness for both the block size and available users in the network.

4.1 Experimental setup

The implementation of trust enable hybrid consensus algorithm is carried out in the PYTHON tool in the windows 10 operating system with 8GB RAM.

4.2 Dataset description

The agriculture crop production in India [18] database is utilized here by splitting into two different databases for analyzing the efficiency of trust enable hybrid consensus algorithm. In the initial database1, three different crop details are considered, which include arhar, cotton at 10 %, and other 39 crops at 80 %. In the second database2, the total production of crops is considered with different varieties of crops.

4.3 Performance measures

The measures considered for identifying the secure data transfer using the trust enable hybrid consensus algorithm is as follows,

Transaction time

The amount of time needed to transfer data from the drive to the host computer. The amount of data being transferred and its pace of transmission to and from the host will determine how long it takes.

Memory usage

The memory utilization command provides information on the amount of RAM space needed to hold a key and its value in bytes. The total amount of RAM allotted for data and administrative requirements that a key and its value require is the reported consumption.

Responsiveness

Responsiveness is the ability of a statistical measure to detect changes over time in the problem under research. If the responsiveness measure is higher, the time needed to inquire is longer. Reduced responsiveness will improve system efficacy and even provide a way to get away from the attacker.

4.4 Comparative analysis

The methods considered for comparing the performance of trust enable hybrid consensus algorithm is triple DES encryption algorithm [17], Hash-based secret key encryption algorithm [19], Certificate less signature scheme [20], checkpoint-enabled scalable Blockchain architecture [21], hybrid access control enabled consensus algorithm [22].

4.4.1 Based on database 1

(i) For block size

In figure 3a), when the initial blocksize is 20 then the attained transaction time is 0.909ms and for the final blocksize is100, the attained transaction time is 0. 856ms.Then the improved variation of the proposed method when compared with the other method is 82.48%.

In figure 3b), when the initial blocksize is 20 then the attained memory usage is 87.684 KB and for the final blocksize is 100, the attained memory usage is 90.164 KB. The improved variation of the proposed method when compared with the other method is 0.08%.

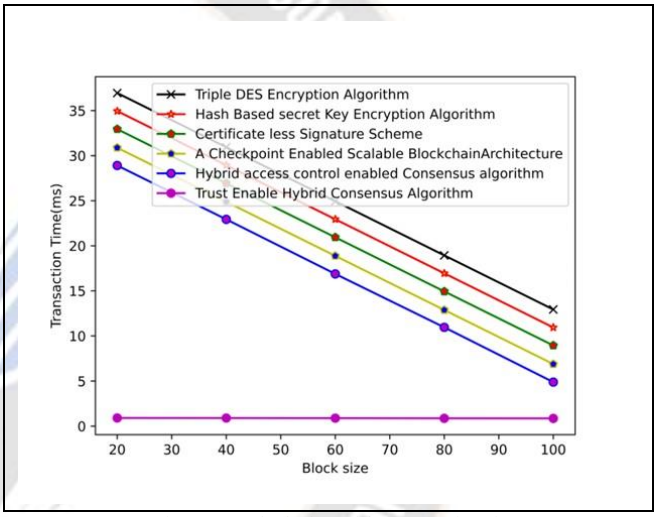

Figure 3a. Block size with Transaction time

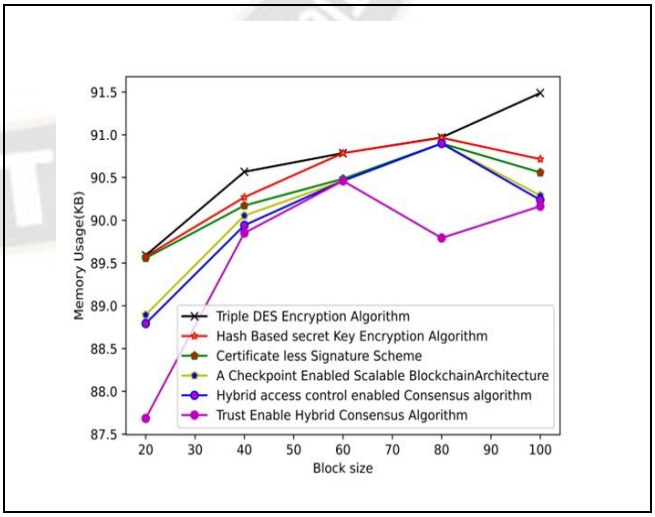

Figure 3b. Block size with memory usage

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8484
Article Received: *27 July 2023* ***Revised:*** *18 September 2023* ***Accepted:*** *02 October 2023*

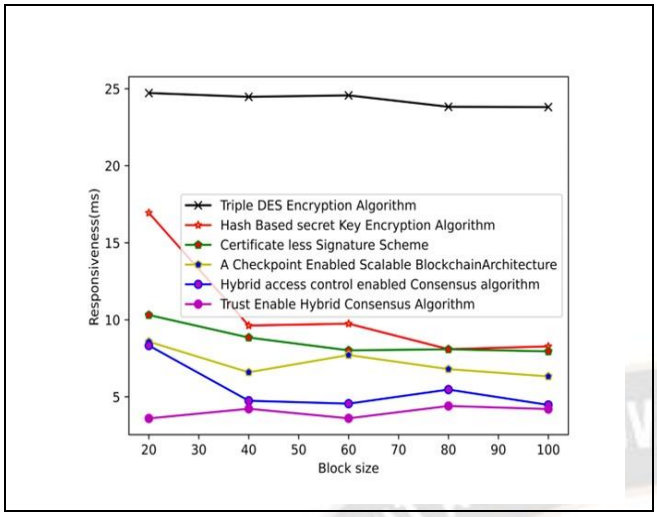

Figure 3c. Block size with Responsiveness

In figure 3c), when the initial block size is 20 then the attained responsiveness is 23.809ms and for the final block size is 100, the attained responsiveness is 4.205ms. Then the improved variation of the proposed method when compared with the other method is 5.99%

ii) For the user

In figure 4a), when the initial user count is 20 then the attained transaction time is 0.932ms and for the final user count is 100, the attained transaction time is 0.878ms. Similarly, when compared with the other method is 81.91%.

In figure 4b), when the initial user count is 20 then the attained memory usage is 90.637KB and for the final user count is 100, the attained transaction time is 90.039KB. Similarly, compared with the other method is 1.49%.

In figure 4c), when the initial user count is 20 then the attained responsiveness is 3.421ms and for the final user count is 100, the attained responsiveness is 16.914ms. Similarly, when compared with the other method is 27.68%.

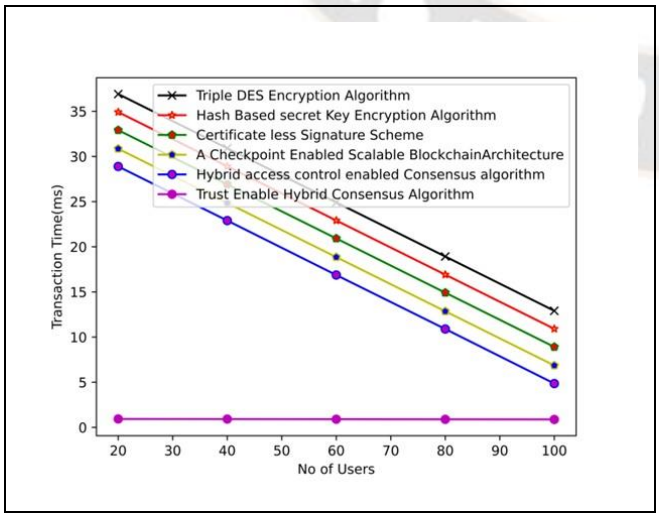

Figure 4a. No of Users with Transaction time

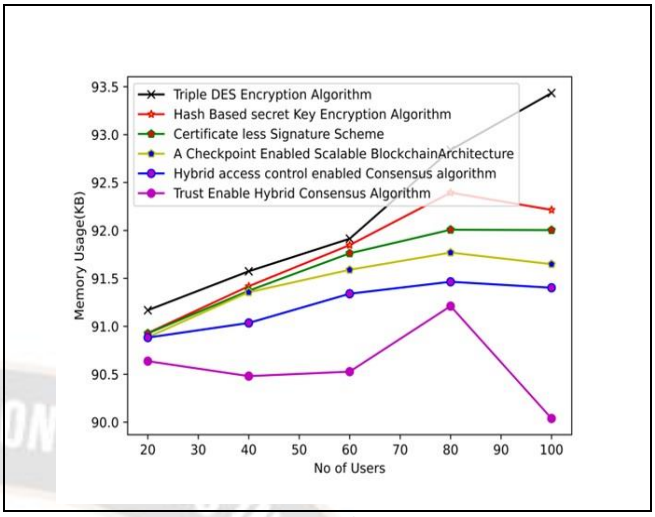

Figure 4b. No of users with Memory usage

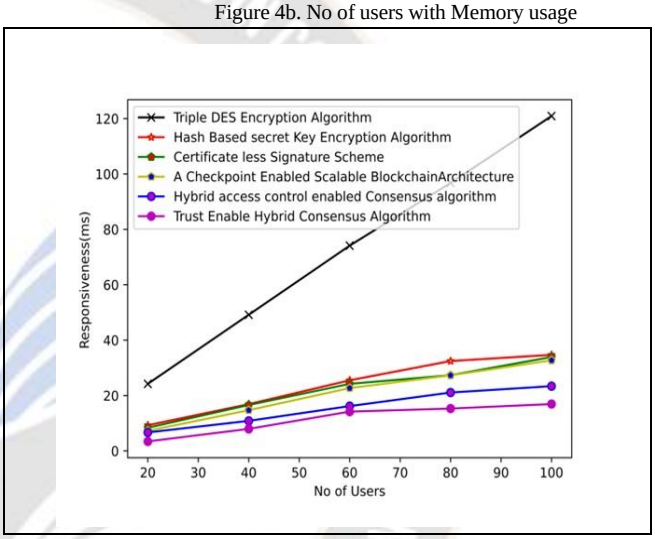

Figure 4c. No of users with Responsiveness

4.4.2 Based on database2

(i) For blocksize

In figure 5a), when the initial blocksize is 20 then the attained transaction time is 20.883ms and for the final blocksize is 100, the attained transaction time is 0.862ms.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8484
Article Received: *27 July 2023* ***Revised:*** *18 September 2023* ***Accepted:*** *02 October 2023*

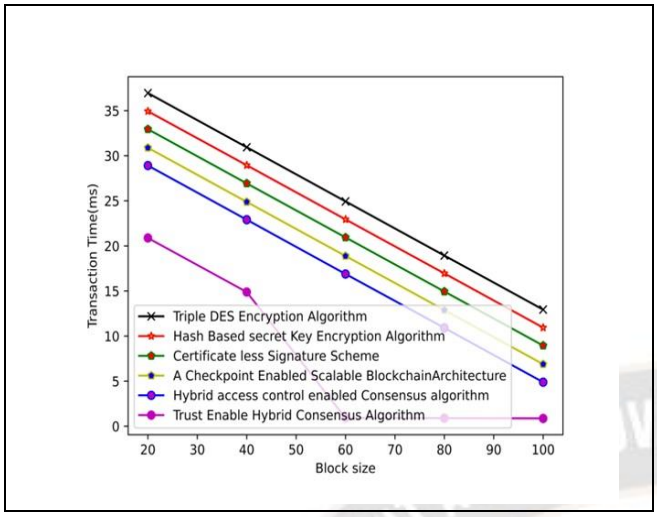

Figure 5a. Block size with Transaction time

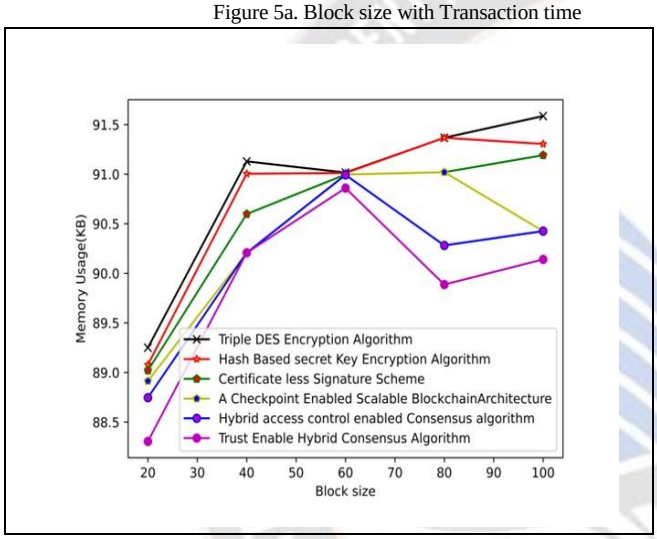

Figure 5b. Block size with Memory usage

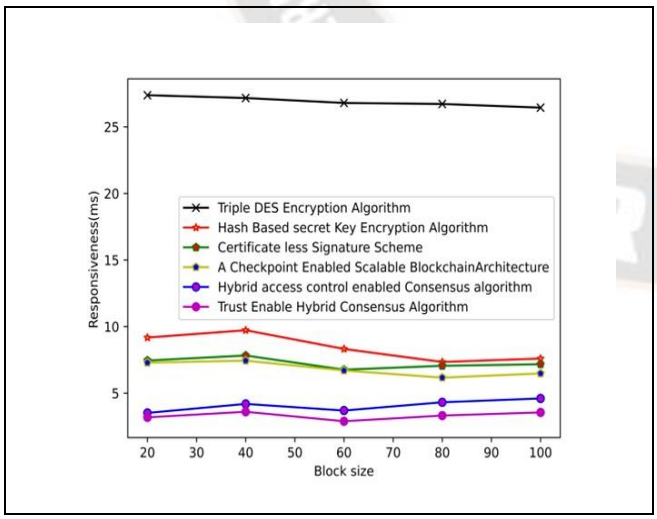

Figure 5c. Blocksize with Responsiveness

In figure 5b), when the initial blocksize is 20 then the attained memory usage is 88.305 KB and for the final blocksize is 100, the attained memory usage is 90.141 KB. Similarly, when compared with the other method is 0.32%.

In figure 5c), when the initial blocksize is 20 then the attained responsiveness is 3.179ms and for the final blocksize is 100, the attained responsiveness is 3.551ms Similarly, when compared with the other method is 22.83 %.

ii) For the user

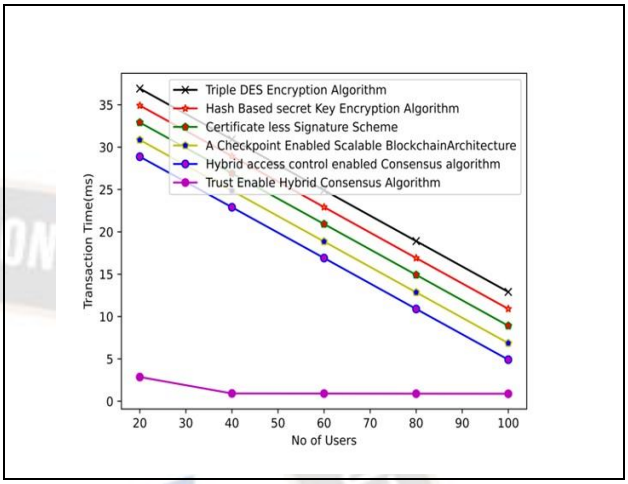

Figure 6a. No of users with Transaction time

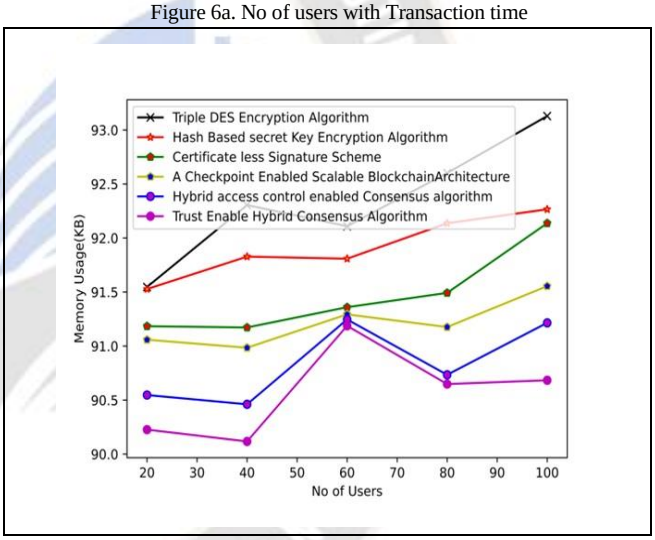

Figure 6b. No of users with memory usage

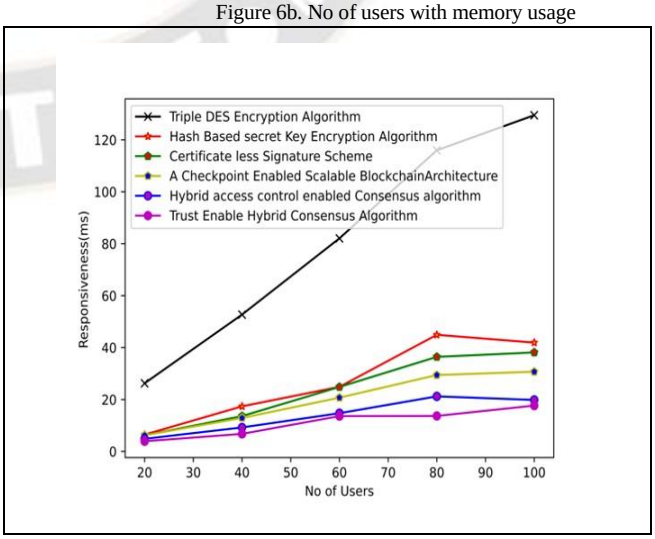

Figure 6c. No of users with responsiveness

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8484
***Article Received:** 27 July 2023 **Revised:** 18 September 2023 **Accepted:** 02 October 2023*

In figure 6a), when the initial user count is 20 then the attained transaction time is 2.856ms and for the final user count is 100, the attained transaction time is 0.880ms. Similarly, when compared with the other method is 82.05%.

In figure 6b), when the initial user count is 20 then the attained memory usage is 90.227 KB and for the final user count is 100, the attained memory usage is 90.684 KB. Similarly, when compared with the other method is 0.58%.

In figure 6c), when the initial user count is 20 then the attained responsiveness is 3.913ms and for the final user count is 100, the attained responsiveness is 17.662ms. Similarly, when compared with the other method is 10.93 %.

Methods	**Database 1**					
	Block size			**User**		
	Transaction time (ms)	***Memory usage (KB)***	***Responsiveness (ms)***	***Transaction time (ms)***	***Memory usage (KB)***	***Responsivenes s (ms)***
Triple DES encryption algorithm	12.938	87.684	3.599	12.910	90.637	3.421
Hash-based secret key encryption algorithm	10.941	89.852	4.225	10.911	90.480	7.943
Certificate less signature scheme	8.947	90.461	3.605	8.911	90.527	14.184
Checkpoint-enabled scalable Blockchain architecture	6.883	89.793	4.405	6.856	91.211	15.294
Hybrid access control enabled consensus algorithm	4.883	90.164	4.205	4.856	90.039	16.914
Trust ensemble hybrid consensus algorithm	**0.856**	**87.684**	**3.599**	**0.878**	**90.637**	**3.421**

Table 1. Comparison with different algorithm of Databse1

Methods	**Database 2**					
	Block size			**User**		
	Transaction time (ms)	***Memory usage (KB)***	***Responsivenes s (ms)***	***Transaction time (ms)***	***Memory usage (KB)***	***Responsivenes s (ms)***
Triple DES encryption algorithm	12.934	88.305	3.179	12.908	90.227	3.913
Hash-based secret key encryption algorithm	10.934	90.207	3.599	10.907	90.117	6.750
Certificate less signature scheme	8.948	90.859	2.887	8.909	91.188	13.620
Checkpoint-enabled scalable Blockchain architecture	6.883	89.887	3.313	6.856	90.648	13.667
Hybrid access control enabled consensus algorithm	4.883	90.141	3.551	4.905	90.684	17.662
Trust ensemble hybrid consensus algorithm	**0.862**	**88.305**	**3.179**	**0.880**	**90.227**	**3.913**

Table 2. Comparison with different algorithm of Databse2

Conclusion

An IoT device integration supply chain solution based on blockchain is not reliant on reliable middlemen since it uses a different method to build trust between parties to transactions. A supply chain can be managed, tracked, and traced using a system like this. As a result, information can be safely

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8484
***Article Received:** 27 July 2023 **Revised:** 18 September 2023 **Accepted:** 02 October 2023*

transmitted between parties that might not have trusted each other's data otherwise. Portable IoT devices provide a hurdle assuming that processing blockchains unavoidably takes a lot of CPU resources. An accessible and traceable system utilizing blockchain systems is promoted by the trust enable hybrid consensus algorithm that is developed in this research. With the help of the proposed model, storage, transaction time, and responsiveness can be decreased. The outcomes of our simulation demonstrate that, in comparison to conventional consensus methods, the suggested model is both secure and effective. The improved efficiency of the proposed model in terms of transaction time, memory usage, and responsiveness is 82.48 %, 0.08 %, and 5.99 % depending on the block size. Future research will focus on investigating the IoT supply chain system's trust model using actual data.

REFERENCES

[1] Al-Rakhami, Mabrook S., and Majed Al-Mashari. "ProChain: Provenance-Aware Traceability Framework for IoT-Based Supply Chain Systems." IEEE Access 10 (2021): 3631-3642.

[2] Bhutta, Muhammad Nasir Mumtaz, and Muneer Ahmad. "Secure identification, traceability and real-time tracking of agricultural food supply during transportation using internet of things." IEEE Access 9 (2021): 65660-65675.

[3] Alkhader, Walaa, Khaled Salah, Andrei Sleptchenko, Raja Jayaraman, Ibrar Yaqoob, and Mohammed Omar. "Blockchain-Based Decentralized Digital Manufacturing and Supply for COVID-19 Medical Devices and Supplies." Ieee Access 9 (2021): 137923-137940.

[4] Cui, Pinchen, Julie Dixon, Ujjwal Guin, and Daniel Dimase. "A blockchain-based framework for supply chain provenance." IEEE Access 7 (2019): 157113-157125.

[5] 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.

[6] Subramanian, Ganesan, Anand Sreekantan Thampy, Nnamdi Valbosco Ugwuoke, and Baghwan Ramnani. "Crypto pharmacy–digital medicine: A mobile application integrated with hybrid blockchain to tackle the issues in pharma supply chain." IEEE Open Journal of the Computer Society 2 (2021): 26-37.

[7] Benčić, Federico Matteo, Pavle Skočir, and Ivana Podnar Žarko. "DL-Tags: DLT and smart tags for decentralized, privacy-preserving, and verifiable supply chain management." IEEE access 7 (2019): 46198-46209.

[8] Jangirala, Srinivas, Ashok Kumar Das, and Athanasios V. Vasilakos. "Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment." IEEE Transactions on Industrial Informatics 16, no. 11 (2019): 7081-7093.

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

[10] 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.

[11] 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.

[12] 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.

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

[14] 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.

[15] Malik, S., Dedeoglu, V., Kanhere, S.S. and Jurdak, R., 2019, July. Trustchain: Trust management in blockchain and iot supported supply chains. In 2019 IEEE International Conference on Blockchain (Blockchain) (pp. 184-193). IEEE.

[16] Das, A. and Islam, M.M., 2011. SecuredTrust: a dynamic trust computation model for secured communication in multiagent systems. IEEE transactions on dependable and secure computing, 9(2), pp.261-274.

[17] Madumidha, S., Ranjani, P.S., Vandhana, U. and Venmuhilan, B., 2019, May. A theoretical implementation: Agriculture-food supply chain management using blockchain technology. In 2019 TEQIP III Sponsored International Conference on Microwave Integrated Circuits, Photonics and Wireless Networks (IMICPW) (pp. 174-178). IEEE.

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

[19] Coppersmith, D., Johnson, D.B. and Matyas, S.M., 1996. A proposed mode for triple-DES encryption. IBM Journal of Research and Development, 40(2), pp.253-262.

[20] Cheddad, A., Condell, J., Curran, K. and McKevitt, P., 2010. A hash-based image encryption algorithm. Optics communications, 283(6), pp.879-893.

[21] Yap, W.S., Heng, S.H. and Goi, B.M., 2006, August. An efficient certificateless signature scheme. In International Conference on Embedded and Ubiquitous Computing (pp. 322-331). Springer, Berlin, Heidelberg.

[22] Javaid, U. and Sikdar, B., 2020. A checkpoint enabled scalable blockchain architecture for industrial internet of things. IEEE Transactions on Industrial Informatics, 17(11), pp.7679-7687.

[23] Bera, B., Das, A.K., Obaidat, M.S., Vijayakumar, P., Hsiao, K.F. and Park, Y., 2020. AI-enabled blockchain-based access control

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8484
***Article Received:** 27 July 2023 **Revised:** 18 September 2023 **Accepted:** 02 October 2023*

for malicious attacks detection and mitigation in IoE. IEEE Consumer Electronics Magazine, 10(5), pp.82-92.

[24] N. Shahid and S. Aneja, "Internet of things: Vision, application areasand research challenges," in I-SMAC (IoT in Social, Mobile, Analytics 2017,pp. 583–587.

[25] Abou-Nassar EM, Iliyasu AM, El-Kafrawy PM, Song O-Y, BashirAK, Abd El-Latif AA (2020) Ditrust chain: towards blockchainbasedtrust models for sustainable healthcare iot systems. IEEEAccess 8:111223–111238

[26] Malik S, Dedeoglu V, Kanhere SS, Jurdak R (2019) TrustChain:management in blockchain and IoT supported supply hains. In: 2019 IEEE international conference on blockchain IEEE, pp 184–193

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

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

[33] 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

[34] 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

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

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

[37] Vadgama, Nikhil, and Paolo Tasca. "An Analysis of BC adoption in supply chains between 2010 and 2020." Frontiers in BC 4 (2021):1247-1259.