Research on Optimization and Risk Control of E-commerce Supply Chain Logistics Management Mode Based on the Internet of Things and Blockchain Technology

Chen Jun
Xi’an Aeronautical University

Jiang Lan (✉ 201903006@xaau.edu.cn )
Xi’an Aeronautical University

Research Article

Keywords: E-commerce, Supply Chain Logistics, Internet of Things, Blockchain, Improved Logistic Advanced Encryption Standard (ILAES), Proof of Logistic Information Share (PoLIS)

Posted Date: August 7th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-3202446/v1

License: ☐① This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License
Abstract

To maintain their position as market leaders in the dynamic business climate, e-commerce businesses must successfully improve their supply chains and logistical processes. Due to complex networks, a lack of information transparency and traceability, and security risks, the information flow management in traditional logistics supply chains using centralized databases is now facing several difficulties. By combining the Internet of Things (IoT) and Blockchain Technology (BT), it may be possible to collect information intelligently, store it decentralized, and allow for reliable, cost-effective information flow. Even while IoT-integrated blockchain-based systems offer sufficient benefits across industries, e-commerce supply chain logistics management has so far had a very low acceptance rate. Therefore, in this research, we suggested an IoT-integrated Blockchain approach for improving information security and traceability in the logistics of the e-commerce supply chain. Utilizing an IoT monitoring module, the data is gathered and processed by a smart contract before being entered into a blockchain. ILAES, an improved logistic advanced encryption method, is used to encrypt the data and generate a new data block. The Proof of Logistic Information Share (PoLIS) consensus mechanism is used to validate the data block before it is uploaded to the blockchain. Throughput, block execution time, encryption time, and avalanche impact are used to assess the proposed system's performance. The findings demonstrated how well the suggested solution improved the security and openness of logistical information.

I. INTRODUCTION

E-commerce was once a strange idea, but now it has got to be a viable replacement trade. E-commerce is becoming a more sustainable practice for several global customers. Now, e-commerce is rising due to greater internet connectivity, but there are also other considerations. Some of these include the growing number of purchasers utilizing mobile devices such as phones as well as the fact that most e-commerce transactions are cheap. Those factors are vital since they shape contemporary e-commerce. Customers could now shop freely and send or receive products in any manner customers like. Every other marketing strategy fails. They may explore some quantitative e-commerce market measures. The proportion of businesses with e-sales climbed by 7%, while e-sales revenue increased by 6%. Sadly, the share of e-sales varies greatly across nations, as does the number of e-sales firms and their revenue [Dragomirov (1)]. To keep up with the rapid expansion of e-commerce, companies must look for new ways to handle as well as organize the whole system. Figure 1 shows the logistics management in e-commerce.

Customers who are looking for specific products or services can immediately find people using on-site search, but also collects valuable information about what customers want or their feelings towards specific items, all of which can be used to customize the offer to each particular consumer. E-commerce platform operations such as plan, purchase, as well as distribution, are impacted by an incorporated methodology, which has a strategic and organizational influence on supply chain management (SCM). With regards to SCM, a wide variety of information is included [Yalan and Wei (2)]. The Internet of Things (IoT) is a grouping of technology that links and organize several approximate objects. The notion of IoT-based E-commerce has emerged as a promising trade system that accomplishes person-to-machine
[P2M] or perhaps even machine-to-machine [M2M] purchases instead of a person-to-person [P2P] money transfers. For instance, Amazon Dash seems to be each purchase of an item. It is a classic example of expanding P2P to P2M E-commerce. So it’s possible to conceive E-future commerce in which all stages of payments are performed independently via M2M [Liu et al. (3)]. Blockchains also developed as technological breakthroughs that will alter various industries and sectors, mainly to the continual growth of network security technology. A blockchain is a technology that is shared and secured across such a distributed system. Increasing development of blockchain technology in e-commerce is eagerly expected; unfortunately, due to basic availability and performance difficulties in major blockchains such as Digital currencies, their application remains unclear [Lim et al. (4)]. Bridge e-commerce has seen enormous expansion in recent years, due to economical globalization and the emergence of the internet. Collaborations amongst partners in the cross-border supply chain for bridge e-commerce trading with delivery requests. Building relationships between supply chain network members is becoming increasingly important. The trust issue cannot be easily managed due to personal, legal, and ideological variations within nations. The connectivity of blockchain technology with supply chain management seems to have some unresolved challenges. Inside a distributed blockchain network, obtaining product specifications traceable necessitates unique scalability, which necessitates industry experience in supply chain management [Liu (5)]. Hence, we proposed IoT integrated Blockchain technique for optimizing information traceability and security in e-commerce supply chain logistics. In this paper, we augment the security and traceability of the logistics transactions in IoT-blockchain networks using the ILAES encryption technique and PoLIS consensus algorithm to optimize the information traceability and reduce security risks. The remaining sections in the paper are structured as follows. The associated literature and the problem statement are presented in Section II. The explanations of the proposed work are provided in Section III. Section IV has results and discussions. The proposed paper’s conclusion is presented in section V.

II. REVIEW OF LITERATURE

[Daneshvarkakhki and Gargeya (6)] offer to conduct thorough data analysis on supply chain and information systems (SCIS) to classify existing research fields. [Wang et al. (7)] selects the organization of the e-commerce supply chain, in which the e-commerce network controls and offers services and products and actual insurance services. [Awwad et al. (8)] focused on the initial adoption of blockchain technology combined with IoT, with a focus on the degrees of adoption of blockchain technology enabling verification, and visibility, including tracing in diverse sectors, including e-commerce, healthcare, or logistics. [Pei and Yan (9)] examined a distributor supply chain in which the e-tailer provides complete payment terms to its customers that both the suppliers as well as the e-tailer use their own associated with technology growth of online marketing. [Ellram and Murfield (10)] examined traditional supply chain management materials released in industrial marketing management to see how the industry has changed because they were released.

[Chen et al. (11)] offers to use JD.com, one of China's major e-commerce sites, as a case study to show how an online company improves its comparative benefit by using distribution network finance strategies
to speed supply chain teamwork. [Dutta et al. (12)] analyzed all advanced work done in the area linked with the usage of blockchain connectivity in Supply chain operations within that research, which includes 178 documents. [Ravi et al. (13)] states that the purpose of Block chain’s capabilities is to enhance supply chain management practices. The research also contains a technique for implementing the proposed notion with Hyperledger Fabric, a blockchain network system. [Zhang et al. (14)] focused on the dual global supply chain with several competitive producers, distributors, as well as demanding marketplaces. Most of these disorders have numerous odontogenic keratocysts. Several odontogenic keratocysts were found in three-years female teenagers. During the study, no further anomalies were detected [Mody and Bhoosreddy (15)]. [Garg and Harita (16)] personalized healthcare uses perfectly alright data to identify specific deviations from the norm. Using ‘Virtual Twins’ within a design, such emerging information health care systems were ethically and ethically examined. Phenomena were digitally linked and shown on the whole of a continuous basis. Moral differences can be discerned obtained from data forms & perceptions. Virtual twins’ social and ethical ramifications are investigated. Information has become increasingly important in the healthcare system. Since it provides practical ways for increasing equality and fairness, this strategy has the potential to become a societal equalizer. Hypersensitivity is a lengthy worldwide epidemic, among often the recommended therapies in Taiwanese medical centers are traditional Chinese or China drugs. Hay fever was the most common chronic condition treated by ambulatory traditional Chinese medicine. In Taiwan, allergic sinusitis is managed with a variety of old Chinese medicine and modern medications [Ahmed et al. (17)]. HDR brachytherapy has been used to reduce radiation and allow outpatient treatment and quicker testing timeframes. By adjusting the latency at each dwell site, a human generator could improve dosage dispersal even more. Because of the short treatment periods, no data validation is possible, and errors can cause harm to people, HDR brachytherapy therapies should be performed accurately [Shahabaz and Afzal (18)]. [Li and Zihan (19)] presented a treatment technique and equipment for residential wastewater to improve rural communities. Zamfara, Nigeria, hydrophilic and organophosphate insecticides were found in soil samples collected from chosen vegetable farms. Focus on three main using GC-MS was used to assess the testing regime and outcomes [Salihu and Zayyanulyya (20)].

**Problem Statement**

In SCM, the main risks encountered by e-commerce logistics in the IoT context are information safety risks, distribution risks, and reputation risks [Chang et al. (23)]. Conventional consensus protocols have high latency, limited throughput, and poor scalability, notwithstanding their benefits. Hence, a novel block validation consensus protocol is required in an IoT-blockchain network in e-commerce supply chain logistic management (SCLM).

**III. PROPOSED WORK**

The major emphasis of this study is to minimize the information security risks and enhance information traceability in the e-commerce supply chain logistics. The manufacturer, wholesaler, and retailer in the SCLM system integrate dynamic IoT technology to provide comprehensive details namely quality,
quantity, cost, and time of receiving. The data acquired by the IoT monitoring module is sent to the blockchain for storage. The smart contract module including functions namely get_supply_data(), get_manufacture_data(), get_wholesale_data(), get_retail_data(), and get_customer_data() is employed to activate data processing in blockchain. The data is encrypted using ILAES before storage in the blockchain. The block is created and validated using the PoLIS consensus algorithm and added to the blockchain. Figure 2 provides the overall flow of the proposed work.

a) IoT monitoring module

The E-commerce supply chain logistics system is comprised of raw material suppliers, manufacturers, retailers, and consumers. IoT monitoring module is present at the warehouses in the manufacturing site and retailer site. The IoT module is made up of a variety of data collection devices, including Radio Frequency Identification (RFID), GPS, sensors, and the networks that connect them. One of the most recent technological advancements in SCLM is the IoT. IoT is an infrastructure that allows items such as automobiles and building structures to gather and share data. An RFID scanner reads or writes data held in so-called RFID tags using radio waves, which is a means for automatically identifying items. Figure 3 illustrates the overall framework of SCLM using IoT and BT.

i) When the product manufacturing site places a purchase order to the raw material supplier through e-commerce websites, the supplier takes the order. Each package of raw materials will be tagged with an RFID tag with a unique code after packing is complete. The raw materials are transported to the manufacturer by transport trucks once the firm has paid the supplier. Transport trucks and warehouses are equipped with RFID readers. It will be immediately recognized when the RFID-tagged items arrive in the storage channel (material ID, material quantity, and price). There is a lot of labor saved and inventory consistency is improved by employing label information to finish the warehouse operation.

ii) Each package of manufactured items will be marked with a unique RFID tag with a code at the end of manufacturing by the producer. When the wholesaler places a purchase order to the manufacturer through e-commerce websites, the manufacturer takes the order. After payment is done by the wholesaler, the manufacturer sends the products to the wholesaler through transport vehicles. As soon as RFID-tagged items arrive at the wholesaler site, the warehouse's RFID readers will instantly recognize and locate the products' RFID tags (product ID, product quantity, and price). A similar process takes place between wholesalers and retailers.

c) Smart Contract module

In a smart contract, built-in software is used to automatically perform activities when specified conditions occur. A smart contract may be thought of as a computer program that can operate on its own in a blockchain. The smart contract is triggered and automatically performed when the requirements defined by the program are satisfied, accomplishing several tasks including data processing and management. The functions involved in the smart contract module in SCLM are described below.
The raw material provider node calls get_Supply_data() to record the material ID and description in the blockchain.

Get_Manufacturing_data(): Each box of goods has a unique product ID, as well as information about its manufacturer, supplier, and manufacturing date and batch. The Get_Manufacturing_data() method is executed by the product manufacturer node and is capable of publishing this information into the blockchain.

Get_Wholesale_data(): It is the product wholesaler node's responsibility to use Get Wholesale data() to save product IDs, product specifics, manufacturer details, wholesaler details, and purchase details on the blockchain.

Get_Retail_data(): It is triggered by retail shop nodes. After the box of products is acquired by retailers the system retrieves the unique number of each box of items and records the purchasing time, location, cost, and other information into the blockchain.

Get_consumer_data(): It is the consumer node that calls this function to scan the QR code on the packing box of items using a Smartphone to receive all the product details.

c) Data Encryption using Improved Logistic Advanced Encryption Standard (ILAES)

Other firms or node owners can get data from the consortium blockchain while it is being sent and stored by each member node. When it comes to the same kind of products, producers A and B would naturally like to keep their source, destination, and other business information private. This is the case with them both being in the same industry. Data encryption with ILAES is used to protect the confidentiality of network transactions to address the problem of data privacy. To ensure that only the people involved in the transaction can access the information, each box of goods is encrypted with a suitable key using ILAES.

There are two sets of 256-bit data and keys in ILAES. It's a symmetric block cipher, so that's why it's called that. To encrypt and decrypt data, both the sender and the recipient must use the same key. Bytes are processed in this method, and the cipher text that is generated is the result of this process. Figure 4 provides the steps involved in ILAES encryption. It consists of sixteen rounds of byte processing. The bytes in the data are mapped logistically into a state array. In each round, different functions are used to modify the bytes in the product/material data. The different functions used in ILAES are Sub_Bytes(), Shift_Row(), Mix_Column(), and Add_Round_key(). But in the last round of ILAES, all functions except Mix_Column() are executed.

i) Sub_Bytes()

Sub_Bytes() implements the substitution process in the state array. A 16 by 16 matrix of bytes known as an S-box is all that is required for its output. Each byte of the state array is translated into a new array by substituting its actual bytes with other new bytes.
ii) Shift_Row()

Shift Row() function executes the cyclic shifting of rows. The moving of rows in this manner is done in a clockwise direction to the left. When a row is shifted, it is shifted by one byte, two bytes, and so on, depending on the number of rows that have been shifted. The first row will not be altered in any way. To make the system more secure, this transformation is usually performed on the matrix, which is composed of rows and columns.

iii) Mix_Column()

Most of the time, this process is done one column at a time. It is at this stage that all four bytes of each column are combined to produce a new value for each byte in the column. This transformation may be defined by multiplying the State array's matrices together. As a consequence, the total of the products of the values in each row and column is equal to the value of each element in the product matrix.

iv) Add_Round_Key()

The state is bitwise XORed with the 128-bit round key in this example. Column-wise operation is used here, although byte-level action may be conducted between the four bytes of the status column and a single word of the round key.

The encrypted logistic information at each node in the supply chain is sent for block creation. In the end, the members of the IoT-blockchain network will be distributed with the encrypted key. When a member of supply chain logistics requires details regarding the product, the member can use the ILAES symmetric key to decrypt the data into original data. The decryption process using ILAES is similar to the ILAES encryption process but the functions used in decryption are inverse to the encryption functions. The functions used in ILAES decryption are Inv_Sub_Bytes(), Inv_Shift_Row(), Inv_Mix_Column(), and Inv_Add_Round_Key(). Inv_Sub_Bytes() applied inverse S-box lookup table for inverse substitution. Using Inv_Shift_Row(), rows are cyclically moved to the right, making this transformation the inverse of the forward shift row transformation. Even in this case, the first row remains unchanged, the second row is moved one byte to the right, the third row is moved two bytes to the right, the fourth row is moved three bytes to the right, and so on. The amount of shifting that occurs depends on the matrix that is being used. To multiply the whole state array by a pre-defined matrix, known as the inverse polynomial matrix, the Inv_Mix_Column() is used. Inv_Add_Round_Key() used the XOR technique between the cipher text and the extended key that corresponds to that specific iteration. The sixteen rounds of the decryption process using ILAES convert the cipher text into plain text which can be read by the requested member of supply chain logistics.

d) Block Validation using PoLIS protocol

The encrypted logistics information is stored in the new block. Data recordings known as blocks are connected and safeguarded in the blockchain, a peer-to-peer decentralized or distributed database. All nodes in the decentralized network are notified of new data that has been added to the block. Blocks in
the blockchain include two components, known as header blocks and transaction sections. The nonce, timestamp, hash value of the block to which it is previously linked, and version are usually included in the block header.

After data block creation, the PoLIS consensus protocol is employed in this work to validate the newly created data block. The pseudocode of PoLIS is provided in algorithm 1. The steps involved in block validation using PoLIS are as follows. Initially, the honest or trusted nodes are selected for block validation based on the honest index. The honest index for each node participating in the data validation process is calculated. To participate in block validation, a node must have an honest index that is larger than or equal to the allocated threshold index. Otherwise, the node will be excluded from the block validation process, which is used to sort out fraudulent nodes. Thus the honest nodes for block validation are selected. Then the transaction to be validated is sent to these selected honest nodes. The selected honest nodes crosscheck the transactions and provide votes. The vote is assigned one if it is correct or zero if it is incorrect. The total correct votes are counted for each transaction. Following this, adaptive weight is determined for each transaction depending on the total correct votes. If the transaction's adaptive weight is greater than the assigned threshold weight, then the transaction is valid and added to the existing blockchain. If the transaction's adaptive weight is lesser than the assigned threshold weight, then the transaction is invalid and not added to the existing blockchain. Thus the valid transactions are attached to the overall blockchain.

**Algorithm 1** Proof of Logistic Information Share (PoLIS) protocol

Initialize the nodes \((g_1, g_2, \ldots, g_n)\) for validation of the new block

Assume the threshold value of the honest index as \(HI_{Th}\) and of the transaction's adaptive weight as \(AW_{Th}\)

For each validating node \((g_i)\)

Determine the Honest_Index

If Honest_Index \(\geq HI_{Th}\)

Allow \(g_i\) in block validation

Else

Reject \(g_i\)

Assume each transaction's adaptive weight to 0

Let the transactions arrive be \((T_1, T_2, \ldots, T_j)\)

Count the votings for each transaction
Determine the adaptive weight of transaction depending on valid miner’s vote

If the transaction’s adaptive weight after voting > \( AW_{Th} \)

The transaction is valid

Else

The transaction is invalid

Determine each miner’s lost weight ratio (LWR)

\[
LWR = 1 - \left( \frac{\text{NumberOfCorrectVotes}}{\text{TotalNumberOfVotes}} \right)
\]

Update miner’s honest index depending on LWR

**IV. RESULTS AND DISCUSSION**

The efficiency of implementation of the IoT-blockchain technologies for logistic information traceability, and for shaping the e-commerce business is studied in this paper. To minimize the information security risks and optimize information traceability, a novel encryption technique (ILAES) and novel consensus algorithm (PoLIS) have been proposed in this research work.

**a) Performance of Consensus algorithm in IoT-Blockchain system for SCLM**

The performance of the proposed consensus algorithm is compared to existing consensus algorithms in terms of throughput, latency, and energy consumption.

**i) Throughput**

The quantity of logistical information transactions performed per unit time by several consensus nodes is referred to as “throughput.” In the blockchain space, transaction throughput refers to the rate of how fast a blockchain processes transactions. It is measured by transactions per second (TPS). Figure 5 depicts the comparative analysis of throughput of the proposed consensus algorithm in IoT-Blockchain-based SCLM. Throughput of PoLIS was higher than that of existing consensus techniques namely Improved Practical Byzantine Fault Tolerance (IPBFT), Scalable hierarchical Byzantine Fault Tolerance (SHBFT), PoS-PBFT (Proof of Stake-PBFT). This shows that PoLIS efficiently validates and stores the information gained with e-commerce supply chain logistics in the blockchain.

**ii) Latency**

Using latency as a measure of system performance and assessing communication and algorithm delays between distributed system nodes is critical. Systems with low latency may promptly process the
transactions and provide an excellent user experience, while a system with high latency cannot effectively process the transaction in time. A distributed system’s latency generally consists of three parts: the time necessary to create a block, the time required to validate a block, and the time required to process and add a block to the system. A comparison of latency of the proposed consensus mechanism in SCLM based on IoT-Blockchain is shown in Fig. 6. IoT-Blockchain with PoLIS has low latency compared to existing methods such as PoS-PBFT and CoC (supply chain on the blockchain), “a supply chain management system based on a hybrid decentralized ledger with a novel two-step block construction mechanism”. This shows that PoLIS quickly validates the logistic transactions compared to existing methods.

iii) Energy Consumption

The amount of energy consumed by a blockchain during block validation and addition is known as energy consumption. Figure 7 illustrates that energy consumed during the validation and addition of logistics data blocks by IoT-Blockchain with PoLIS is lesser than that of conventional methods such as Proof-of-work (PoW), Proof-of-Authentication (PoAh), and PoS. This indicated that IoT-Blockchain with PoLIS is energy efficient.

b) Performance of encryption algorithm in IoT-Blockchain system for SCLM

The performance of the encryption algorithm is compared to conventional encryption algorithms such as optimal Blowfish, AES, and RSA (Rivest, Shamir, and Adleman encryption) in terms of encryption time, and decryption time, and security level.

a) Encryption Time

The time consumed by the encryption algorithm to convert plaintext into cipher text is referred to as the encryption time. An encryption scheme’s throughput is determined by the amount of time it takes to encrypt the logistics data. It tells you how fast the encryption process is. Figure 8 depicts the comparative analysis of the encryption time of the proposed encryption algorithm (ILAES) in the IoT-Blockchain system in SCLM. The encryption time of ILAES is lower than that of existing methods namely optimal blowfish, AES, and RSA. This shows that ILAES encrypts the logistics data fastly.

ii) Decryption Time

The time consumed by the cryptographic algorithm to convert a cipher text into plain text is referred to as the decryption time. Figure 9 depicts the comparative analysis of the decryption time of the proposed encryption algorithm (ILAES) in the IoT-Blockchain system in SCLM. The decryption time of ILAES is lower than that of existing methods namely optimal blowfish, AES, and RSA. This shows that ILAES decrypts the logistics data quickly when any member of SCLM requests logistics information in e-commerce.

iii) Security level
The security level of a cryptographic cipher or hash function is a measure of its strength in cryptography. Figure 10 shows the comparative analysis of the security level of the proposed encryption techniques. It shows that the security level of ILAES is higher than that of optimal blowfish, AES, and RSA. ILAES efficiently preserves the confidentiality, privacy, and integrity of logistics data in SCLM.

Discussion

As the market and technology have evolved, the conventional way of manually documenting financial data has fallen behind. In this paper, we suggested IoT-Blockchain for system dependability, traceability efficiency, and improving security and reliability of information traceability in the distributed supply chain network, by using the benefits of blockchain technology. These improvements are critical for fostering a favorable environment in e-commerce firms. Typically, logistics has been seen as a costly, but absolutely important component of any company's operations. Inventory management in the e-commerce supply chain has been made easier because of the combination of smart sensing equipment and the Internet. E-commerce enterprises may better monitor and manage their logistics systems with an IoT and BT-enabled SCLM in place. It is possible to monitor and share the flow of e-commerce supplies, as well as evaluate, predict, and store product information at every level of the supply chain in a decentralized database. It is possible to track and monitor the full product life cycle using IoT, which offers an efficient information technology support platform. Using IoT and BT, the closed-loop SCLM system can incorporate real-time tracking and monitoring of the supply chain's production, distribution (including retail and recycling), as well as information transparency, and allow the e-commerce supply chain to interact quickly with market demand.

We employed ILAES for data encryption and a novel PoLIS consensus protocol for block validation. Along with the capacity to track goods, CoC can help with numerous supply chain management activities, like international trade compliance, bill of lading, and clearing customs [Gao et al. (25)]. However, its performance in a production context is less effective. Energy-intensive, expensive, and requires a lot of computer power, PoW is not apt for blockchain. In the event of an assault, the network might be taken over by rogue miners, rendering decentralization ineffective [Sedlmeir et al. (26)]. There is limited scalability and low throughput in the POS and PBFT algorithms [Zhang et al. (28), Wu et al. (24)]. As a result of the huge numbers involved, RSA has a sluggish data transmission rate. Sometimes a third party is required to validate the trustworthiness of public keys [Xiong et al. (31)]. However, [Gangireddy et al. (29)] did not use smart contracts in blockchain to improve the correctness of cyber security for all confidential information. The proposed system enhanced the transparency of information, and data processing enhanced security and also reduced data duplication.

V. CONCLUSION

IoT and blockchain integration has been a remarkable advancement in both industries. The Internet of Things may benefit from the decentralization, security, traceability, and transparency attributes of blockchains. For IoT applications, standard BT is not a viable choice due to insufficient resource control.
If blockchain is to be employed in IoT applications, the consensus algorithms, which consume the most energy, must be streamlined. To save energy and speed up the consensus process in blockchains used for e-commerce, we have suggested a revolutionary consensus algorithm (PoLIS). By ensuring confidentiality, traceability, and transparency, blockchain plus IoT may provide an intelligent solution for e-commerce logistics. We measured the blockchain-based IoT application's throughput, latency, and energy use. Comparing the proposed method to prior Blockchain systems, throughput is increased while latency and energy consumption are decreased. It will be necessary to assess the efficacy of additional procedures afterwards, such as quality management in SCLM. In the future, users will be able to make educated judgments because of the users' storage of IoT sensor data on a blockchain.

Declarations

Conflict of Interests
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Consent to Participate: Informed consent was obtained from all individual participants included in the study.

Consent to Publish: The participant has consented to the submission in this Journal.

Data Availability Statement
The data used to support the findings of this study are available from the corresponding author upon request.

Ethical approval: This article does not contain any studies with human participants or animals performed by any of the authors.

Fund statement
There is no funding for this research.

Author's contributions: Chen Jun and Jiang Lan contributed to the design and methodology of this study, the assessment of the outcomes and the writing of the manuscript.

References


18. Shahabaz A, Afzal M (2021) "Implementation of High Dose Rate Brachytherapy in Cancer Treatment, SPR, Volume 1, issue, 3, Page No.: 77–106." DOI: https://doi.org/10 52152
19. Li Z (2022) "Treatment and Technology of Domestic Sewage for Improvement of Rural Environment in China-Jiangsu: A Research."
20. Salihu SO (2022) and Zayyanulya. "Assessment of Physicochemical parameters and Organochlorine pesticide residues in selected vegetable farmlands soil in Zamfara State, Nigeria." Science Progress and Research (SPR) 2.2

Figures
Figure 1

E-commerce logistics management
Figure 2

Flow of the proposed work
Figure 3

Overall framework of e-commerce supply chain logistics management using IoT-blockchain
Figure 4

Flow of ILAES encryption
Figure 5

Number of nodes versus Throughput
Figure 6

Number of nodes versus latency
Figure 7

Energy consumption of different consensus algorithms
Figure 8

File size versus encryption time
Figure 9

File size versus decryption time
Figure 10

File size versus security level