An innovative blockchain-based secured logistics management architecture: utilizing an RSA asymmetric encryption method

mathematics

MDPI

Article

An Innovative Blockchain-Based Secured Logistics Management Architecture: Utilizing an RSA Asymmetric Encryption Method

Nwosu Anthony Ugochukwu [1], S. B. Goyal [1], Anand Singh Rajawat [2], Sardar M. N. Islam [3], Jiao He [4,*] and Muhammad Aslam [5,6]

[1] The Faculty of Information Technology, City University, Petaling Jaya 46100, Malaysia
[2] School of Computer Sciences and Engineering, Sandip University, Nashik 422213, India
[3] Institute for Sustainable Industries & Livable Cities, Victoria University, Melbourne 14428, Australia
[4] School of International Business and Management, Sichuan International Studies University, Chongqing 400031, China
[5] School of Computing Engineering and Physical Sciences, University of West of Scotland, Blantyre, Glasgow G72 0LH, UK
[6] Scotland Academy, Wuxi Taihu University, Wuxi 214063, China
* Correspondence: hejiao@drhj.net.cn

Abstract: ***Purpose:*** The recent development in logistics due to the dawn of Logistics 4.0 has made global logistics providers more dependent on intelligent technologies. In this era, these technologies assist in data collection and transmission of logistical data and pose many security and privacy threats in logistics management systems. The customer's private information, which is shared among the logistics stakeholders for optimal operation, faces unauthorized access due to a lack of privacy. This, amongst others, is a critical problem that needs to be addressed with blockchain. Blockchain is a disruptive technology that is transforming different sectors, and it has the potential to provide a solution to the issues mentioned above, with its unique features such as immutability, transparency, and anonymity. ***Method:*** This study designed a blockchain-based logistics management architecture on a decentralized peer-2-peer network using Ethereum smart contracts. The proposed system deployed the Rivest–Shamir–Adleman (RSA) asymmetric encryption method to protect the logistics system from cyber-attacks and secure customers' private information from unauthorized access. ***Findings:*** Furthermore, the security and privacy of the proposed system are evaluated based on the theorem. The proof shows that the system can provide security to the logistics system and privacy to customers' private data. The performance evaluation is based on throughput and latency. It shows that the proposed system is better than the baseline system, and the comparatives analysis shows that the proposed system is more secure and efficient than the existing systems. ***Implication and Limitation:*** The proposed system offers a better solution to the security/privacy of the logistics management system and provides recommendations to key stakeholders involved in the logistics industry while adopting blockchain technology. Apart from the study's methodological limitation, it is also limited by a lack of reference materials.

Keywords: blockchain; algorithm; Ethereum; smart contract; smart logistic system; information security; privacy

MSC: 68U99

1. Introduction

1.1. Problem Contexts

The recent development in smart technologies has brought meaningful transformation to different sectors such as healthcare, smart cities, automotive, manufacturing, and logistics domains. These smart technologies, which consist of cloud computing, the Internet of

check for updates

Citation: Ugochukwu, N.A.; Goyal, S.B.; Rajawat, A.S.; Islam, S.M.N.; He, J.; Aslam, M. An Innovative Blockchain-Based Secured Logistics Management Architecture: Utilizing an RSA Asymmetric Encryption Method. *Mathematics* **2022**, *10*, 4670. https://doi.org/10.3390/math10244670

Academic Editors: Andrej Brodnik and Frank Werner

Received: 1 November 2022
Accepted: 6 December 2022
Published: 9 December 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Things (IoT), artificial intelligence (AI), and others, have not only digitalized the logistics system in terms of efficient handling of large data associated with logistics, rather they pose some security threats to logistics systems. Most smart logistics systems are vulnerable to cyberattacks, particularly one-point-of-failure assaults, due to their centralized database systems [1]. Because of this flaw, logistics systems can easily be compromised via these technologies, and sensitive data can be stolen. Logistics is a networking activity that involves procuring, storing, and conveying goods from the point of production to the end users. It also entails sharing information among the logistics stakeholders [2]. This information, which consists of customers' private details (customers' names, mobile numbers, addresses, and credit cards), lacks privacy and faces unauthorized disclosure among these global logistics partners. The lack of proper verification procedures among these global logistics partners (suppliers, transporters, manufacturers, and customers) is a serious security threat [3]. This can lead to the transmission of unauthenticated or unverifiable information from these logistics partners, which can lead to a breach in the security of the logistics system and jeopardize the integrity of the logistics data. Blockchain, a disruptive technology, will be deployed to address this security problem. However, this study asks the following questions.

RQ1—What are the sources of attack challenging the security of smart logistics systems?

RQ2—How does Blockchain technology provide security to smart logistics systems and privacy for customers' private information?

RQ3—How can Blockchain technology be implemented in a logistics management system?

1.2. Motivation

Security is a fundamental problem in every organization, and the logistics sector is not left out. The survival of any organization depends on how secure its system is and its customers' information security. Sometimes, the organization focuses more on protecting its system against external forces and undermining the potential threat of internal force. Most of the threats in the logistics system might be internally motivated. Therefore, this study will deploy a blockchain-based architecture that is efficient, fast, and secure [4] to address the aforementioned problem.

1.3. Contributions of This Study

The main contributions of this study are as follows:

i. This study identified the kinds of cyber-attacks challenging smart logistics systems.

ii. A blockchain-based secured and efficient logistics management system architecture on a peer-to-peer decentralized network was proposed to secure and enhance the efficiency of the logistics management system.

iii. iAn innovative asymmetric RSA encryption method was deployed to enhance the security of the logistics system and provide privacy to customers' private information.

iv. blockchain-based algorithms with specified smart contracts utilizing the Ethereum platform were proposed and implemented to address security issues and enhance the efficiency of the logistics system.

v. Finally, security and privacy analyses were done to assess the security of the logistics system and the privacy of customers' data. The latency and throughput of the proposed system were compared with a baseline system.

1.4. Paper Organization

The remaining part of this study article is organized as follows: Section 2 concentrates on a literature review and related works and limitations of the previous works. Section 3 focuses on the overview of the smart logistics system, the cyber-attack challenges of the smart logistics system, the security mechanism of blockchain, and the rationale for using RSA over the ECC encryption method. Section 4 presents the proposed methodology, the proposed system architecture, the specified smart algorithm, and the materials and method deployed to solve the identified problem. Section 5 discusses the evaluation of the proposed system based on security, privacy, and performance. Section 6 focuses on the experiment's result and corresponding findings, security analysis, and evaluation with a comparative analysis of the existing logistics system. Section 7 concludes the research with future research scope.

2. Literature Review and Related Works

Numerous studies have been conducted on the use of blockchain in various contexts. Still, in this section, we are reviewing different streams, which include blockchain technology and its applications in different domains, the impacts of blockchain on logistics sustainability, and the implementation of blockchain innovation on logistics systems.

2.1. Blockchain Technology and Its Applications in Different Areas

Blockchain is a distributed record of pertinent transaction data that all members of a peer-to-peer network agree upon and share [4]. There are three key concepts which power blockchain: cryptography, distributed databases, and a consensus mechanism [5]. Transactional data is encrypted using cryptography following the established protocol, making the data difficult to alter [6]. Blockchain has been applied in many areas, such as edge computing [7], the automotive industry [8], identity management [9], IoT [10,11], smart factories [12,13], e-voting and data processing [14]. Although blockchain-based logistics research is still in its early phase, some pilot-scale projects based on blockchain adoption in logistics and supply chain management have recently tried to use the technology's distinctive features [15]. For instance, with a long history, successful major corporations such as IBM (International Business Machines) released the world's first blockchain-based system for monitoring vaccines from production to administration [16]. This technology aids manufacturers in monitoring the supply chain of vaccines and improving recall management, promoting confidence between the government and private sectors. This technology can detect fraud, checks storage conditions, and notifies logistics of issues.

2.2. Blockchain-Based Logistics Systems

Several kinds of research have been carried out on the applicability of blockchain to logistics, but only a few implementations have been conducted so far. For instance [17], examined how blockchain technology could enhance the sustainability of logistics. The authors discovered that blockchain technology provides superior traceability mechanisms, security, reliability, and cost-efficiency. They also identify that blockchain technology has sustainability, social, and economic impacts. The author proposed a blockchain-enabled logistics supply chain system that helps to trace the product's location, as well as the number of carbon emissions to prevent breaking of environmental law and improve resource management. Furthermore, the study stated that the system helps enterprises to track their waste emissions, allowing them to recycle and reuse the waste products to promote environmental sustainability. Finally, they concluded that adopting blockchain technology into logistics supply chain management systems can increase their long-term visibility.

A blockchain-based solution was presented by [18] to track pharmaceutical products in a logistics supply chain network. Blockchain was deployed to enhance security, transparency, and traceability. The authors employed a questionnaire and interviews as a method of data collection to assess the new system's needs and requirements, and the results were used to determine functional and non-functional requirements.

In terms of implementation, a complete blockchain-based agriculture and food (Agri-Food) logistic supply chain system was designed by [19] using an Ethereum blockchain platform and smart contracts. Blockchain guarantees the immutability of data and records in the network. The blockchain-based storage system ensures safe and efficient data retrieval. However, the limitation of the system is that it cannot handle some crucial issues in supply chain management, such as the parties' credibility, the accountability of trading practices, and product traceability. A blockchain-based IoT-integrated logistics management framework employing Ethereum smart contracts was introduced by [20]. In the proposed system, all transactions are recorded on blockchain, then uploaded to the interplanetary file, although no implementation was made to evaluate the framework's reliability. Rather, they presented a sequence diagram for the framework. For effective product tracking in the healthcare supply chain [21], designed a smart contract and decentralized the off-chain storage-based Ethereum blockchain-based system. The smart contract ensures data provenance, removes the need for intermediaries, and provides all stakeholders with a safe, immutable transaction history. The system architecture and the intricate algorithms that underlie the fundamental concepts of the proposed solution were demonstrated. The test for the validation of the system's performance in enhancing traceability throughout pharmaceutical supply chains, and a cost and security analysis were analyzed.

2.3. Limitations of Existing Literature/Works

This literature review reveals that not much work has been carried out to provide security to the logistics management system and privacy to customers' private information. In this study, we are filling a methodological gap by implementing a blockchain-based logistics management system with the Ethereum smart contract on a peer-to-peer network. This system will enhance the security of the global logistics management system and provide privacy to customer information from attackers with the use of the RSA asymmetric encryption method.

3. Definition of Smart Logistics Systems and Cyber-Attack Challenges

3.1. Smart Logistics Definition

Smart logistics is defined as the application of intelligent technologies [22–24] that intelligently collect and analyze data for effective planning, management, and control of the logistics management process. These processes include transportation warehousing and customer support. Smart logistics is technology-driven, and the enabling technologies in the logistics management system are depicted in Figure 1 [25,26].

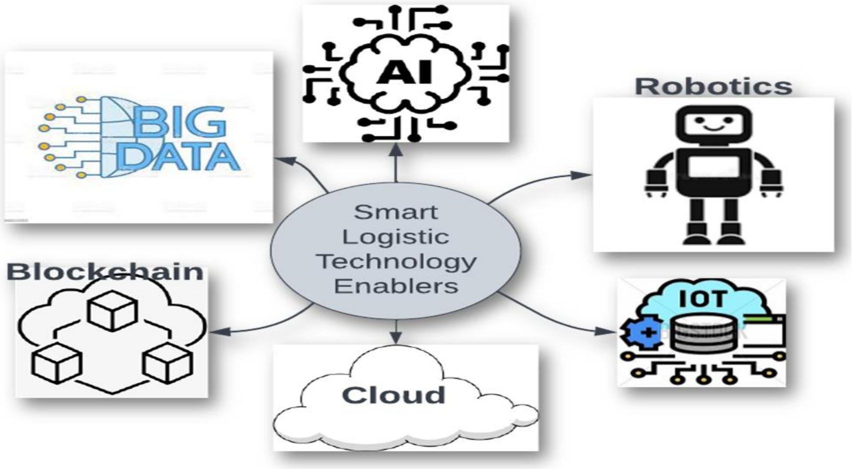


Figure 1. Smart logistic system enablers.

The innovations of logistics systems with these technologies are categorized into the following: fast decision support, seamless information transfer, automation, connectivity, and identification [27].

- **Fast Decision Support:** This involves the utilization of big data analytics and artificial intelligence (AI) to automate fast decision support through a data-driven method.
- **Seamless Information Transfer:** IT systems are combined with cloud computing to provide users with fast access to data and information from several sources and to enable more flexible real-time production planning and scheduling.
- **Automation with robotics:** This is the development of smart/intelligent transportation systems that support or substitute human labor in manual processes.

- **Connectivity and Identification:** These refer to applications of IoT and smart sensor technologies that can uniquely identify goods, improving the tracking and tracing of goods both within and outside of the warehouse.

3.2. Kinds of Cyber-Attacks Challenging Smart Logistics Systems

The kinds of attacks prevalent in logistics systems that challenge the integrity of logistics data consist of computational attacks, denial service attacks, communication attacks, and password attacks [28–38].

- **Computational Attack:** In the logistics domain, smart contract computation performs the mathematical operations that typically establish interactions of smart contracts that facilitate business processes in a logistics application. The computational attack occurs when the smart contract transaction can accept any unauthorized input or data. In a computation attack, the adversary uses various techniques, such as smart contract overflow, etc., to compromise the logistics system's functionality. Smart contract overflow occurs when more value is provided than the maximum value, 256 bits. An increase of 1 value would result in an overflow.
- **Denial of Service Attack:** This attack arises when malicious code is sent across a logistics network to breach the network communication, thereby creating an avenue to steal sensitive information. Most smart logistics systems are prone to this attack due to their centralized database system.
- **Communication Attack:** This kind of attack is sometimes perpetrated by an insider. The interchange of data between various parties (processes or persons) involved in logistics is handled by the communication process. An adversary engaging in a communication attack seeks to compromise the data transferred among numerous connected services. For instance, the attacker might tamper with input values for smart contracts or other components, violate the integrity of the communication by using a selective forward, and drop or insert fake information based on mining public contracts and the ledger.
- **Password Attack:** This attack refers to the stealing of identification information of legitimate logistics stakeholders to carry out nefarious activities.

3.3. Blockchain Innovations and Smart Contract

Blockchain is a decentralized ledger technology with distributed architecture and operates on a peer-to-peer network. It does not require a centralized authority to carry out a transaction. Figure 2 depicts the special characteristics of blockchain, an amazing and unique technology [22].

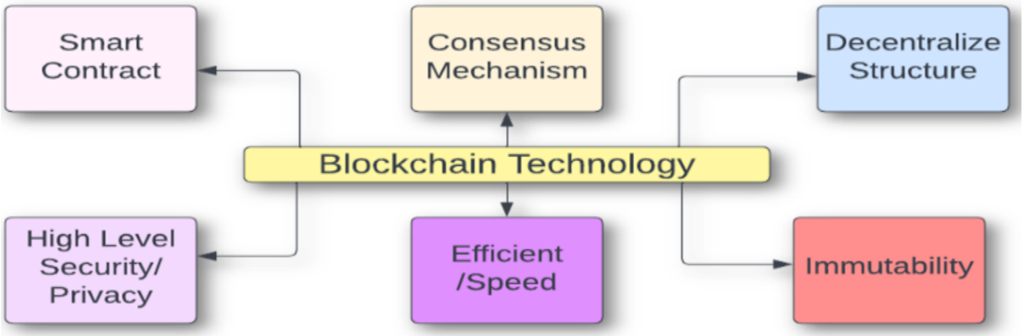


Figure 2. Special characteristics of blockchain technology.

Blockchain can enforce security since each transaction is verified using public–private key encryption. The blockchain transactions recorded on blocks cannot be modified once they have been accepted by a consensus mechanism. Numerous nodes on the network would detect any attempt to alter a transaction record; this ensures that recorded data content is immutable [23].

The innovation of blockchain technology is that it transforms existing systems or components, and it guarantees the confidentiality and integrity of recorded data. Blockchain promotes confidence without the need for a third party. The three types of innovation that blockchain operates on are radical or incremental, competent, and architectural/component innovation.

- Radical or Incremental Innovation: The ability of blockchain to improve existing processes or services
- Competent Innovation: The capability of blockchain to build on an existing system and replace the existing system
- Architectural or Component Innovation: blockchain innovates by changing how systems operate or how components interact.

Smart contracts are self-executing and non-tampering computer programs kept on a blockchain server. Smart contracts are distributed and immutable, so it is difficult to alter their code once written and saved on a blockchain server. Blockchain smart contracts can configure the blockchain to control transactions between parties involved, and aid in the collection and access to data to facilitate decision-making [30]. A smart contract can confirm the accuracy of the rules, directives, and enforced conditions. Solidity is a programming language that can be used to create smart contracts. Smart contracts follow the same procedure of blockchain in storing transaction data [31]. Smart contracts can develop function libraries and are efficient in authenticating by encoding business processes into smart contracts that impose the proper verification among untrusted parties.

3.4. Security Protection Mechanism of Blockchain Using RSA Encryption

Blockchain deploys RSA asymmetric encryption method to enhance the confidentiality, and integrity of shared information on the blockchain network. An RSA algorithm is asymmetric cryptography where two different keys, the private and the public key, are utilized, and the private key is always kept private. Blockchain without a digital signature guarantees message secrecy but not authentication. To build a digital signature for privacy and data protection based on RSA (Rivest, Shamir and Adelman) asymmetric encryption, the mathematical equation given below is deployed;

$$\text{S} = \text{RSA (data, key)}, \text{V} = \text{RSA (S, K)} = = \text{data} \tag{1}$$

where S = private signing key, V = Public Verification Key

The intended data is signed using an RSA algorithm with the private key, further sealed with the public key, and evaluated to see whether the results match the expected data. This approach might occasionally provide longer keys, but the cryptographic hashes provided in Equation (2) are used to address this problem

$$\text{S} = \text{RSA (hash of data, key)}, \text{v} = \text{RSA (s, k)} = = \text{(hash of data)} \tag{2}$$

The general proposed mathematical model for security and privacy protection of data using RSA digital signature is depicted in the equations below;

$$\text{Encrypt (hash of data, key) RSA (data, key)} \tag{3}$$

$$\text{Decrypt (hash of data, key) RSA (data, key)} \tag{4}$$

In a real-world application, the hash function is used for signing, and the post-processing is used for decryption. For a signature, the hash function is used first, then the RSA function, and vice versa. This approach aims to decrease the misuse of information while being shared among a range of people. Figure 3 shows the privacy and security mechanism of asymmetric RSA encryption.

Before data are sent from A to B, it will be encrypted, utilizing the private key of the sender (A) and the receiver's public key (B). For receiver (B) to access data, it has to be decrypted using the receiver(B)private key and the sender(A) public key. This ensures data privacy and keep data from unauthorized access except the authorized entity.

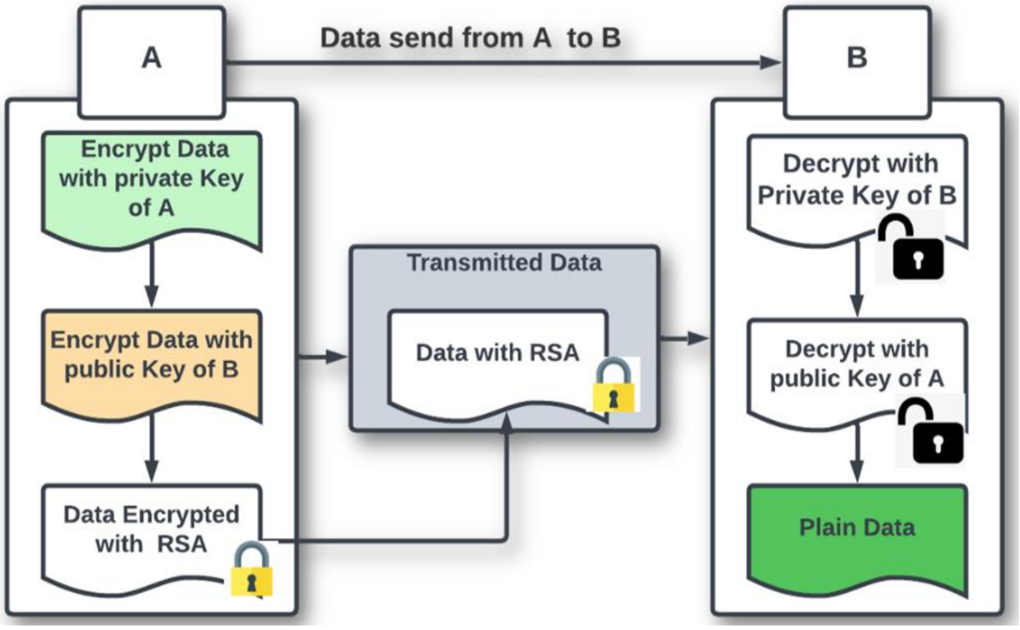

A
Data send from A to B
B
Encrypt Data with private Key of A
Encrypt Data with public Key of B
Data Encrypted with RSA
Transmitted Data
Data with RSA
Decrypt with Private Key of B
Decrypt with public Key of A
Plain Data

Figure 3. Blockchain privacy and security mechanism using asymmetric RSA encryptions.

3.5. Advantages of RSA over ECC

The security offered by RSA with a 2048-bit key is equivalent to that offered by the ECC algorithm with a 256-bit key, but these are advantages of RSA over the ECC encryption method.

(a) ECC is sluggish at encryption and very fast at decryption,
(b) RSA has proven to be quite successful at encrypting but not very efficient at decrypting.
(c) RSA allows for the encryption of messages before transmitting. It also helps to certify the message so that the recipient will know that it has not been altered during transmission.
(d) RSA is easier to implement than ECC.

3.6. Blockchain-Based Logistics Management System

A typical blockchain-based logistics management system [37,38] is depicted in Figure 4.

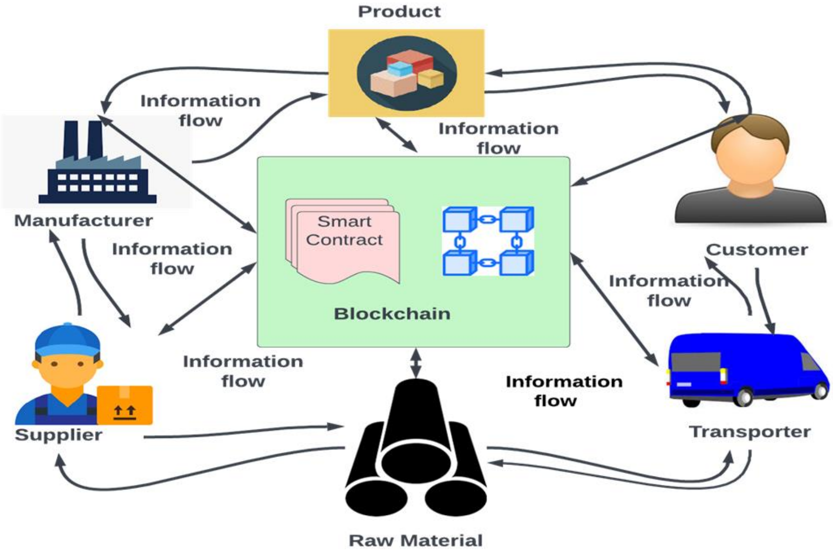


Figure 4. Blockchain-based logistics management system.

It illustrates the flow of goods, raw materials, and information among the logistics entities that interact and collaborate through blockchain. Every transaction recorded in the blockchain network is immutable and time-stamped; this helps to avoid unnecessary tampering [32] and keep track of the transaction. All logistics entities verify their authenticity before accessing the system. Suppliers deliver raw materials to the manufacturer and record their transactions on the blockchain network. Manufacturers upload new products, which are broadcasted on the blockchain network. Customers will order products from the manufacturers, and the product will be delivered to the customer by a transporter

4. Proposed Methodology

This section discusses the proposed system architecture and highlights the specified smart contract algorithms, materials, and methods deployed in the experiment.

4.1. System Architecture

The proposed system architecture integrates smart contracts on the Ethereum platform for seamless global transactions. The system architecture comprises four major players: manufacturers, suppliers, transporters, and customers, as depicted in Figure 5.

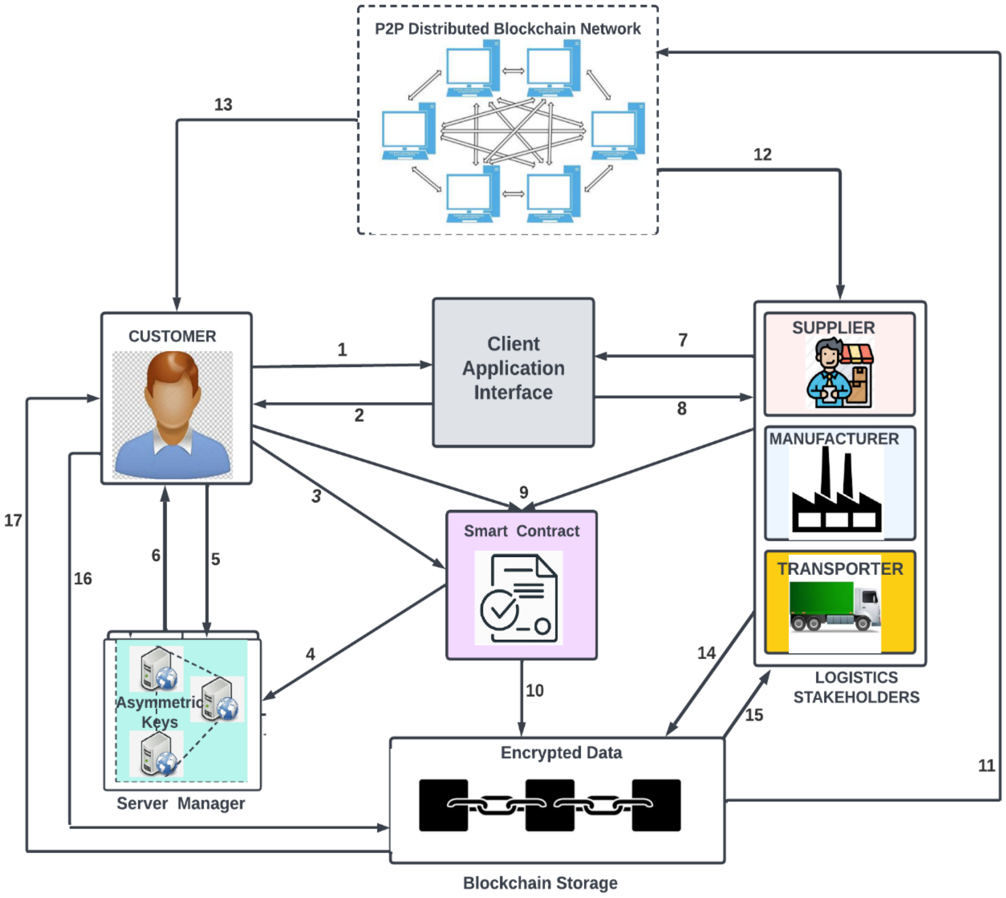


Figure 5. Proposed blockchain-based secure and efficient logistics management system architecture.

The proposed system's architecture workflow is described in the following steps below:

1. The customer creates an account through the client application interface and is assigned user identification by the system
2. Customer logs in to the system with the user identifications.
3. The customer generates an asymmetric key through the smart contract.
4. The generated encrypted key is validated and stored in the decentralized server. The decentralized server manager is used to store all the private keys,

5. The customer can query for the asymmetric key.
6. The feedback of the query is sent to the customer and it can be decrypted by the customer.
7. The other logistics stakeholders (manufacturers, supplier, and transporters) with different roles and designations create accounts through the client application interface and are assigned user identifications.
8. The stakeholders log in to the system with the user identification.
9. The customers and other logistics stakeholders initiate a transaction such as a manufacturer adding products in the blockchain network, a customer purchasing products, product change of ownership. Customers encrypt personal data and transmit to the corresponding receiver (logistics stakeholder) using the customer's private key and the receiver's public key. The receiver will decrypt the data using the customer's public key and the receiver's private keys. This mechanism protects customers' data from unnecessary access and verifies the message's source.
10. All the transactions that are executed by the smart contract are validated and recorded in the block once they pass the validation check. and then added to the blockchain. All transaction is completely secure because transactions are merely added to the previous hash with a time stamp.
11. The stored information is broadcasted on the p2p distributed blockchain network. This process ensures that every transaction over the network is distributed to all system stakeholders
12. The logistics stakeholders (manufacturers, suppliers, and transporter) connected to the network have access to updated information.
13. The customer also has access to the updated distributed information on the blockchain network.
14. The logistics stakeholders make queries from the blockchain repository.
15. The quarried information is retrieved from the blockchain storage or repository and sent back to the corresponding entity.
16. Customers make queries from the blockchain storage
17. The information is retrieved from the blockchains repository and feedback is sent to the customer.

4.2. Specified Smart Contract

The various smart contracts specified for blockchain-based logistics management consist of:

- Secured sharing of customer information among stakeholders with encryption and decryption using asymmetric encryption
- Creation of product records on the blockchain network,
- Validation check for stakeholders to perform a transaction
- Obtain the asymmetric keys from the server
- Purchase product, change of ownership, and delivery of the product

All notations utilized in the smart contract algorithm are listed in Table 1.

A. Secured sharing of customer information among stakeholders using RSA asymmetric encryption and decryption method.

To encrypt a customer's data (C_{data}) and transmit it to a logistics stakeholder (receiver R), the hash of the customer data and receiver public key and the hash of customer data and the private receiver key with a 2048-bit asymmetric keys encryption is used. The transaction data (T_{c1}) of customer 1 is given in the equation below;

$$T_{c1} = \text{Enc hash of } \{(C_{data}, C_{privatekey}), (C_{data}, R_{publickey})\}, \text{ timestamp} \quad (5)$$

where,

Enc hash of (C_{data}, $C_{privateKey}$) = SHA244
The hash of (C_{data}, $R_{publicKey}$) = SHA256

Algorithm 1 deploys asymmetric RSA encryption for customers′ data security and privacy using the customer′s private key and the receiver′s public key. Decryption by the transporter is facilitated by using the receiver′s private key and the customer′s public key. This mechanism protects customer data from unauthorized access and authenticates the source of information. Customers use the same mechanism to share private data with other logistics stakeholders, which requires customer data to carry out logistics operations.

Table 1. List of notations and descriptions.

Notations	Meaning
M_{id}	Manufacturer unique identifier
$M_{privatekey}$	Manufacturer private key
C_{Id}	Customer unique identifier
$C_{privatekey}$	Customer private key
$C_{publickey}$	Customer public key
C_{data}	Customer data (name, address, mobile no, etc)
$(C_{data})_{Enc}$	Encrypted customer data
S_{Id}	Supplier unique identifier
T_{Id}	Transporter unique identifier
$T_{publickey}$	Transporter public key
$T_{privatekey}$	Transporter private key
P_{Id}	Product unique identifier
P_P	Product Price
E_{nc}	Encryption
D_{ec}	Decryption
B_{Id}	The unique ID of the buyer of the product
Sel_{Id}	The unique ID of the seller of the product
$Sel_{publickey}$	Seller public key
Sol_{date}	The date on which the purchase is being made.
$R_{privateKey}$	Receiver private key
$R_{publicKey}$	Receiver Public Key

Algorithm 1: Smart contract for secured sharing of customer data

```
Input: ($C_{privateKey}$, $C_{publicKey}$, $T_{privateKey}$, $T_{publicKey}$, $C_{data}$)
Output: Encryption and Decryption of Customer Data
            Encrypt (hash of $C_{data}$) using $C_{privatekey}$ = M
            Encrypt (hash of $C_{data}$) using $T_{publickkey}$ = X
if {(M, X) $E_{nc}$} = $(C_{data})_{Enc}$ then
                Transmit $(C_{data})_{Enc}$ to $T_{id}$
        else
                Declare Error Message and Return to none
    end if
    If ($T_{privateKey}$ exists), then
                Decrypt {$(C_{data})_{Enc}$} using $T_{privateKey}$
                Decrypt {$(Cdata)_{Enc}$} using $C_{publicKey}$,
                Acknowledge $C_{data}$ by $T_{id}$
        else
                Declare a message that the transporter does not exist
end if
```

B. Creation of product records on the blockchain network

Algorithm 2 describes smart contract transactions to create a product. It deploys the manufacturer′s public key and product ID. Product creation marks the beginning of the product life cycle in the blockchain network. A product created will be declared for sale if the manufacturer′s private ID is the same as the product owner′s ID. Manufacturers have the sole authority to add products to the blockchain network.

Algorithm 2: Smart contract for creation of product on blockchain network

```
Inputs: $M_{private\_key}$, $P_{Id}$, p_p
Output:   Product created and out for sale
If ($M_{private\_key}$ and $P_{Id}$ exist) then
            create _product details
              increment Product Count
            update Product_Details
      if else
         Declare error message cannot create a product
end if
if ($M_{private\_key}$ = ProductOnwer$_{id)}$ then
            Declare ProductforSale
      if else
            Declare error message that product owner is not correct
end if
```

C. Validation check for Stakeholders to perform a transaction

Algorithm 3 is implemented with a validation check; it is used to authenticate the logistics stakeholders before they can access the blockchain network and perform any transaction. The stakeholder's user ID and password are deployed for the validation check.

Algorithm 3: Consensus algorithm for validation check for stakeholders

```
Input: ($C_{Id}$, $M_{Id}$, $S_{Id}$, $T_{Id}$)
Output: Log in to the blockchain network
  if ($C_{Id}$ and Password are valid) then
         Log in Customer to the blockchain Network
      else
         Declare customer does not exist and create a customer account
      end if
if ($M_{Id}$ and Password are valid) then
              Log in Manufacturer to the blockchain Network
      else
      Declare Manufacturer does not exist and Create a Manufacturer account
  end if
  if ($S_{Id}$ is valid) then
              Log in Supplier to the blockchain Network
      else
              Declare Supplier does not exist and Create a Supplier account
  end if
if ($T_{id}$ is valid) then
              Log in Transporter to the blockchain Network
      else
     Declare Transporter does not exist and Create a Transporter account
end if
```

D. Get the asymmetric keys from the server

In Algorithm 4, the customer can retrieve their asymmetric key using (C_{id} and $C_{publickey}$). If (C_{id} and $C_{publickey}$) exit, the server manager administers and keeps the list of asymmetric keys, and only the customer can decrypt the asymmetric key's encrypted form.

Algorithm 4: Smart contract for obtaining asymmetric key for customer

```
Inputs: $C_{id}$, $C_{publickey}$
Output:   Asymmetric Key of Customer
 if ($C_{id}$ and $C_{publicKey}$ exit) then
          Get_asymmetrickey of $C_{id}$ from the server
          Encrypt (asymmetric key, $C_{publickey}$)
          Return as (asymmetric key) $E_{nc}$
      else
            Return to None
end if
```

E. Purchase product, change of ownership, and delivery of the product

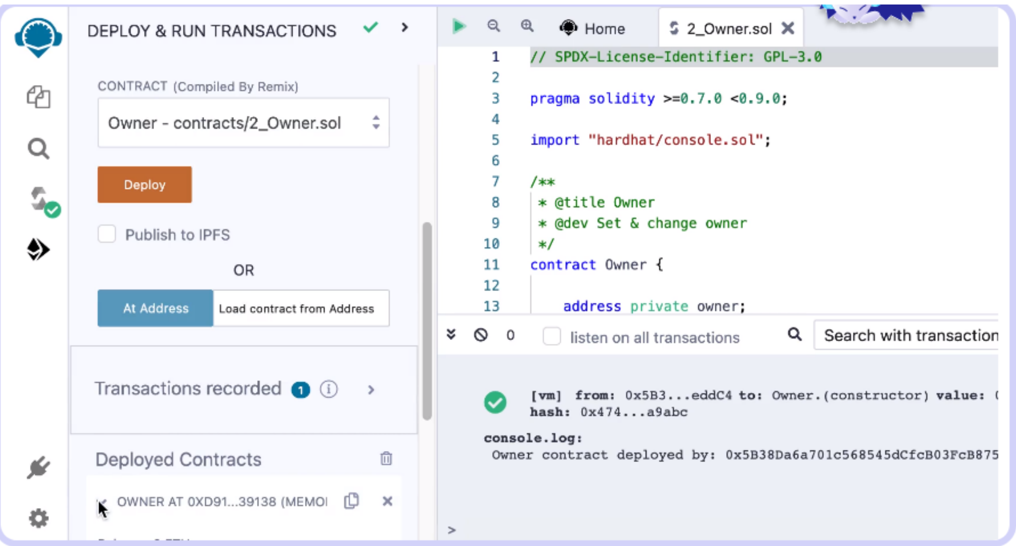
In Algorithm 5, the validation to purchase, change of ownership, and delivery of the product is deployed using (Selpublickey, b_{id} P_{id}). If the check for the availability of the product is accepted, the purchase of the product will proceed. If the product's ownership validation is confirmed with ($sel_{publickey = ProductOwnerId}$), the payment and product ownership change will be initiated. If the product delivery time agrees with that of the buyer, the blockchain will be validated and the product will be delivered to the buyer by the transporter.

Algorithm 5: Smart contract for purchase, transfer, and delivery of product

```
Inputs: $Sel_{publickey}$, $Pi_{d}$, $B_{Id}$, $sol_{date}$, status,p_p
Output: Purchase And delivery of Product
  if ($P_{id}$ exists) then
          if (product is available) then
                Proceed with the purchase of the product
             else
                Report with a message that the product is not available
             end if
end if
if ($Sel_{publickey =}$ $productOnwer_{id}$) then
              Proceed with payment for the product
      else
              Declare an error message that the seller is fake
end if
if (buyer account balance $\geq$ p_p), then
                        transfer funds from the buyer account to the seller account
                      update $productOwner_{Id}$
                      update the ownership Address
                   Update Status to product successfully purchased
                else
                      Report with error message insufficient fund
  end if
           if (product delivery date is in agreement with the buyer) then
             if ($T_{id}$ exists) then
                   Deliver product
                  Acknowledge delivery by the buyer
           else
              Reschedule delivery of the product
      end if
end if
```

4.3. Materials and Method

The specified smart contracts are created using the Remix IDE (integrated development environment)'s solidity language and are then converted into Ethereum Virtual Machine (EVM) bytecode for deployment. Figure 6 depicts the smart contract deployment environment.


DEPLOY & RUN TRANSACTIONS
CONTRACT (Compiled By Remix)
Owner - contracts/2_Owner.sol
Deploy
□ Publish to IPFS
OR
At Address
Load contract from Address
Transactions recorded 1
Deployed Contracts
OWNER AT 0XD91...39138 (MEMOI
Home
2_Owner.sol
0
□ listen on all transactions
Search with transaction

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.7.0 <0.9.0;

import "hardhat/console.sol";

/**
 * @title Owner
 * @dev Set & change owner
 */
contract Owner {

    address private owner;
```

```
[vm] from: 0x5B3...eddC4 to: Owner.(constructor) value: (
hash: 0x474...a9abc
console.log:
 Owner contract deployed by: 0x5B38Da6a701c568545dCfcB03FcB875
>
```

Figure 6. Ethereum Remix IDE smart contract deployment environment.

Stress testing is carried out initially to determine how many simultaneous transactions the systems can handle. The smart algorithm to create a product is deployed to measure the proposed system overhead. To assess the performance of the blockchain-based line system and proposed approach, various numbers of transactions and submission-timed execution were timed. Table 2 depicts the tool specification deployed in the experiment.

Table 2. Tools with specifications.

S/No	Tools	Specifications
1.0	Solidity version,	0.7.0 and more
2.0	REMIX IDE	Intel (R) Core (TM), i5—8250U
3.0	CPU, Windows 10	1.60 GHz, 8 GB of RAM, 64-bit OS

5. Proposed System Evaluation

The viability and efficacy of the proposed system depicted in Figure 5 are evaluated on three conditions: security, privacy, and performance.

5.1. Privacy Evaluation

The following theorems are used to evaluate the privacy efficacy of the proposed system:

Theorem 1. *Suppose an adversary X launches an attack to decrypt and access encrypted data of a customer1 to transmit it to transporter 1 for logistics purpose. It is assumed that adversary X obtains the encrypted data from the public network, and the customer deployed two-way asymmetric RSA encryption utilizing the customer1 private key and transporter 1 public key.*

Proof of Theorem 1. For adversary X to decrypt and access the transmitted customer data, it has to deploy the customer1 public key and the transporter 1 private key. The private key is always kept secret, making it difficult to access transmitted data. □

Theorem 2. *Consider a scenario in which an adversary logistics user (U_1) acquires the product creation (smart contract algorithm 2) intended for manufacturer M1. They can request the creation of a product, but the smart-contract transaction cannot be authenticated or validated on the blockchain.*

Proof of Theorem 2. The validator will not validate the transaction since the signer's and manufacturer M1's public keys must match. The private key is always kept secret, since it is used to create the public key. □

5.2. Security Evaluation

Consider an adversary who became a user of the blockchain-based logistics system network; then, the user may obtain all the blockchain data. The first field of (E_{nc} Hash of C_{data}, $C_{privateKey}$) is irreversible, and the second field of E_{nc} ($C_{data,}$ $R_{publicKey}$) is also irreversible. With these two steps of encryption, to crack a blockchain-based logistics system that deployed 2048 RSA encryption, it will take a fully-fledged quantum computer with 20 million quantum bits (q-bits) [33]. This will not likely happen soon since it involves a lot of funds to acquire this kind of computer with the right specifications.

5.3. Performance Evaluation

The performance evaluation is measured in terms of throughput and latency.

Throughput: This is the pace at which transactions are added to a blockchain. The average throughput can be determined using the equation below;

$$\text{Average Thoughput}\ \left(\text{Tav}_{\text{tput}}\right) = \frac{1}{n}\sum_{i=1}^{n}\frac{Ni}{tci} \tag{6}$$

tci: Is the transaction committed time,
Ni: is the total number of transactions for the ith trial, and
n: is the total number of trials run.

Latency is the period between the submission and execution of the transaction, referred to as the processing time. The latency (L) is calculated as follows.

$$\text{Latency}(L) = \frac{1}{n}\sum_{i=1}^{n}\frac{Ni}{tci}\,(tci - tsi)\frac{1}{Ti} \tag{7}$$

where:
tsi: Is the transaction submission time for the ith trial,
tci: Is the transaction execution times for the ith trial,
Ti: indicates how many transactions were submitted for the ith trial.

6. Results and Findings

6.1. Results

The proposed system's security and privacy are evaluated based on the theorem. The performance is evaluated using two blockchain baseline systems, namely, the blockchain baseline system with RSA asymmetric encryption algorithm and the blockchain baseline system without the RSA asymmetric RSA encryption algorithm). Table 3 and Figure 7 show the comparison result of blockchain baseline system submission and execution time of transactions without RSA encryption.

Table 3. The comparison results of blockchain baseline system submission and execution time of transactions without RSA encryption.

No of Transactions	Submission Time (s)	Execution Time (s)
100	6.0	6.1
200	12	12.3
300	17	17.57
400	22.5	23.2
500	27.7	28.4

Table 4 and Figure 8 depict the result of the submission and execution time of the transaction with RSA encryption.

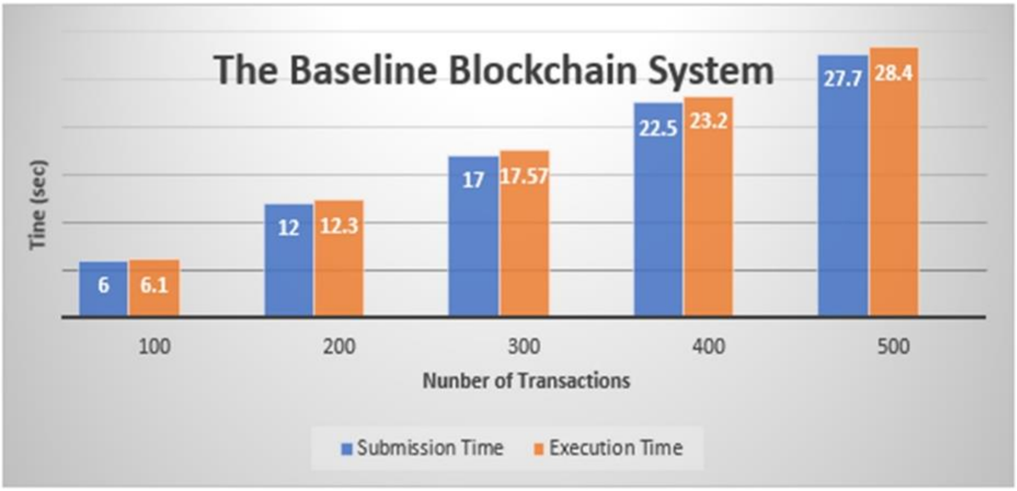


Figure 7. Transactions without encryption algorithm.

Table 4. The comparison results of the proposed system submission and execution time of transactions with RSA Encryption.

No of Transactions	Submission Time (s)	Execution Time (s)
100	6.0	6.4
200	12	12.9
300	17	18.3
400	22.5	24.2
500	27.7	29.2

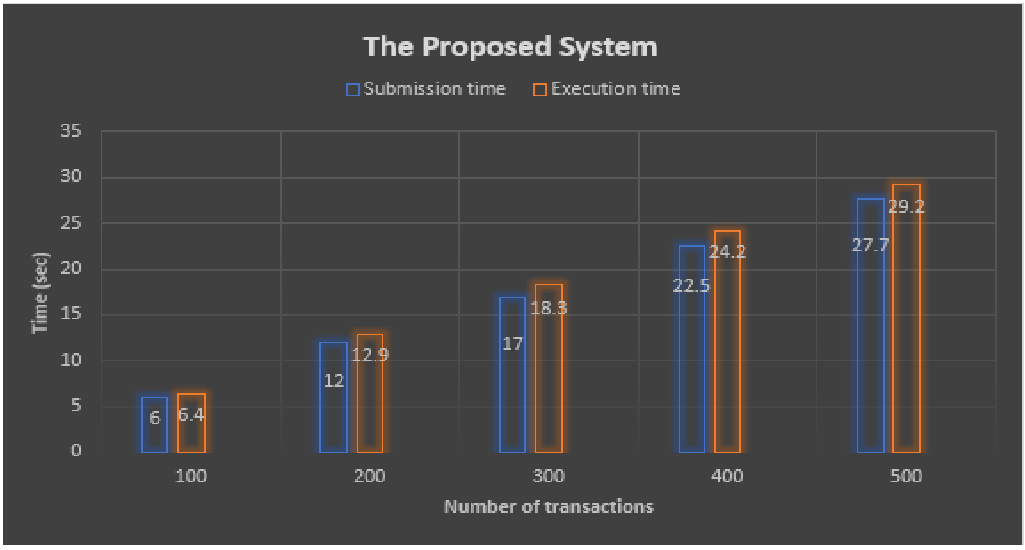


Figure 8. A transaction with an RSA encryption algorithm.

6.2. Findings

The security of the proposed system is evaluated using a theorem, and the theorem-proof indicates that the system is secured from internal and external attacks. The performance results of the two blockchain systems (baseline system and proposed approach) are compared in terms of throughput and latency. Based on Equation (6) and the results (Figures 7 and 8), the projected throughput for the baseline and proposed systems were (18.4456 and 17.5236), respectively. These two results showed that the proposed system added an extra overhead of 4.206%. The RSA algorithms did not have any significant effect on the overhead.

Based on Equation (7) and results from Figures 7 and 8, the latency calculation of the two systems (the proposed system and the baseline system), the latency values were (0.00150 and 0.00400), respectively. The proposed system*s* and baseline's latency were too low to be compared. The combined outcome of the baseline and the proposed approach is depicted in Figure 9.

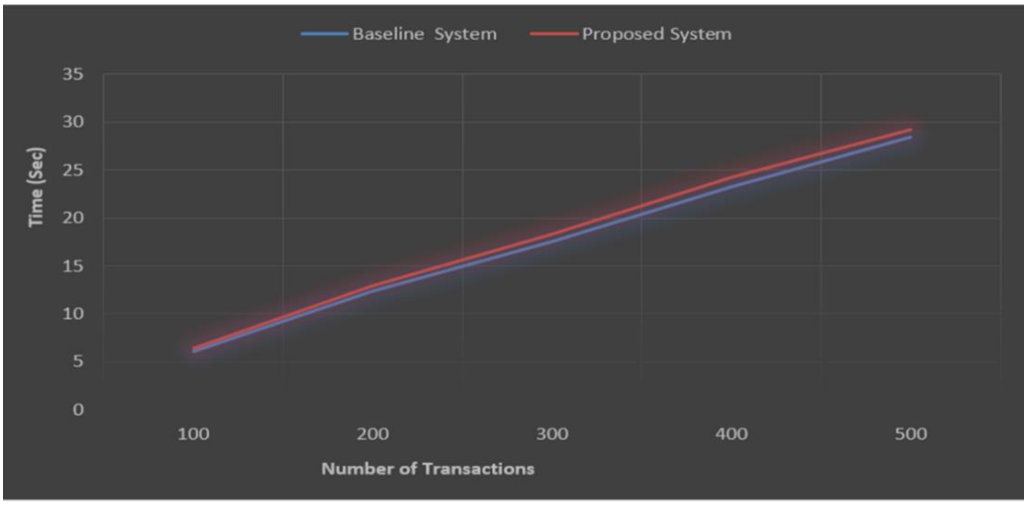


Figure 9. The comparison of baseline and proposed system.

6.3. Comparison of Proposed System with Exiting System

A range of blockchain-based logistics systems was chosen to compare the proposed work. Table 5 depicts the comparison between the existing blockchain-based system and the proposed system.

Table 5. Comparison of the proposed system with existing systems.

Authors	Blockchain Platforms	Encryption Method	Transaction Privacy and Security	Efficiency
[34]	Ethereum	none	low	low
[35]	Hyperledger fabric	Homomorphic encryption	high	high
[36]	Hyperledger sawtooth	Symmetric encryption	high	high
Proposed system	Ethereum	RSA Asymmetric encryption	very high	very high

7. Conclusions and Future Work

This study identified the security and privacy challenges in smart logistics systems, the source of cyber-attacks prevalent in smart logistics contracts, which is a critical issue for the optimal operation of logistics operations.

This paper contributed to addressing the security and privacy issues in smart logistics systems by proposing a blockchain-based logistics management system. This system enhances the security of the logistics management system against cyber-attacks and provides privacy to customers' data against unauthorized access while being shared among logistics stakeholders by deploying asymmetric RSA encryption.

The findings show that the implemented blockchain smart contracts for sharing customers' private information among the logistics partners are cyber-attack proof. The proposed system allows for the efficient creation and transfer of assets. The evaluation of the case study demonstrated that the proposed system is secured against all possible security and privacy threats. The performance outcomes of a proof-of-concept implementation acquired by utilizing the Ethereum platform showed that the proposed system adds just a small amount of overhead. The comparative analysis shows that the proposed system is better than the existing systems. With higher security and higher efficiency, the proposed system can support logistics business models with low cheap computer configuration costs. Overall, our research provides various benefits to make logistics management stakeholders deploy blockchain-based solutions that are better than the traditional system.

This study has some limitations despite its significance. There is considerable overlap in the research on logistics and SCM, although we focused primarily on logistics tasks rather than SCM. Moreover, only a few research papers on this domain deal with the implementation aspect; others are theoretical papers.

In future research, we will focus on integrating artificial intelligence (AI) systems and blockchain technology into logistics management for improved security of logistics data and enhancement of logistics procurement for improved sourcing of quality goods.

Author Contributions: Conceptualization, writing—original draft, N.A.U. and S.B.G.; supervision, S.B.G.; validation, N.A.U. and A.S.R.; propose the new method or methodology, N.A.U.; formal analysis, investigation, N.A.U.; resources, J.H. and M.A.; software, N.A.U. and S.B.G.; writing—review and editing, S.M.N.I., J.H. and M.A. All authors have read and agreed to the published version of the manuscript.

Funding: The National Natural Science Foundation of China (No. 62106024), the China Postdoctoral Science Foundation (No. 2022M711458), the Natural Science Foundation of Chongqing, CSTB2022NSCQ-BHX0018.

Data Availability Statement: Dataset is available in Kaggle.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and IoT Integration: A Systematic Survey. *Sensors* **2018**, *18*, 2575. [CrossRef] [PubMed]
2. Council of Supply Chain Management Professionals (CSCMP). *Grants Regist.* **2021**, 303–304. [CrossRef]
3. Akram, Asif, and Bross, Philipp Trust, Privacy, and Transparency with Blockchain Technology in Logistics. CIS Proceedings. 2018. Available online: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1021&context=mcis2018 (accessed on 24 September 2022).
4. Rosenberger, P. Satoshi Nakamoto (Bitcoin and Blockchain), Blockchain Is a Peer 2 to-Peer-Distributed Decentralized network. In *Bitcoin und Blockchain*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 25–34. [CrossRef]
5. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE 6th International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564. [CrossRef]
6. Beck, R.; Stenum Czepluch, J.; Lollike, N.; Malone, S. Blockchain–the gateway to trust-free cryptographic transactions. In Proceedings of the Twenty-Fourth European Conference on Information Systems(ECIS), Istanbul, Turkey, 12 June 2016.
7. Xiong, Z.; Yang, Z.; Niyato, D.; Wang, P.; Han, Z. When Mobile Blockchain Meets Edge Computing. *IEEE Commun. Mag.* **2017**, *56*, 33–39. [CrossRef]
8. Shrestha, R.; Nam, S.Y. Regional Blockchain for Vehicular Networks to Prevent 51% Attacks. *IEEE Access* **2019**, *7*, 95033–95045. [CrossRef]
9. Dunphy, P.; Petitcolas, P. A First Look at Identity Management Schemes on the Blockchain. *IEEE Secur. Priv.* **2018**, *16*, 20–29. [CrossRef]
10. Sun, Y.; Zhang, L.; Imran, M.A. Blockchain-Enabled Wireless Internet of Things: Performance Analysis and Optimal Communication Node Deployment. *IEEE Internet Things J.* **2019**, *6*, 5791–5802. [CrossRef]
11. Liu, C.H.; Wen, S. Blockchain-Enabled Data Collection and Sharing for Industrial IoT with Deep Reinforcement Learning. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3516–3526. [CrossRef]
12. Wan, J.; Li, J.; Imran, M.; Li, D. Fazal-e-Amin Based Solution for Enhancing Security and Privacy in Smart Factory. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3652–3660. [CrossRef]
13. Dinh, T.T.A.; Liu, R.; Zhang, M.; Chen, G.; Ooi, B.C.; Wang, J. Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Trans. Knowl. Data Eng.* **2018**, *30*, 1366–1385. [CrossRef]
14. Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted blockchain technology. *IEEE Access* **2019**, *7*, 24477–24488. [CrossRef]
15. Imeri, A.; Khadraoui, D.; Agoulmine, N. Blockchain Technology for the Improvement of SCM and Logistics Services: A Survey. In *Industrial Engineering in the Big Data Era. Lecture Notes in Management and Industrial Engineering*; Calisir, F., Cevikcan, E., Camgoz, A.H., Eds.; Springer: Cham, Switzerland, 2019; pp. 349–361.
16. IBM. Vaccine Distribution on Blockchain. 2020. Available online: https://www.ibm.com/blockchain/solutions/vaccine-distribution (accessed on 10 September 2022).
17. Park, A.; Li, H. The Effect of Blockchain Technology on Supply Chain Sustainability Performances. *Sustainability* **2021**, *13*, 1726. [CrossRef]
18. Muniandy, M.; Ern, O.; Tze, G. Implementation of Pharmaceutical Drug Traceability Using Blockchain Technology. 2019. Available online: http://eprints.intimal.edu.my/1308/1/vol.2019_035.pdf (accessed on 14 September 2022).

19. Shahid, A.; Almogren, A.; Javaid, N.; Al-Zahrani, F.A.; Zuair, M.; Alam, M. Blockchain-Based Agri-Food Supply Chain: A Complete Solution. *IEEE Access Inst. Electr. Electron. Eng.* **2020**, *8*, 69230–69243. [CrossRef]
20. Ugochukwu, N.A.; Goyal, S.B.; Arumugam, S. Blockchain-Based IoT-Enabled System for Secure and Efficient Logistics Management in the Era of IR 4.0. *J. Nanomater.* **2022**, 1–10. [CrossRef]
21. Musamih, A.; Salah, K.; Jayaraman, R.Y. Blockchain-Based Approach for Drug Traceability in Healthcare Supply Chain. IEEE Access. *Inst. Electr. Electron. Eng.* **2021**, *9*, 9728–9743. [CrossRef]
22. Hackius, N.; Petersen, M. Blockchain in logistics and supply chain: Trick or treat? In Proceedings of the Hamburg international conference of Logistics (HICL), online, 12 October 2017; pp. 3–18.
23. Önder, I.; Treiblmaier, H. Blockchain and tourism: Three research propositions. *Ann. Tour. Res.* **2018**, *72*, 180–182. [CrossRef]
24. Ding, Y.; Jin, M.; Li, S.; Feng, D. Smart logistics based on the internet of things technology: An overview. *Int. J. Logist. Res. Appl.* **2020**, *24*, 323–345. [CrossRef]
25. Aziz, M.F.; Khan, A.N.; Shuja, J.; Khan, I.A.; Khan, F.G.; Khan, A. A lightweight and compromise-resilient authentication scheme for IoTs. *Trans. Emerg. Telecommun. Technol.* **2019**, *33*, e3813. [CrossRef]
26. Anwar, M. Connect2smallports Project: South Baltic Small Ports–Gateway to Integrated and Sustainable European Transport System: Project Brief and Updates on the Project Activities: Digital Audit. Blockchain Design Strategy. Call for Collaboration. Reports and Scientific Publications. 2019. Available online: http://urn.kb.se/resolve?urn=urn:nbn:se:bth-18763 (accessed on 2 October 2022).
27. Cimini, C.; Lagorio, A.; Romero, D.; Cavalieri, S.; Stahre, J. Smart Logistics and the Logistics Operator 4.0. *IFAC* **2020**, *53*, 10615–10620. [CrossRef]
28. Al-Farsi, S.; Rathore, M.M.; Bakiras, S. Security of Blockchain-Based Supply Chain Management Systems: Challenges and Opportunities. *Appl. Sci.* **2021**, *11*, 5585. [CrossRef]
29. Sayeed, S.; Marco-Gisbert, H. On the effectiveness of control-flow integrity against modern attack techniques. In *ICT Systems Security and Privacy Protection*; Dhillon, G., Karlsson, F., Hedström, K., Zúquete, A., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 331–334. [CrossRef]
30. Banerjee, M.; Lee, J.; Choo, K.K.R. A Blockchain future for the internet of things security: A position paper. *Digit. Commun. Netw.* **2018**, *4*, 149–160. [CrossRef]
31. Rane, S.; Thakker, S. Green procurement process model based on Blockchain–IoT integrated architecture for a sustainable business. *Manag. Environ. Qual. Int. J.* **2019**, *31*, 741–763. [CrossRef]
32. Korpela, K.; Hallikas, J.; Dahlberg, T. Digital supply chain transformation toward Blockchain integration. In Proceedings of the 50th Hawaii International Conference on System Sciences, Hilton Waikoloa Village, HI, USA, 4–7 January 2017; pp. 4182–4191.
33. Amy, N. Quantum Computer Comes Closer to Cracking RSA Encryption Shor's Algorithm Performed in a System less than Half the Size Experts Expected. 2016. Available online: https://spectrum.ieee.org/encryptionbusting-quantum-computer-practices-factoring-in-scalable-fiveatom-experiment (accessed on 30 September 2022).
34. Toyoda, K.; Mathiopoulos, P.T.; Sasase, I.; Ohtsuki, T. A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain. *IEEE Access* **2017**, *5*, 17465–17477. [CrossRef]
35. Du, M.; Chen, Q.; Xiao, J.; Yang, H.; Ma, X. Supply Chain Finance Innovation Using Blockchain. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1045–1058. [CrossRef]
36. Mohit, M.; Kaur, S.; Singh, M. Design and implementation of transaction privacy by ownership and traceability in the blockchain-based supply chain. *Clust. Comput.* **2021**, *25*, 2223–2240. [CrossRef]
37. Ugochukwu, N.A.; Goyal, S.B. Logistics Management Using Blockchain: A Review of Literature and Research Agenda. *IGI Global* **2022**, 122–144. [CrossRef]
38. Ji, T.; Goyal, S.B.; Arumugam, S. A Regulated Anticounterfeiting Traceability Metamodel Based on Blockchain in Supply Chain in the Era of IR 4.0. *J. Nanomater.* **2022**, *11*, 4305966. [CrossRef]