

Article

A Blockchain-Enabled IoT Logistics System for Efficient Tracking and Management of High-Price Shipments: A Resilient, Scalable and Sustainable Approach to Smart Cities

Mohammed Balfagih ¹, Zain Balfagih ², Miltiadis D. Lytras ^{3,*}, Khaled Mofawiz Alfawaz ⁴, Abdulrahman A. Alshdadi ⁵ and Eesa Alsolami ⁵

- ¹ Department of Computer and Network Engineering, College of Computer Science and Engineering, University of Jeddah, Jeddah 23890, Saudi Arabia; mabalfagih@uj.edu.sa
 - ² Computer Science Department, Effat Energy and Technology Research Center, Effat College of Engineering, Effat University, Jeddah P.O. Box 34689, Saudi Arabia; zbalfagih@effatuniversity.edu.sa
 - ³ Management Information Systems Department, School of Business and Economics, American College of Greece, 15342 Athens, Greece
 - ⁴ Management Information System Department, King Abdulaziz University, Jeddah 23890, Saudi Arabia; kalfawaz@kau.edu.sa
 - ⁵ Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah 23890, Saudi Arabia; alshdadi@uj.edu.sa (A.A.A.); emaillesa@gmail.com (E.A.)
- * Correspondence: mlytras@acg.edu

Abstract: The concept of a smart city is aimed at enhancing the quality of life for urban residents, and logistic services are a crucial component of this effort. Despite this, the logistics industry has encountered issues due to the exponential growth of logistics volumes, as well as the complexity of processes and lack of transparency. Consequently, it is necessary to develop an efficient management system that offers traceability and condition monitoring capabilities to ensure the safe and high-quality delivery of goods. Moreover, it is crucial to guarantee the accuracy and dependability of distribution data. In this context, this paper proposes a blockchain-enabled IoT logistics system for the efficient tracking and management of high-price shipments. A smart contract based on blockchain technology has been designed for automatic approval and payment, with the aim of distributing shipping information exclusively among legitimate logistics parties. To ensure authentication, a zero-knowledge proof is used to conceal the blockchain address. Moreover, an intelligent parcel (iParcel) containing piezoresistive sensors is developed to pack delivered goods during the shipping process for violation detection such as severe falls or theft. The iParcels are automatically tracked and traced, and if a violation occurs, the contract is cancelled, and payment is refunded. The transaction fee per party is reasonable, particularly for high-price products that guarantee successful shipment.

Keywords: smart logistics; smart contract; Ethereum; security and privacy; cargo shipment



Citation: Balfagih, M.; Balfagih, Z.; Lytras, M.D.; Alfawaz, K.M.; Alshdadi, A.A.; Alsolami, E. A Blockchain-Enabled IoT Logistics System for Efficient Tracking and Management of High-Price Shipments: A Resilient, Scalable and Sustainable Approach to Smart Cities. *Sustainability* **2023**, *15*, 13971. <https://doi.org/10.3390/su151813971>

Academic Editor: Socrates Basbas

Received: 9 July 2023

Revised: 10 September 2023

Accepted: 15 September 2023

Published: 20 September 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The employment of logistic services has been increasing in recent years, driven by a variety of factors including the growth of e-commerce and the need for flexible and agile supply chains. According to a report by Armstrong & Associates, the global market of third-party logistics providers was valued at approximately \$935 billion in 2020 and is expected to continue growing at a compound annual growth rate of around 6% through 2025 [1]. This trend is being driven by factors such as the rise of e-commerce and the need for companies to have more agile and flexible supply chains to meet the demands of online customers. In addition, the COVID-19 pandemic has also had an impact on the logistics industry, with many companies turning to third-party logistics to help them navigate disruptions in global trade and supply chains. The increased demand for third-party logistics services has been

particularly pronounced in sectors such as healthcare and pharmaceuticals, where the need for timely and reliable delivery of critical goods has been heightened.

Internet of Things (IoT) has been utilized in a variety of ways to improve efficiency, accuracy, and transparency in the supply chain. One common use of IoT in logistics is asset tracking and monitoring. By attaching sensors to shipping containers, pallets, or other assets, companies can track their location, temperature, humidity, and other factors in real-time. This information can be used to optimize routes, reduce spoilage, and ensure that goods are delivered on time and in good condition. However, while businesses may effectively manage their internal operations using centralized systems and individual local databases, there is still a need for increased transparency and trust among stakeholders in various processes [2]. For example, real-time tracking in supply chains can help reduce the wait for confirmation of information and improve efficiency. In addition, using a distributed system and disintermediating certain supply chain processes can enhance overall efficiency, particularly in cases of ownership or status changes between parties [3].

In this context, the integration between blockchain and IoT in smart contracts have been proposed to allow the creation of decentralized networks of devices that can autonomously carry out tasks and make decisions based on the data collected by the devices. The data collected by IoT devices can be securely and transparently recorded, ensuring the integrity and authenticity of the data. Smart contracts play a pivotal role in advancing smart cities, fostering efficiency, transparency, and security across urban logistics and infrastructure. They streamline supply chains, enabling faster deliveries and curbing congestion. Real-time tracking through IoT-linked contracts ensures timely deliveries. Automated payments benefit stakeholders such as drivers. Secure data exchange among parties boosts coordination. By digitizing agreements, smart contracts reduce manual paperwork. Optimized routing curtails congestion and improves fuel efficiency. Immutable contracts enhance trust, providing transparent records [4].

There have been several studies conducted on the integration of blockchain and IoT, with a focus on the potential applications and challenges of this integration. Some studies have identified the potential benefits of integration, such as improved security, transparency, and efficiency. However, there are also challenges to be addressed, such as reliability, interoperability, and privacy issues. This paper addresses these challenges by proposing a blockchain-based smart contract for automatic approval and payment with the consideration of distributing the shipping Information between legitimate logistics parties only. A zero-knowledge proof is utilized to conceal the blockchain address and verify the authentication. An intelligent Parcel (iParcel) containing piezoresistive sensors is also proposed for automatic tracking and tracing in which upon violation occurrence, the contract is cancelled and the payment is refunded. The main contributions of the paper can be summarized in the following:

- (i) A novel IoT-enabled parcel called iParcel for shipment tracking through the reading of GPS locations, and piezoresistive sensors to detect route change, opening, and severe falls. Although the explanation of how iParcel can be utilized in smart contract to ensure reliable shipment tracking has been presented, the detailed description of the iParcel was not presented.
- (ii) A privacy-preserving smart logistics contract using Ethereum blockchain for shipment supply chain management. The smart contract ensures that the distribution of shipment information remains between legitimate logistics parties only. This eliminates sharing personal data with third parties and distributing end users' personal information without permission.
- (iii) An implementation of the proposed system for a single echelon supply chain transaction between sender and receiver has been detailed, including the overall system architecture, party relations, and interactions among participating parties.

The rest of the paper is organized as follows: Section 2 discusses the related works and highlights the main difference between the proposed system and the existing systems; Section 3 details the proposed blockchain-enabled IoT logistics system including the archi-

texture and operation, iParcel, and smart contract; in Section 4, the implementation and the findings are discussed; finally, the paper is concluded.

2. Related Works

The application of IoT and blockchain in supply chain managements has attracted researchers in both academia and industry. The integration between these technologies is an enabler economy [5] and has been employed to improve supply chain management in different industries such as energy market [6], missile industry [7], agricultural food supply [8], healthcare [9,10], Industry 4.0, and Society 5.0 [11]. IoT technology could be used to convert the physical flow of the supply chain into a digital flow. IoT tools are used to acquire real-time data on product location, condition, and environment. Numerous IoT-based logistic systems have been proposed in the literature [12–17]. In contrast, blockchain technology is a potential solution for improving supply chain transparency, security, and traceability; however, there is still a need for further research to fully understand its implications and to develop best practices for its implementation [7].

The authors in [18] explored how blockchains and smart contracts can be used in IoT devices, discussing the benefits and restrictions associated with such applications. They concluded that incorporating blockchain and smart contract solutions in IoT ecosystems has made sharing IoT data and resources more convenient and has enabled the automation of slow workflows through cryptographically authenticated mechanisms. A blockchain-regulated, secure, verifiable, and automatic key refreshment mechanism for IoT systems has been proposed in [7] to enable users to verify the freshness of security keys being used. The proposed solution was implemented using Ethereum and Hyperledger Fabric blockchains. The authors carried out cost, scalability, and security analyses for performance evaluation. The results show that the proposed mechanism is economically viable and has strong security. However, the study has some limitations. It does not address all possible attack scenarios, which may limit its effectiveness in real-world scenarios. Additionally, the proposed solution may not be suitable for all types of IoT systems due to differences in system architecture and requirements.

An integrated Building Information Modeling BIM-IoT-Blockchain model has been proposed in [19] to help automate the monitoring process of mega complex infrastructure projects. It creates a Decentralized Common Data Environment (DCDE) for data management. This model would enable the real-time monitoring of construction projects, and improve construction supply chain management, construction asset management, and administration of smart construction contracts. The results show that the proposed BIM-IoT-Blockchain model can significantly improve the efficiency and transparency of construction projects. It can also reduce errors and delays by providing real-time monitoring and improved supply chain management. In [20], a solution that integrates blockchain and IoT technologies into the supply chain management system has been proposed to create a sustainable virtual closed-loop supply chain in E-commerce. The implementation of this solution involves developing an optimization model that considers the reduction of total supply chain costs, sustainability, circular economy, and the integration of blockchain and IoT technologies. The model also includes reselling, refurbishing, recycling, and disposing of products in a single framework to achieve circular economy and sustainability.

The authors in [11] aimed to address the limitations and challenges of using blockchain technology in industries, including scalability, energy consumption, security, and regulatory concerns. A blockchain-based solution was proposed to leverage artificial intelligence (AI) and the Internet of Things (IoT) for secure and efficient data sharing in various industries. The solution involves smart contracts for automated transactions and data integrity, and AI algorithms for optimized resource allocation and system performance improvement. The main limitation of the study is the suitability of the solution for different use cases or industries due to regulatory frameworks or technical requirements. Moreover, further evaluation of scalability and energy efficiency on a larger scale is required.

The potential of smart contracts using blockchain technology in improving transparency, security, and traceability in supply chain operations was also explored. In [21], a peer-to-peer transaction model was proposed based on blockchain for IoT operations, along with a technique for recording smart property and payment data transactions using smart contracts and smart coding. The authors in [9] investigated how blockchain technology can improve the IoT and suggest incorporating it into government infrastructures through regulations. It is expected that cryptocurrencies will become on par with fiduciary money in the future due to the integration of IoT and blockchain. A supply blockchain-based platform has been proposed in [7] to leverage Hyperledger Fabric to develop a proof-of-concept framework. The platform includes smart contracts to automate aspects of supply chain management and simulation software to model different scenarios for evaluation. Although the findings indicated that employing blockchain technology has the potential to improve supply chain transparency and reduce fraud risks through the real-time tracking of goods, it could face several challenges such as scalability and legal/regulatory concerns. The main limitation of the study is the focus on a single case study and the use of simulation software instead of real-world testing.

In [22], an IoT-blockchain-integrated, hospital-side-oriented Pharmaceutical Supply Chains (PSC) management model has been proposed with three layers: IoT-based physical data layer, blockchain-based data control layer, and data storage and management layer. The authors discussed how this model can enhance supply chain resilience through improved information sharing, traceability, security, and efficiency. A literature review was combined with semi-structured interviews to investigate PSC characteristics, key aspects affecting PSC, and challenges faced by PSC stakeholders for implementation. The authors provide a detailed description of the proposed model's architecture and components. The findings suggest that IoT-blockchain integration can enhance PSC resilience by enabling the real-time monitoring of drug quality and location, reducing counterfeiting risks, improving supply chain visibility and transparency, enhancing trust among stakeholders, and enabling efficient collaboration. However, limitations such as high implementation costs and interoperability issues between different systems or platforms used by different stakeholders in the supply chain should also be considered.

A smart cargo management and monitoring method using blockchain technology and UHF RFID has been proposed in [23] for faster and contactless traceability. Ethereum-based smart contract between the parties has been developed as an automatic payment and approval mechanism. However, the study focused only on local cargo distribution networks rather than global logistics networks within the supply chain. Additionally, further research is needed to evaluate the scalability and feasibility of this approach in real-world scenarios. A new federated, learning-enabled, blockchain-based framework has been developed in [24] that ensures the security and privacy of sensor-IoT-based architectures using sampled Electrochemical sensors (ECS) data. The performance of the framework has been evaluated in terms of the immutability and traceability of data. The findings revealed that the developed framework achieved high levels of security and privacy while maintaining data integrity. However, small-scale testing of the framework on a sensor network and the lack of evaluation in larger-scale deployments are the main limitations of the study. The authors also recognized that other factors beyond security and privacy could impact the effectiveness of the framework in real-world applications.

Table 1 summarizes the existing blockchain-enabled IoT logistics systems. While there have been previous studies on the integration of blockchain and IoT technologies, there are still gaps in the literature that call for further research to achieve comprehensive integration between the two technologies. Despite the potential benefits of IoT devices in providing real-time data on product location and condition, there are concerns about their vulnerability to cyber-attacks or data breaches, which can compromise the security and integrity of supply chain data. Furthermore, implementing blockchain technology poses challenges due to its complexity and high computational requirements. Issues with

reliability and privacy preservation of distribution information also arise in the context of blockchain integration with IoT technologies.

Table 1. A Summary of the most related blockchain-enabled IoT logistics systems.

Attributes	Sarkar, D. et al., 2023 [19]	Sezer B. et al., 2023 [24]	Prajapati, D. et al., 2022 [20]	Baygin M. et al., 2022 [23]	Chen, X. et al., 2023 [9]	Our Work
Data acquisition	RFID, temperature, humidity, and GPS	Not specified	Not specified	RFID, temperature, and GPS	RFID, temperature, humidity, and GPS	Piezoresistive and GPS
Communication technology	Not specified	Cellular networks	Not specified	WiFi or Cellular networks	Not specified	Cellular networks
IoT container	No	Yes	Yes	Yes	Yes	Yes
Distribution type	None	Single echelon	Multi echelon	Single echelon	Multi echelon	Single echelon
Smart contract	Yes	Yes	Yes	Yes	Yes	Yes
Privacy consideration	No	Yes	No	No	No	Yes
Application area	Construction project monitoring	Logistics	Supply chain	Logistics	Pharmaceutical supply chain	Logistics

3. Proposed Blockchain-Enabled IoT Logistics System

The proposed blockchain-enabled IoT logistics system monitors and tracks shipments through a sensory data flow during freight shipment from the source to the end destination. The following sub-sections describe the main components of the system in detail, including architecture and operation, iParcel, and smart contract.

3.1. Architecture and Operation Workflow

A multi-layer IoT architecture for the blockchain-enabled IoT logistics system is employed to meet the needs of freight shipment in the logistics industry. The architecture consists of three layers: the sensing layer, network layer, and application layer, as shown in Figure 1.

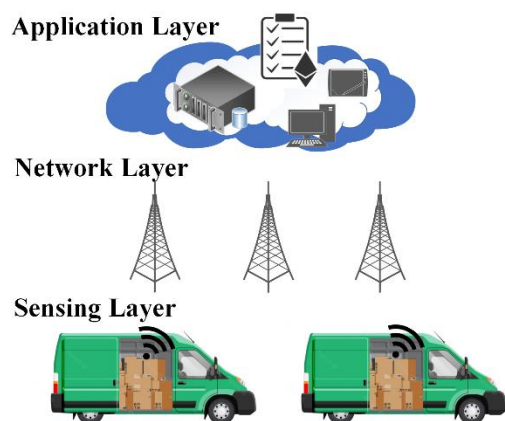


Figure 1. The architecture of the proposed blockchain-enabled IoT logistics system.

In the sensing layer, the system employs piezoresistive pressure sensors embedded in iParcel, and Global positioning System (GPS) to monitor and track shipments by detecting abnormal events such as heavy dropping or stealing. A battery is used to supply the power required for sensors. In the network layer, a cellular network is employed to notify the smart contract immediately upon an abnormal event detection, and upload the shipment ID, time, location, and event information to the application layer. Related information such as battery charge percentage and shipment status could also be included. The application layer is the highest layer, which includes the developed web-based online platform and smart contract. The platform is developed using the PHP programming language and communicates with a MySQL database to monitor the status of high-price shipments

during distribution. In contrast, smart contracts are computer programs that self-execute and identify the parties, their duties, and the payment mechanism between the parties. The platform and smart contracts receive related information transmitted by iParcel.

The workflow of smart contract and shipment distribution that is successfully completed without any violation event is shown in Figure 2. The system considers four main parties involved in the distribution process: sender, receiver, courier office, and distributors. All the parties participate in smart contracts in which each party has their own Ethereum address. The addresses are generated instantly without a centralized entity [25]. The proposed shipping model is single echelon, with a single sender and single recipient; however, it may be expanded to enable multi-echelon shipments, in which the receiver becomes the subsequent sender.

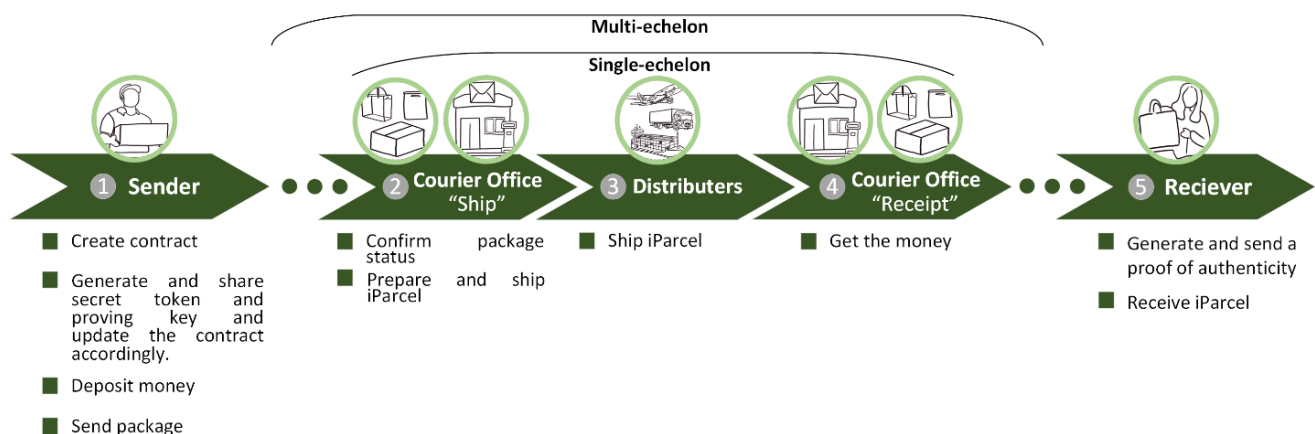


Figure 2. The workflow of proposed blockchain-enabled IoT logistics system.

3.2. Intelligent-Parcel (iParcel) Based on IoT

The proposed iParcel comprises of flexible sensing circuits containing piezoresistive pressure sensors (i.e., Uneo GD05, UNEO Inc., Taiwan) and a terminal hardware circuit comprised of a motherboard and a daughterboard. Flexible sensing circuits are connected to a terminal hardware circuit, which collects and analyses sensing data. The basic operation of piezoresistive sensors is based on variations in the resistance value of a material under mechanical stress, causing the output voltage signal to fluctuate with pressure. The violation events are detected by reading the GPS location to detect route change, and the readings of piezoresistive sensors to detect openings and severe falls of the iParcel. Cellular networks are used to notify the smart contract about violation occurrence.

3.3. Smart Contract

Smart contracts are computer programs that self-execute and identify the parties, their duties, and the payment mechanism between the parties. For each iParcel shipment, a separate smart contract can be created by either the sender or the courier office. As stated earlier, there are four main parties involved in the distribution process: sender, receiver, courier office, and iParcel. Figure 3 describes the operation of the proposed smart contract.

In the first process (1), the sender or the courier office initiates the shipment distribution by creating the smart contract, generating a secret token, and encrypting the next owner address A_{No} (i.e., the receiver address since the single echelon scenario is considered) to obtain $Enc(A_{No})$. The address is encrypted using elliptic curve ElGamal encryption, as presented in [26]. The sender completes the trusted setup by generating a proving key pair and employs Verifier Contract (VC) on the blockchain for proof confirmation. The zero-knowledge proofs (zk-SNARKs) are used in the trusted setup to generate the proving key pair, as specified in [27]. Then, the ciphertext of the next owner address $Enc(A_{No})$ and VC address are recorded in the smart contract. In the second process (2), the sender deposits the payment for shipping and hands over the package to the courier

office. The courier proceeds with the shipment process if the payment is successful, but it is cancelled otherwise. In the third process (3), upon receiving the goods from the sender, the courier office ensures that the package conditions are as specified in the contract. If the conditions are met, the package is approved, enclosed in iParcel, and shipped to the receiver. Otherwise, the package is aborted and the contract is cancelled.

Proposed Smart contract;

BEGIN;

(1) Create the contract by the sender or courier office

Sender or courier initiate the smart contract;

Generate a secret token, and encrypt the next owner address;

Generate proving-key and employ Verifier Contract (VC);

(2) Deposit the money by the sender

Deposit the payment to the smart contract;

If the payment successful and sufficient **then**

 The courier office proceeds with the shipment process;

Otherwise

 the shipment process will be cancelled;

end if;

(3) Package approving and shipping by the courier office

Confirm receiving the package;

If the package is as specified in the contract **then**

 Approve the package, prepare iParcel & initiate shipping process;

Otherwise

 The shipment is cancelled;

end if;

(4) Successful iParcel receiving

The receiver sends the proof once iParcel notifies about package arrival;

If the proof is verified **then**

 The smart contract notifies the courier office about iParcel receiving;

 Complete the payment and notify the sender and courier office;

Otherwise

 the shipment is cancelled;

end if;

(5) Violation events

iParcel notifies the smart contract about violation events;

If violation event occurred **then**

 The shipment is cancelled;

 The payment is refunded to the sender;

Otherwise

 Continue shipping;

end if;

END;

Figure 3. The operation of the proposed smart contract.

Upon the arrival of the package to the destination, as stated in process (4), the courier office will not release the shipment unless the receiver sends the correct proof based on the sender's shared proving key to the contract, which in turn verifies if the proof is valid and updates the recorded owner. Consequently, the payment will be released to the courier office. If a violation occurs during the shipment process, the shipment is canceled, and the sender is refunded. The smart contract ensures that the legitimate receiver receives the shipment. If a violation occurs, as described in process (5), the iParcel notifies the smart contract about the violation event. Accordingly, the contract is cancelled, and the payment is refunded to the sender. The violation criteria such as route, fall threshold, and payment terms are defined during contract creation.

The smart contract includes the following key elements: (i) variables that represent values and states reflecting the shipment state, type of violation, and the addresses of the involved parties, (ii) methods related to contract functionality that notify about violation events and authenticate the legitimate receiver, and (iii) events that are used to broadcast

information to all parties or record vital information on the ledger. Figure 4 shows the steps of smart contract and shipment distribution from the initiation until shipping. The details of the seven steps that are carried out among the parties are as follows:

1. **CreateContract():** The contract is created in this stage by the sender or the courier staff through the courier platform (i.e., courier application, website or management platform). However, the study will consider the scenario of creating the smart contract by the sender.
2. **TrustSetup():** Generate a secret token and encrypt the next owner address A_{No} to obtain $Enc(A_{No})$. Complete trusted setup and deploy verifier contract. Specify the receiver as $Enc(A_{No})$ and set the VC address as AVC . The method is called by the contract creator (i.e., sender or courier office).
3. **ShareKey():** Generate a proving key pair and employ Verifier Contract (VC) on the blockchain for proof confirmation. This method can also only be called by the contract creator.
4. **DepositMoney():** deposit the payment to the smart contract. If the payment is successful, the courier proceeds with the shipment process. Otherwise, the shipment process is cancelled. This method can only be called by the sender.
5. **PackageSent():** handing over the package to the courier office, which in turn ensures that the package conditions are as specified in the contract. This method can only be called by the courier office.
6. **PackageApproved():** confirm and check if the package is as specified in the contract. If it is not, the package will be rejected, and the contract will be cancelled; otherwise, the package will be approved. The method can only be called by the courier office.
7. **IparcelShipping():** prepare iParcel and initiate shipping process upon the package approving. This method can also only be called by the courier office.

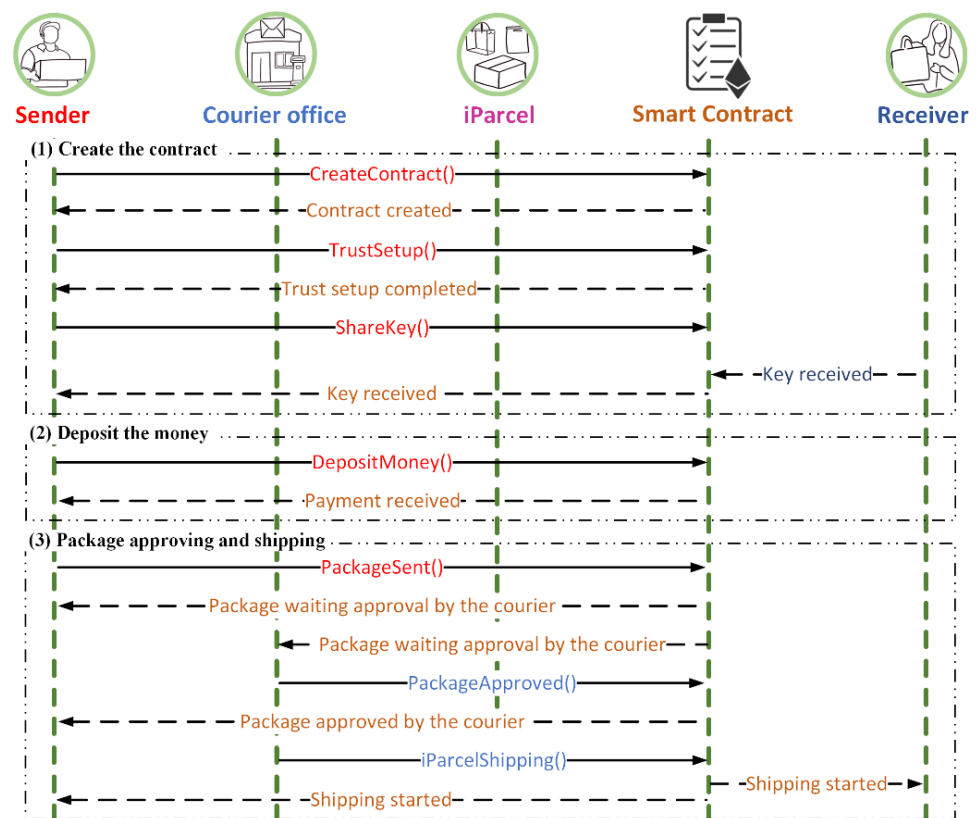


Figure 4. Messages sequence from contract creation until iParcel shipment start in the proposed blockchain-enabled IoT logistics system.

If the package is delivered successfully without any violation event, the steps shown in Figure 5 will be conducted. The details of these steps that are carried out among the parties are as follows:

1. iParcelArrived(): notify the receiver and the smart contract of iParcel arrival.
2. SendProof(): upon package arrival, the receiver generates proof based on the sender's shared proving key and delivers the proof to the smart contract, which in turn verifies if the proof is valid and updates the recorded owner to $Enc(A_{No})$.
3. GetMoney(): claim the money that has been deposited in the smart contract if the proof is verified. Once the payment is done, the sender and courier office will be notified.

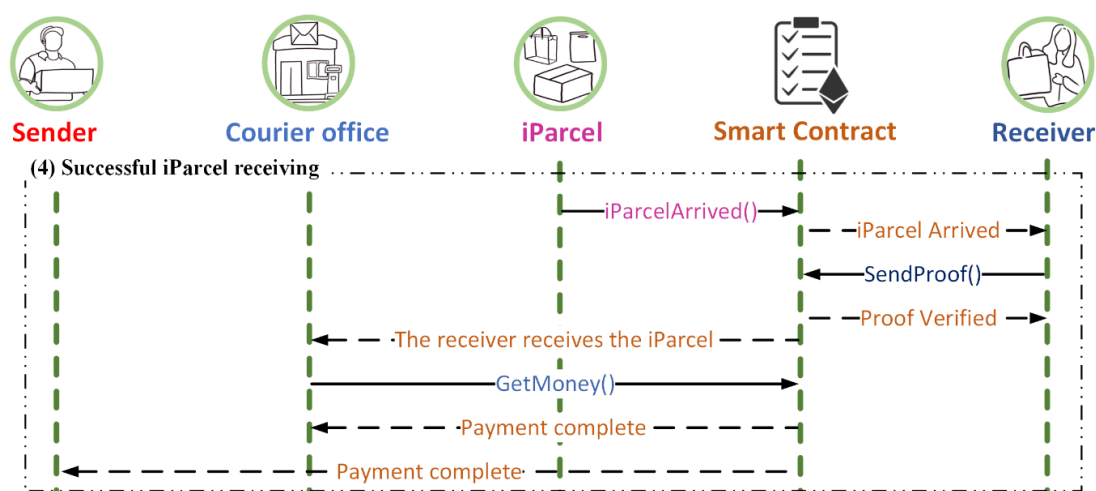


Figure 5. Messages Sequence of iParcel shipment with no violation.

The steps outlined above represent a successful shipment transfer between parties. However, unforeseen situations may arise at any point, including deposit failure, problem detection from iParcel, or authorization issues during shipment receipt. If a violation occurred during the shipment, the messages sequence shown in Figure 6 will be conducted as follows:

1. ViolationOccurred(): once a violation occurs, iParcel will notify the smart contract, which will in turn cancel the shipment and notify all parties.
2. GetMoney(): Because the shipment process is cancelled, the sender will get refund of the deposit money.

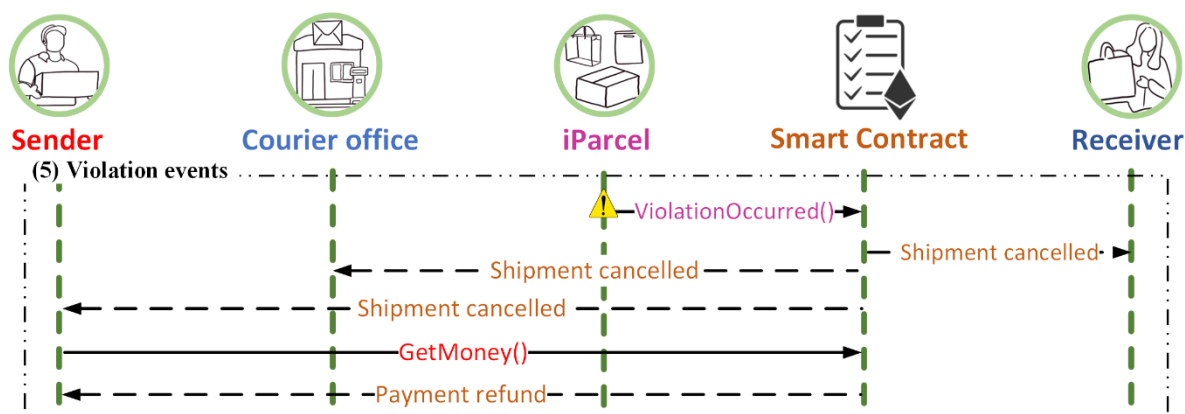


Figure 6. Message Sequence of iParcel shipment with Violation.

Different access permissions are allocated to the involved parties to facilitate the protection of privacy and possible attacks for inhibiting traceability. Figure 7 shows the access permissions to the shipment information of each party, in which access is prevented to unauthorized parties. This is achieved using the encrypted sender address and zero-knowledge proof. The security of the encrypted address could be granted using cryptographic security, which varies according to key length and cryptographic algorithm. It is extremely difficult to decrypt the encrypted address in a reasonable period if the private key is unknown. The suggested approach employs a 254-bit elliptic curve to assure the security of the encrypted address [28]. In contrast, since unauthorized parties are unable to extract data from the proof such as the address and the secret token, the proposed solution's zero-knowledge proof eliminates privacy breaches, including the sender's private address.

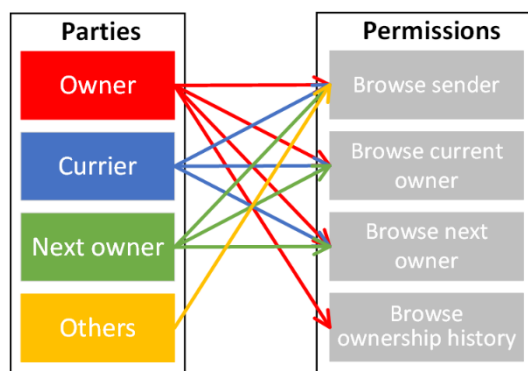


Figure 7. Access permissions to the shipment information of each party.

4. System Implementation and Results

Remix IDE has been used to implement and test the proposed system due to its rich features that enable testing and debugging smart contracts before deployment [29,30]. It comes with a built-in debugger that allows the investigation of various transactions to ensure the correct behavior of the contract in various conditions. Ethereum smart contracts were used due to their extensive documentation and their use in blockchain-based applications, and because Remix could provide multiple Ethereum wallets that allow simulating real-life scenarios. ZoKrates [31] was also used to implement zero-knowledge proof. However, several noteworthy alternatives to Ethereum are available in the blockchain landscape that could be used. Binance Smart Chain (BSC) stands out for its cost-effectiveness and rapid transactions, employing a unique Proof of Staked Authority consensus mechanism. Cardano (ADA) differentiates itself with its research-focused development approach and the Ouroboros Proof of Stake protocol, ensuring scalability and security. Solana (SOL) caters to speed, utilizing the Proof of History consensus for quick transaction finality. Polkadot (DOT) prioritizes interoperability by allowing different blockchains to operate in parallel through sharding. Lastly, Avalanche (AVAX) offers a secure environment for decentralized applications and financial projects, propelled by the Avalanche consensus for swift confirmation [32].

This section provides implementation details and primarily focuses on testing the correct functionality and interaction among system participants using the Ethereum smart contract.

4.1. Implementation Details

The code was written in the Solidity programming language, based on the code presented in [29], using Remix IDE and tested for the Ethereum blockchain [30]. Each of the four parties participating in the contract has an Ethereum address with an initial balance 100 ETH and can call methods in the smart contract using the modifiers that restrict methods calling to specific parties. For instance, CreateContract() can be called by the sender or

courier office only, and DepositMoney() can be called by the sender. The wallet addresses allocated to the parties are shown in Figure 8.



Figure 8. The wallet addresses allocated to the parties.

After creating the smart contract, the courier office, upon getting the item from the sender, checks if the item is as specified in the contract. The shipment is aborted if it is not as specified. Otherwise, the item is included in the iParcel and sealed. This ensures that the iParcel is trusted by all parties and operates flawlessly before shipment. The parcel state is maintained throughout the code to ensure the shipment’s logical flow. The enum variable named “packageState” is used to represent the parcel’s state. At the start of each method call, the current state of the parcel is checked, and based on the execution, any necessary state changes are made and updated. The new state is then communicated as an event to all Involved parties, allowing the next caller to act accordingly. Figure 9 shows the attributes of the smart contract code.

```
pragma solidity ^0.8.0;

contract iParcel {
    //participating entities with Ethereum addresses
    address public parcel;
    address public sender_owner;
    address public courier_office;
    address public receiver;
    string public content;
    bytes32 public passphrase;
    string public receivedCode;
    enum packageState {
        NotReady, PackageContainerReadyForSelfCheck, ReadyforShipment, MoneyDeposited,
        StartShipment, WaitingforPassphrase, ReceiverAuthenticated, WaitingForCorrectPasscode,
        ShipmentReceived, AuthenticationFailureAborted, Aborted
    }
    packageState public state;
    uint256 public startTime;
    uint256 public shipmentPrice;
    //sensors
    enum violationType {
        None, Heavydrop, Open, Route
    }
    violationType public violation;
    int256 public heavydrop; //if the parcel heavily dropped 1 , 0
    int256 public open; //if the container opens 1 , 0
    int256 public onTrack; //to track the route 1 , 0
}
```

Figure 9. The attributes of the smart contract code.

If any preidentified violation occurred after shipping, iParcel will call the function “violationOccurred(string, violationType, int)” with parameters including a string message for the triggered event, an enum for the violation type, and an integer for the violation value. This function then changes the state of the package to “Aborted” and issues a refund to the sender. Figure 10 displays the code that is executed by iParcel when a violation occurs. To verify the receiver’s authenticity when the shipment reaches its destination, the receiver generates proof based on the sender’s shared proving key and delivers the proof to the smart contract, which in turn verifies if the proof is valid and updates the recorded owner.

```

//after violation, a refund
function Refund() OnlyParcel {
    require(state == packageState.Aborted); //violation occurred
    if (violation != violationType.None) {
        receiver.transfer(shipmentPrice);
        ShipmentViolatedandRefund(msg.sender);
        selfdestruct(msg.sender);
    }
}

function violationOccurred(
    string msg,
    violationType v,
    int256 value
) OnlyParcel {
    require(state == packageState.StartShipment);
    violation = v;
    state = packageState.Aborted;
    if (violation == violationType.Heavydrop) {
        heavydrop = value;
        HeavydropViolation(msg, true, heavydrop);
    } else if (violation == violationType.Open) {
        open = value;
        SuddenContainerOpening(msg, true, open);
    } else if (violation == violationType.Route) {
        onTrack = value;
        OutofRoute(msg, true, onTrack);
    }
    Refund();
}

```

Figure 10. The smart contract code for iParcel when a violation occurs.

4.2. Results and Discussion

The proposed system is tested to validate the correct functionality based on four scenarios. The first scenario tests the successful shipment to ensure the correct state change of the package with the shipment flow and sequence. It also ensures that events and logs are updated accordingly. The results confirmed that the system does not execute any function before its turn or get called by the wrong party. For instance, an error occurs when the function `IparcelShipping()` is executed before approving the package as stated in the contract and executing `PackageApproved()`, as shown in Figure 11.



[vm] from: 0x369...8dc7f, to: browser/iParcel.sol:iParcel.IparcelShipping(bytes32) 0xde3...94b2c value: 0 wei data: 0x7bt...02k53 logs: 0 hash: 0xf34...a3439

Debug v

Transact to browser/iParcel.sol:iParcel.IparcelShipping(bytes32) errored: VM error.revert.revert The transaction has been reverted to the initial state. Debug the transaction to get more information.

Figure 11. Error message due to shipping package before approval.

The second scenario examines the detection of violations and errors. For instance, if iParcel is dropped heavily or opened, the function `ViolationOccurred()` is called and the message “the shipment is aborted” will be written in the log, as shown in Figure 12. If the function `DepositMoney()` is not executed successfully because the money is not deposited yet or deposited money is less than the shipment price, the log will have the message “Money deposited is insufficient”.

logs	 [<pre> { "topic": "8ds85h899k53a89df3k126pp566sdsg0n99m8ff f35677115a011kdfm5886re", "event": "HeavyDropViolation", "args": ["the shipment is aborted", "true", "heavydrop"] } </pre>]
------	--

Figure 12. Violation is detected and HeavyDropViolation event is triggered.

The third scenario tests the privacy preservation of distribution information to ensure that any party not involved in the product distribution cannot know any distribution information. The distribution information is encrypted; hence, any party not involved in the product distribution does not have the means of decryption. This indicates that the proposed system is able to preserve the privacy of distribution information. Finally, the fourth scenario tests the verification process of the receiver's authenticity and the update of the owner record. The package will be released once the smart contract gets the correct proof based on the sender's shared proving key from the receiver. Consequently, the recorded owner will be updated to $Enc(A_{No})$ and the event Receiver-AuthenticatedSuccessfully will be triggered with the message "Authenticated successfully", as shown in Figure 13. The package is not released if the receiver failed to provide the correct proof, which indicates that the proposed method is able to authorize and release the package successfully.

logs	 [<pre> { "topic": "8e750ffe3450da86mc778xx998jddfl997730urfg9455okm n44822dsei86", "event": "ReceiverAuthenticatedSuccessfully", "args": ["Authenticated successfully", "0xD12333dbDD035c2654E9d785Ba6aDa0D1f52 f059"] } </pre>]
------	--

Figure 13. The receiver is authenticated and ReceiverAuthenticatedSuccessfully is triggered.

The transaction cost per party in the first and second scenarios was also evaluated. The transaction cost was calculated by multiplying the output value per unit by the gas price, which were then converted into USD. Gas unit is a measurement of the computational work necessary to implement contracts on the Ethereum blockchain platform. The gas price was 20.19×10^{-6} USD per gas at time of evaluation on 27 November 2022 at 22:05 (EST). The maximum transaction charge in the contract differs between parties because each party executes different processes. Different functions are executed by each party to implement the shipping process in which the proof process is implemented utilizing zero-knowledge proof. The transaction costs differ from one party to another, which reflects the different functions and the instructional complexity and data size conducted by each party. The transaction cost per party in the first scenario is shown in Figure 14.

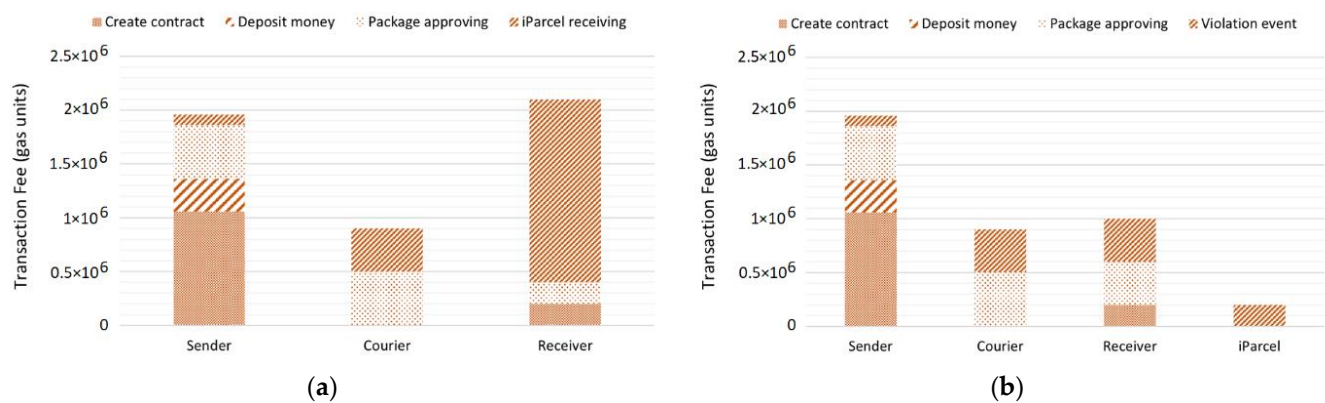


Figure 14. Transaction cost per party in (a) successful shipment scenario, and (b) violation event scenario.

The results show that the transaction paid by the receiver was higher than other parties. This is because the shipping–receiving process has high complexity compared to the creating contract process. The total transaction fees for sender, receiver, and courier office are 1.96×10^6 , 2.1×10^6 , and 0.9×10^6 gas units, respectively. This is equal to the range between 16.15 and 42.40 USD at the time of evaluation. In contrast, for the transaction cost in the second scenario (i.e., violation occurrence), the sender has the highest cost because the enrollment process was conducted only. The total transaction fees for sender, receiver, courier office, and iParcel are 1.96×10^6 , 1×10^6 , 0.9×10^6 , and 0.2×10^6 gas units, respectively. This is equal to the range between 4.1 and 39.57 USD at the time of evaluation. Such fees are reasonable charges in the payment of guaranteed successful shipment, especially with high-price products such as automobiles and large home appliances.

The proposed system addresses privacy preservation, cyber-attack vulnerabilities, and data breaches, but requires significant computational resources for shipments. It has not been extensively tested for scalability and energy efficiency in large deployments. Moreover, the evaluation does not cover all potential attack scenarios, potentially limiting its real-world effectiveness. Our work's limitation is summarized by the research context, which is a prototype environment designed to respond to real-world problem challenges within the principles and conditions of scientific research. The innovative approach we introduced in this research is a showcase, a bold case study for the capacity of emerging technologies such as Internet of Things and blockchain to support novel, sophisticated implementations for the efficient tracking and management of shipments with cost-fair methodologies that are scalable and robust. In a greater context, this blockchain prototype challenges the regulatory framework for the adoption of blockchain and IoT and the need to provide a transparent financial system. In other words, our application is also limited in the sense that while it delivers the core business and the main objectives of its design, it requires additional adjustments for a fully scalable platform capable of addressing all the requirements of the regulatory framework. At the moment, these frameworks are under development by the government and the supervising authorities.

The key implications of our research are summarized as follows:

Efficiency: The proposed methodology and proposed installation of the blockchain-based IoT logistic systems for efficient tracking and management of shipments leads to a fully secure, trusted, cost-fair, and efficient solution capable of improving the management of high-value shipments in the context of smart cities and global trade.

Scalability: Our research communicated a fully scalable and integrated approach, which means that it can be applied in the context of any smart transportation and supply chain management projects in a smart city at a global scale. This leads to the sustainability of implementation. The algorithms that power our approach can also serve a bid data smart logistics ecosystem, where more sophisticated analysis and analytics methods for

enhanced decision making can be executed. In our research in this paper, we focused on the efficient tracking and management of high-value shipments; in the future, we intend to also focus on the proactive analysis towards optimization and additional value-adding analytical services. This will lead to a sophisticated holistic approach to management of efficient tracking and management of shipments. The integration of this system to AI-enabled intelligent agents can also significantly promote a novel industry of data-driven and blockchain-enabled secure e-marketplaces of shipment management.

Extensibility: Our methodology and implementation can be extended to other various phases of the logistics lifecycle that include the value-adding stages of efficient tracking and management of shipments. As we discussed in the previous paragraph, phases such as utilization or scheduling can be integrated in our methodological approach by extending the lifecycle of the logistics lifecycle and by providing rich data for sophisticated analysis and enhanced decision making.

The key findings that are summarized in the previous section also provide evidence for a strategic interpretation. The first bold interpretation is that modern applied sciences and robust information processing capabilities can empower smart logistics systems that enhance sustainable and resilient economic development. Our interdisciplinary research proved that the deployment of the blockchain-based IoT logistics system for efficient tracking and management of shipments can significantly improve the capacity of systems to enhance the unique value proposition of smart logistics applications in the areas of commerce, supply chain efficiency, and traffic management, including financial management.

Another key implication of our research is related to the data intensity and the network capability of smart logistics systems for the efficient tracking and management of high-value shipments. Our methodological approach proved that it is feasible to set up scalable and integrated units of processing to shipments and to manage them effectively. It is obvious that a scalable approach to this phenomenon to cover the entire Smart Logistics context will require significant data processing, network capacity, and IoT capabilities. In our opinion, these resources are available nowadays, so the design and implementation of integrated systems for the efficient tracking and management of shipments in smart cities is feasible and can exploit our unique value propositions.

One more significant implication is that systems similar to ours that utilize machine-generated and managed data through IoT and blockchain applications can be enhanced with complementary methodologies and approaches. One direction that summarizes one proposition is that AI-enabled applications for end-to-end logistics management can likely accompany our methodology by integrating production and supply-driven data that will enhance the overall efficiency of logistics in the context of smart cities.

Another bold proposition of our research is that the IoT data ecosystem in the context of smart logistics can support parallel diverse objectives and can significantly enhance the decision-making capability related to bold problems and challenges of supply chain management, such as tracking efficiency, smart pricing, and sophisticated security management. This implies that there is also a requirement from policy making of view for integrated actions such as:

- Regulations for the standardization of blockchain-based IoT data generation for smart logistics and shipment management.
- Regulations and policies for the integration of such secure systems in the financial system towards embedded systems of IoT services that will adopt same standards, making the adoption of sophisticated shipment management systems easier in the core of smart cities infrastructures.
- Policy guidelines for blockchain IoT-enabled intelligence for secure and trusted logistics and financial systems and fraud avoidance.

It is also obvious from our unique, resilient approach that there is a lot of space for Artificial Intelligence-enabled enhancement of our approach. This is another future research direction that we intend to undertake in the near future.

5. Conclusions and Future Works

This paper focused on developing a smart and secure logistics system to manage the growing logistics volume efficiently. The system is designed to ensure the quality and safe delivery of high-price goods while maintaining privacy. To achieve this, a smart contract based on blockchain was developed for automatic approval and payment with the consideration of distributing the shipping information between legitimate logistics parties only. A zero-knowledge proof was used to conceal the blockchain address and prove the authentication. Moreover, an intelligent parcel (iParcel) with piezoresistive sensors is used for violation detection during the shipping process. The iParcel automatically tracks and traces the delivery, and in case of any violation, the transaction is cancelled, and the payment is refunded. By implementing this smart logistics system, the distribution of high-price goods can be managed effectively with traceability and condition monitoring capabilities. Successful shipment and violation occurrence scenarios were implemented. The transaction fees range between 16.15 and 42.40 USD for the first scenario and between 4.1 and 39.57 USD for the second scenario. The transaction fee per party is reasonable for high-price products in the payment of guaranteed successful shipment. Although the work described a logistic system based on the integration between blockchain and IoT in detail, only a single echelon scenario was illustrated. The system could be easily extended for multi-echelon scenarios where the receiver becomes the subsequent sender. In addition, the iParcel will be fabricated and tested to investigate violation detection accuracy.

Our research paper contributes significantly to the theory of Smart Logistics and smart cities, with a focus on the efficient, intelligent, and secure management of growing logistics volumes. It also contributed to the practice and the applied sciences by providing a cost-effective pilot system that is fully scalable and extended. This can potentially lead to a patent and commercialization through technology transfer and startup business that will specialize in this very delicate and sensitive research problem of the smart logistics industry. As it was also communicated in the previous section, additional future research is related to the integration of Artificial Intelligence for the orchestration of the decision-making capability of the entire production and logistics lifecycle, as well as the analysis of big data analytics and infrastructure for a holistic smart logistics application for materials and financial management. The limitation of our work is summarized by the research context itself, which is a prototype environment under the principles and the conditions of scientific research that responds to real world problems and challenges. Issues with reliability and privacy preservation of distribution information could be raised in the context of blockchain integration with IoT technologies. Also, in our work, we focused on a very specific research problem. The visualization of smart cities [33] requires integration of this kind of solution to an integrated marketplace of services that add value to the industrial and the financial value chain. Thus, the integration of our approach to one-stop-shop services available to businesses and users is necessary. Last but not least, our solution can be a bold enabler of the New Silk Road, as it is connected to the Gulf Cooperation Council Countries. The provision of fully secured services can also promote the value perception of high-profit-margin transactions contributing to customer loyalty and trust; this can be another direction also for our future research.

Author Contributions: Conceptualization, M.B., Z.B. and A.A.A.; methodology, M.B., Z.B., M.D.L. and K.M.A.; software, M.B., Z.B. and K.M.A.; validation, M.B., Z.B. and M.D.L.; investigation, M.B., Z.B., M.D.L., K.M.A. and E.A.; writing—original draft preparation, M.B., Z.B. and M.D.L.; writing—review and editing, A.A.A., K.M.A. and E.A.; visualization, M.B.; project administration, A.A.A. and E.A.; funding acquisition, M.B. and A.A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by the University of Jeddah, Jeddah, Saudi Arabia, under grant No. (UJ-21-ICL-1). Therefore, the authors acknowledge the University of Jeddah with thanks for technical and financial support.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Armstrong & Associates. Global Third-Party Logistics Market Size Estimates. 2021. Available online: <https://www.3plogistics.com/3pl-market-info-resources/3pl-market-information/global-3pl-market-size-estimates/> (accessed on 11 September 2023).
2. Vigna, P.; Casey, M.J. *The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order*; Macmillan: New York, NY, USA, 2016.
3. Cecere, L. Moving blockchain forward: Seven use cases for hyperledger in supply chain. *Supply Chain. Q.* **2017**. Available online: <https://www.supplychainquarterly.com/articles/1359-moving-blockchain-forward-seven-use-cases-for-hyperledger-in-supply-chain> (accessed on 11 September 2023).
4. Treiblmaier, H.; Rejeb, A.; Strebing, A. Blockchain as a driver for smart city development: Application fields and a comprehensive research agenda. *Smart Cities* **2020**, *3*, 853–872. [\[CrossRef\]](#)
5. Pennino, D.; Pizzonia, M.; Vitaletti, A.; Zecchini, M. Blockchain as IoT Economy enabler: A review of architectural aspects. *J. Sens. Actuator Netw.* **2022**, *11*, 20. [\[CrossRef\]](#)
6. Afanasyev, V.Y.; Lyubimova, N.G.; Ukolov, V.F.; Shayakhmetov, S.R. Impact of blockchain technology for modification of the supply chain management in energy markets. *Int. J. Supply Chain. Manag.* **2020**, *9*, 757–762.
7. Cerchione, R.; Centobelli, P.; Angelino, A. Blockchain-based IoT model and experimental platform design in the defence supply chain. *IEEE Internet Things J.* **2023**. [\[CrossRef\]](#)
8. Jahanbin, P. The Investigation of Blockchain and IoT Integration for Designing Trust-Driven Information Systems in Agricultural Food Supply Chain. Ph.D. Thesis, University of Canterbury, Canterbury, UK, 2022.
9. Chen, X.; He, C.; Chen, Y.; Xie, Z. Internet of Things (IoT)—Blockchain-enabled pharmaceutical supply chain resilience in the post-pandemic era. *Front. Eng. Manag.* **2023**, *10*, 82–95. [\[CrossRef\]](#)
10. Rahman, M.S.; Islam, M.A.; Uddin, M.A.; Stea, G. A survey of blockchain-based IoT eHealthcare: Applications, research issues, and challenges. *Internet Things* **2022**, *19*, 100551. [\[CrossRef\]](#)
11. Tyagi, A.K.; Dananjayan, S.; Agarwal, D.; Thariq Ahmed, H.F. Blockchain—Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0. *Sensors* **2023**, *23*, 947. [\[CrossRef\]](#) [\[PubMed\]](#)
12. Chang, W.J.; Chen, L.B.; Su, J.P. Design and implementation of intelligent tape for monitoring high-price and fragile cargo shipments during transport procedures. *IEEE Sens. J.* **2020**, *20*, 14521–14533. [\[CrossRef\]](#)
13. Alyousifi, Y.; Othman, M.; Almohammed, A.A. A novel stochastic fuzzy time series forecasting model based on a new partition method. *IEEE Access* **2021**, *9*, 80236–80252. [\[CrossRef\]](#)
14. Balfaqih, M.; Ismail, M.; Nordin, R.; Balfaqih, Z. Handover performance analysis of distributed mobility management in vehicular networks. In Proceedings of the 2015 IEEE 12th Malaysia International Conference on Communications (MICC), Kuching, Malaysia, 23–25 November 2015; pp. 145–150.
15. Yusof, M.H.M.; Abd Khalid, I. Precision education reviews: A case study on predicting student's performance using feed forward neural network. In Proceedings of the 2021 International Conference of Technology, Science and Administration (ICTSA), Taiz, Yemen, 22–24 March 2021; pp. 1–4.
16. Gaid, A.S.; Qaid, O.A.; Alhakimi, A.M. Microstrip antennas for next generation wireless devices. In Proceedings of the 2019 First International Conference of Intelligent Computing and Engineering (ICOICE), Hadhramout, Yemen, 15–16 December 2019; pp. 1–4.
17. Sergi, I.; Montanaro, T.; Benvenuto, F.L.; Patrono, L. A smart and secure logistics system based on IoT and cloud technologies. *Sensors* **2021**, *21*, 2231. [\[CrossRef\]](#) [\[PubMed\]](#)
18. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the internet of things. *IEEE Access* **2016**, *4*, 2292–2303. [\[CrossRef\]](#)
19. Sarkar, D.; Dhaneshwar, D.; Raval, P. Automation in Monitoring of Construction Projects Through BIM-IoT-Blockchain Model. *J. Inst. Eng. (India) Ser. A* **2023**, *104*, 317–333. [\[CrossRef\]](#)
20. Prajapati, D.; Jauhar, S.K.; Gunasekaran, A.; Kamble, S.S.; Pratap, S. Blockchain and IoT embedded sustainable virtual closed-loop supply chain in E-commerce towards the circular economy. *Comput. Ind. Eng.* **2022**, *172*, 108530. [\[CrossRef\]](#)
21. Zhang, Y.; Wen, J. An IoT electric business model based on the protocol of bitcoin. In Proceedings of the 2015 18th International Conference on Intelligence in Next Generation Networks, Paris, France, 17–19 February 2015; pp. 187–191.
22. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *88*, 173–190. [\[CrossRef\]](#)
23. Baygin, M.; Yaman, O.; Baygin, N.; Karakose, M. A blockchain-based approach to smart cargo transportation using UHF RFID. *Expert Syst. Appl.* **2022**, *188*, 116030. [\[CrossRef\]](#)
24. Sezer, B.B.; Turkmen, H.; Nuriyev, U. PPFchain: A novel framework privacy-preserving blockchain-based federated learning method for sensor networks. *Internet Things* **2023**, *22*, 100781. [\[CrossRef\]](#)

25. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [[CrossRef](#)]
26. Uesugi, T.; Shijo, Y.; Murata, M. Design and evaluation of a privacy-preserving supply chain system based on public permissionless blockchain. In Proceedings of the ISEEIE 2021: 2021 International Symposium on Electrical, Electronics and Information Engineering, Seoul, Republic of Korea, 19–21 February 2021; pp. 312–321. [[CrossRef](#)]
27. Pinto, A.M. An introduction to the use of zk-SNARKs in blockchains. In *Mathematical Research for Blockchain Economy*; Springer: Cham, Switzerland, 2020; pp. 233–249.
28. WhiteHat, B.; Baylina, J.; Bellés, M. Baby Jubjub Elliptic Curve. Ethereum Improvement Proposal, EIP-2494, 29, 2020. Available online: <https://eips.ethereum.org/EIPS/eip-2494> (accessed on 11 September 2023).
29. Solidity. Available online: <https://solidity.readthedocs.io/> (accessed on 17 March 2020).
30. Remix—Ethereum IDE. Available online: <https://remix.ethereum.org> (accessed on 17 March 2020).
31. ZoKrates. Available online: <https://github.com/Zokrates/ZoKrates> (accessed on 17 March 2020).
32. Busayatananphon, C.; Boonchieng, E. Financial technology DeFi protocol: A review. In Proceedings of the 2022 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON), Online, 26–28 January 2022; pp. 267–272.
33. Visvizi, A.; Lytras, M.D. Sustainable Smart Cities and Smart Villages Research: Rethinking Security, Safety, Well-being, and Happiness. *Sustainability* **2020**, *12*, 215. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.