OPEN ACCESS JOURNALS
Indiana Journal of Multidisciplinary Research
Abbreviated Tittle- Ind J Multi Res
ISSN *(Online)*- 2583-3820
Journal Homepage Link- https://indianapublications.com/Journals/IJMR
DOI: https://doi.org/10.5281/zenodo.21604687

INDIANA PUBLICATIONS
PRODUCTIVE AND QUALITY RESEARCH

Research Article

Volume-06|Issue-04|2026

Blockchain Privacy in Supply Chains

Sunit Bhagwan Moorjani & Dr. V. R. Palanivelu

[1]Sunit Bhagwan Moorjani, Part-time Ph.D. Research Scholar, Department of Management Studies, Periyar University, Salem – 636011, Tamil Nadu, India.
[2]Research Supervisor and Professor, Department of Management Studies, Periyar University, Salem – 636011, Tamil Nadu, India.

Article History
Received: 05.05.2026
Accepted: 22.06.2026
Published: 25.07.2026

Citation
Moorjani, S. B. & Palanivelu, V. R. (2026) Blockchain Privacy in Supply Chains. *Indiana Journal of Multidisciplinary Research, 6*(4), 253-260.

Abstract: Product traceability within supply chains is a critical concern that has gained increasing attention in recent years. One promising solution to this problem is the use of Public Blockchain (PBC) technology, which offers an immutable, transparent, and decentralized ledger for storing key information such as ownership transfers and distribution records. These blockchain-based systems significantly enhance traceability by ensuring that data, once recorded, cannot be altered. However, a key challenge arises from the fact that information stored on public blockchains is freely accessible to anyone, potentially exposing sensitive distribution data.

In this paper, I introduce a novel method that preserves the privacy of distribution data while maintaining high traceability in supply chain systems leveraging PBC. The proposed method utilizes encryption to safeguard sensitive data and Zero-Knowledge Proofs (ZKPs) to allow supply chain participants to authenticate themselves without revealing private information, such as their blockchain addresses.

The solution was implemented using Ethereum smart contracts and evaluated for its cost-effectiveness. The results show that the transaction fee per supply chain participant is capped at USD 2.6, demonstrating that the approach is practical for real-world deployment.

Keywords: Blockchain, Supply Chain, Privacy Preservation, Zero-Knowledge Proofs, Smart Contracts, Product Traceability, Public Blockchain, Ethereum.

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (**CC BY-NC 4.0**).

INTRODUCTION

The increasing globalization and complexity of modern supply chains have introduced significant challenges in ensuring reliable product traceability. A major consequence of this trend has been the alarming rise in counterfeit goods circulating within global markets. According to a comprehensive study conducted by the Organisation for Economic Co-operation and Development (OECD), in collaboration with the European Union Intellectual Property Office (EUIPO), the estimated value of counterfeit and pirated goods in international trade reached approximately USD 509 billion in 2016. This marked a notable increase from USD 461 billion reported in 2013 [1]. Such proliferation of fraudulent products not only results in substantial economic losses for legitimate businesses but also poses serious risks to consumer health and safety, particularly when counterfeit products include pharmaceuticals, electronics, or food items.

Beyond the economic implications, the intricate nature of global supply networks has further compounded traceability issues, making it increasingly difficult to identify the origin of specific components or ingredients in the event of a quality control failure or health hazard. A prominent example illustrating the severity of such challenges is the 2015 outbreak of *Escherichia coli* (*E. coli*) linked to the restaurant chain Chipotle Mexican Grill. The incident, which affected dozens of customers across multiple U.S. states, highlighted the company's inability to identify and isolate the contaminated ingredient due to limitations in its supply chain traceability mechanisms [2]. Such incidents emphasize the urgent need for more transparent, resilient, and technologically advanced solutions to improve accountability and safety throughout supply chains.

In response to these challenges, blockchain technology has emerged as a promising approach for enhancing product traceability.

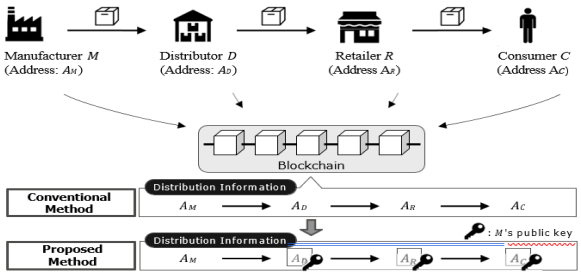

Fig. 1. Comparison between conventional blockchain-based supply chain systems and the proposed privacy-preserving method.

***Corresponding Author:** Dr. V. R. Palanivelu

Public blockchains, in particular, have been proposed as decentralized platforms for recording distribution data such as ownership transfers, ensuring that records remain immutable and transparent. Blockchain-based systems have the potential to prevent fraud and improve visibility into product journeys from manufacturing to consumption [3]–[5]. These systems utilize smart contracts to enforce business rules, thereby preventing fraudulent registrations and ensuring that blockchain records remain tamper-proof.

While blockchain transparency offers many advantages, it also introduces significant privacy concerns. In a PBC-based system, sensitive business information, including distribution relationships and ownership transfers, is accessible to anyone querying the blockchain. For many organizations, this exposure of confidential information presents a substantial risk, particularly when distribution records reveal strategic details such as supplier relationships and pricing structures.

To address these privacy concerns, this paper proposes a novel method that enables secure product traceability while safeguarding sensitive distribution data. The proposed approach encrypts sensitive information, including blockchain addresses, using the manufacturer's public key, ensuring that only authorized parties can decrypt the data. Furthermore, the method employs Zero-Knowledge Proofs (ZKPs) to allow supply chain participants to authenticate themselves without revealing private information, including their blockchain addresses. This approach preserves privacy while maintaining the integrity and traceability of the supply chain.

The remainder of this paper is organized as follows. Section II reviews related work on blockchain-based supply chain systems. Section III presents the proposed privacy-preserving method in detail. Section IV verifies the proposed method with respect to privacy preservation and traceability. Section V describes the experimental setup and evaluation results, including transaction costs. Finally, Section VI concludes the paper and outlines directions for future research.

MATERIALS AND METHODS

Related Work

Over the past decade, several blockchain-based systems have been proposed to improve product traceability within supply chains. Toyoda *et al.* [3] introduced the Product Ownership Management System (POMS), which utilizes blockchain technology to manage product ownership, thereby preventing counterfeit product distribution while maintaining transparent and immutable records. The system tracks products throughout the supply chain and provides real-time visibility to all stakeholders.

Kim *et al.* [4] proposed a method for tracking products at the raw materials stage using Traceable Resource Units (TRUs). This approach enables the origin and movement of raw materials to be monitored throughout the supply chain, thereby improving production transparency.

Huang *et al.* [5] developed a blockchain-based solution specifically for food supply chains, where high-frequency distribution events are common. By integrating off-chain technology with blockchain, the proposed system improves scalability and efficiency, making it more suitable for industries requiring continuous product distribution and traceability.

Despite these advances, privacy concerns have received comparatively little attention. Most existing systems, including POMS, store blockchain addresses and transaction data directly on the blockchain, making sensitive distribution information publicly accessible. Although blockchain ensures transparency, the public availability of such data compromises business confidentiality. This important issue remains insufficiently addressed in the existing literature.

Proposed Method

In this paper, I propose an enhancement to the POMS system [3] that addresses the privacy concerns associated with public blockchain-based supply chain systems. The proposed method ensures that sensitive distribution information remains private while preserving the traceability and immutability benefits of blockchain. Specifically, the proposed method includes the following components:

- **Encryption of Blockchain Addresses:** The manufacturer's public key is used to encrypt blockchain addresses before they are stored on the public blockchain. This ensures that only the manufacturer, who possesses the corresponding private key, can decrypt and access the list of blockchain addresses.
- **Zero-Knowledge Proofs (ZKPs):** Supply chain participants (e.g., manufacturers, distributors, and retailers) must prove their authenticity when shipping and receiving products. Using ZKPs, they can demonstrate knowledge of a secret token proving that they are legitimate participants without revealing any sensitive information, such as their blockchain addresses.

The proposed method consists of three key components:

- **Manufacturer-Manager Contract (MMC):** This contract manages the manufacturer's information, including public keys and the products they manufacture.
- **Products Manager Contract (PMC):** This contract tracks product ownership and distribution events. It stores encrypted blockchain addresses, ensuring that only authorized parties can access them.
- **Verifier Contract (VC):** This contract verifies Zero-Knowledge Proofs, ensuring that only legitimate supply chain participants can take part in the distribution process.

***Corresponding Author:** Dr. V. R. Palanivelu

The proposed method ensures that only legitimate supply chain participants can track products while preserving the privacy of their blockchain addresses.

The proposed method was implemented on the Ethereum blockchain to evaluate its performance. The evaluation consists of two main aspects:

1. The privacy-preserving features of the proposed method.
2. The cost-effectiveness of the proposed method, specifically the transaction fees.

To evaluate privacy preservation, the method was tested to verify that blockchain addresses were successfully encrypted and that only authorized parties could access the distribution data. The use of Zero-Knowledge Proofs was also evaluated to ensure that only legitimate participants could authenticate themselves.

The cost evaluation focused on the transaction fees associated with executing the smart contracts. The results indicate that the transaction fee per participant is capped at USD 2.6, making the proposed method practical for real-world supply chain applications.

This paper presents a privacy-preserving method for securing traceability in blockchain-based supply chain systems. Encrypting blockchain addresses and utilizing Zero-Knowledge Proofs protects sensitive distribution information while ensuring that only legitimate participants can access and manage the data. The solution was implemented on the Ethereum blockchain and demonstrated its effectiveness in terms of privacy preservation and cost efficiency. The results show that the proposed method is both feasible and effective for real-world supply chain applications. Future work will focus on further improving scalability, reducing transaction costs, and exploring applications across a wider range of industrial sectors.

Preparation for Distribution

Before initiating the distribution process of any product within the system, it is essential to establish the identity of the manufacturer through a dedicated registration process in the Manufacturer-Manager Contract (MMC). This step is critical for maintaining the integrity and traceability of the supply chain. At the core of this registration procedure is the association of two distinct and mandatory identifiers: the manufacturer's blockchain wallet address and its corresponding public cryptographic key. Together, these two components serve as a digital fingerprint, uniquely identifying each manufacturer and enabling secure interactions within the decentralized infrastructure.

This identity framework is not only essential for authentication but also plays a significant role in ensuring accountability and data transparency throughout the product lifecycle. The association between the blockchain address and the public key guarantees that all future transactions or actions performed by the manufacturer can be securely validated and traced back to the originating entity.

Moreover, the registration process allows the inclusion of supplementary metadata, such as the manufacturer's official name and contact number. Although these additional details are optional, they provide a convenient human-readable layer of information that can be beneficial for administrative purposes or customer service interactions. By incorporating these optional fields, the system achieves a balance between strong cryptographic security and practical usability, facilitating efficient manufacturer onboarding without compromising system robustness.

The process of registering a manufacturer's details within the MMC is secure, and only a designated administrator is authorized to perform this operation. For example, organizations such as GS1 [6], a globally recognized non-profit organization responsible for developing and maintaining supply chain standards, can perform this registration process. Furthermore, the MMC not only manages manufacturer information but also establishes an association between the manufacturer's blockchain address and the products it manufactures. This relationship ensures that every product can be traced back to its original manufacturer, thereby providing transparency and accountability throughout the product lifecycle.

Product Registration

To maintain the accuracy and reliability of product ownership tracking within the supply chain, only legitimate and verified manufacturers are permitted to register products in the Products Manager Contract (PMC). This legitimacy is established through prior registration in the Manufacturer-Manager Contract (MMC), which serves as a prerequisite and prevents unauthorized entities from manipulating ownership records.

Once a manufacturer has been successfully authenticated and registered in the MMC, it gains the exclusive authority to register its manufactured products within the PMC. This registration process involves providing comprehensive product metadata, including serial numbers, model information, production batch details, and timestamps, thereby establishing a formal and immutable record of the product's origin and its association with the manufacturer.

The product registration process serves two important purposes. First, it establishes the initial ownership record of the product. Second, it officially marks the beginning of the product's distribution lifecycle. This registration event acts as a verifiable checkpoint, indicating that the product is ready to enter the downstream supply chain. Importantly, this can occur only after the manufacturer's

***Corresponding Author:** Dr. V. R. Palanivelu

association with the product has been validated against the MMC database, thereby preserving the integrity of the system and ensuring that the chain of custody begins with a legitimate and verified source. Through this mechanism, the PMC provides a secure and transparent foundation for subsequent ownership transfers while strengthening trust among all supply chain stakeholders.

Within the PMC, the manufacturer's blockchain address is stored in its original, unencrypted form rather than in encrypted form. This design choice allows the manufacturer to establish and demonstrate authorship of the product. Consequently, anyone with access to the PMC can trace the product back to its original owner—the manufacturer—by identifying the first recorded owner in the system.

Distribution Management

Fig. 2 illustrates the comprehensive flow of the distribution management process within the proposed system. The distribution process is divided into two major phases: the shipping phase (Steps 1–4) and the receiving phase (Steps 5–8). These phases are outlined below.

1. The initial step involves the product owner confidentially transmitting a pre-agreed secret token to the designated recipient. This transmission must occur through a secure and trusted communication channel to maintain the token's confidentiality and mitigate any risk of interception or misuse by unauthorized entities.
2. Once the secret token has been securely shared, the product owner uses it, together with the manufacturer's publicly available cryptographic key, to encrypt the recipient's blockchain address, denoted by AR. This encryption process produces a ciphertext representation of the address, denoted as Enc(AR), thereby preserving the recipient's privacy during the transaction.
3. Subsequently, the product owner publishes the Verifiable Credential (VC) to the blockchain network. This smart contract serves as a tamper-proof, decentralized record attesting to the legitimacy of the product transfer and binds the product identity to the recipient's encrypted credentials.
4. Following the deployment of the VC, the owner records the encrypted recipient address, Enc(AR), together with the address of the deployed VC smart contract in the Product Management Contract (PMC). This step ensures that the required verification information is permanently recorded and available for future validation.
5. On the recipient's side, a cryptographic proof is generated to demonstrate knowledge of the secret token initially shared in Step 1. This proof employs Zero-Knowledge Proof (ZKP) techniques, enabling the recipient to prove possession of the secret without revealing any information about it, thereby preserving both security and privacy.
6. The recipient then submits the Zero-Knowledge Proof to the PMC, thereby signalling the intention to claim ownership and providing the necessary cryptographic evidence to support that claim.
7. Upon receiving the proof, the PMC communicates with the VC contract to authenticate the recipient's proof. It verifies the validity of the Zero-Knowledge Proof according to the verification rules defined in the VC smart contract.
8. If the submitted proof is successfully verified, the system executes a secure ownership transfer. This final step results in the product's ownership being formally and irreversibly transferred to the recipient's encrypted blockchain address, Enc(AR), thereby completing the verifiable and privacy-preserving transfer process.

The PMC is responsible for managing the critical stages of the protocol, specifically Steps 4, 6, 7, and 8, thereby ensuring the security and traceability of the product transfer. These key stages are explained in greater detail below.

The encryption of the recipient's address, performed in Step 2 of the protocol, is a fundamental component for preserving confidentiality. This encryption employs the elliptic curve variant of the ElGamal encryption scheme, as mathematically expressed in Equation (1). In this process, the recipient's address AR is transformed into its encrypted representation Enc(AR) using a randomly selected ephemeral key k, the elliptic curve base point G, and the manufacturer's public key Q. The resulting ciphertext consists of two elliptic curve points: the ephemeral public key kG and the masked address AR + kQ.

$$\mathrm{Enc}(AR) = (kG,\ AR + kQ) \qquad (1)$$

In this formulation, AR represents the recipient's blockchain address encoded as a point on the elliptic curve. The variable k denotes a secret nonce or token that is either pre-shared between the device owner and the recipient or generated dynamically for the session. The symbol Q represents the manufacturer's public key and serves as a critical element of the encryption process. The security of this encryption scheme relies on the computational hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP). It is also essential that AR represents a valid point on the elliptic curve because all elliptic curve operations require operands to lie on the same curve to maintain cryptographic correctness. By encrypting the address in this manner, unauthorized entities are prevented from discovering or linking the recipient's blockchain address, thereby strengthening privacy throughout the communication protocol.

Next, in Step 5, the recipient demonstrates legitimacy using a Zero-Knowledge Proof. This proof enables the recipient to correctly compute the encrypted address Enc(AR) without revealing any sensitive information, including the secret token k or the recipient's blockchain

***Corresponding Author:** Dr. V. R. Palanivelu

address AR. Zero-Knowledge Proofs, particularly zk-SNARKs, are well suited for this purpose because of their computational efficiency and compatibility with blockchain platforms. They enable the recipient to prove knowledge of the secret token k without disclosing it, thereby protecting the privacy of both communicating parties.

The Zero-Knowledge Proof is subsequently verified in Step 7 by the PMC, which invokes the deployed VC smart contract and confirms that the submitted proof is valid, thereby preserving the integrity of the distribution process.

Furthermore, even during Step 4, the product owner must first demonstrate legitimacy before recording the recipient's encrypted address in the PMC. This requirement prevents unauthorized product shipments by ensuring that only the legitimate owner can initiate the distribution process. Similar to the recipient, the owner must prove the ability to correctly compute the encrypted address Enc(AO), thereby ensuring a secure and verifiable ownership transfer.

Product Tracking

The blockchain plays a fundamental role in tracking product distribution. By recording the encrypted blockchain addresses of product owners at every stage of the distribution process, the PMC maintains an immutable and transparent ownership history. These encrypted addresses are linked to the product's lifecycle and are encrypted using the manufacturer's public key, allowing only the manufacturer to decrypt them using the corresponding private key. This mechanism enables the manufacturer to trace the product's movement throughout the supply chain by sequentially decrypting the recorded addresses and arranging them in chronological order, thereby ensuring complete traceability from the manufacturer to the final recipient.

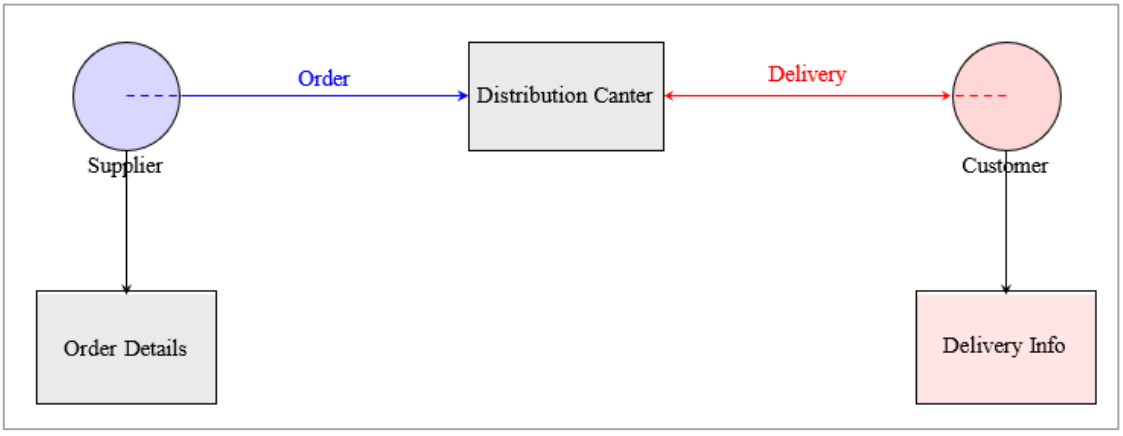

Fig. 2. Flow of distribution management in the proposed method.

VERIFICATION

In this section, the traceability and privacy properties of the proposed method are verified by considering potential fraudulent activities and attacks from malicious entities. By evaluating the system's resilience against these threats, it is demonstrated that the proposed method preserves both participant privacy and the integrity of product distribution.

A. Traceability

One potential security threat arises if an adversary attempts to manipulate the decryption process of the owner's encrypted address by compromising the authenticity of the manufacturer's private key. Specifically, an attacker could attempt to publish an encrypted message on the blockchain using a public key that does not correspond to the legitimate manufacturer's key. However, the proposed protocol inherently prevents such behavior.

Step 7 of the verification process explicitly references the manufacturer's authentic public key, which is permanently stored on the blockchain. Consequently, any decryption proof generated using an incorrect or unauthorized public key will automatically fail verification because the proof must correspond exactly to the original blockchain-registered public key. Therefore, even if a forged encrypted message is submitted, Step 7 rejects it due to inconsistent cryptographic evidence. This design effectively prevents such attacks and ensures that the distribution process remains secure and tamper-resistant.

A second attack scenario involves a third party that is not part of the legitimate distribution process attempting to impersonate either the product owner or the recipient. Successfully executing this attack requires the generation of a valid cryptographic proof. However, because the system relies on the **soundness property** of Zero-Knowledge Proofs, only parties possessing the required secret information can generate a valid proof. Without access to this knowledge, an attacker cannot forge a valid transaction. Consequently, such impersonation attacks are computationally infeasible and are effectively prevented by the cryptographic guarantees provided by the Zero-Knowledge Proof protocol.

***Corresponding Author:** Dr. V. R. Palanivelu

The third attack scenario considers a more subtle threat involving collusion between the legitimate owner and the recipient with the objective of concealing the identity of the actual owner. In this case, the colluding parties use either a randomly generated blockchain address or a genuine address that does not belong to the actual recipient. By sharing an arbitrary blockchain address together with a secret token, they can jointly generate a valid proof. This manipulation allows the owner information stored in the PMC to be updated successfully despite the use of an incorrect or proxy blockchain address.

Such an attack circumvents individual accountability and weakens supply chain traceability. Therefore, it is acknowledged as a potential limitation of the current protocol. Addressing collusion attacks of this nature represents an important direction for future research.

B. Privacy

A critical aspect of the proposed method is ensuring privacy, which could potentially be compromised if an attacker attempts to retrieve the owner's address from either the encrypted address or the cryptographic proof recorded in the PMC. Two possible attack vectors are considered to address this concern.

The first concerns the encrypted address itself. Its security relies on the strength of the underlying cryptographic algorithm and the key length. For example, the use of 254-bit elliptic curve cryptography (ECC), as proposed in [7], provides an extremely high level of computational security against unauthorized decryption attempts. Without the corresponding private key, it is computationally infeasible to recover the original blockchain address. Consequently, the encrypted address remains confidential, preserving the privacy of the product owner.

The second concerns the cryptographic proof generated during the authentication process. The proposed protocol employs a zero-knowledge proof (ZKP) mechanism that satisfies the zero-knowledge property. As a result, the proof reveals no confidential information, including the owner's blockchain address or the secret token used during authentication. The proof enables successful verification without disclosing any underlying private information. Therefore, even if an attacker gains access to the proof stored on the blockchain, no sensitive data can be extracted from it.

Based on these security mechanisms, the proposed method effectively prevents attackers from retrieving or inferring the owner's blockchain address, thereby preserving user privacy.

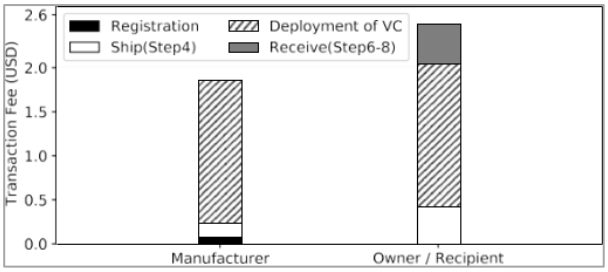

Fig. 3. Transaction fee per party for a certain product.

EVALUATION

To evaluate the effectiveness and efficiency of the proposed method, the protocol was implemented on the Ethereum blockchain. The evaluation included functional verification of the proposed approach together with an analysis of the associated transaction costs. In addition, practical application scenarios of the proposed protocol were examined.

Environment Setup

For the evaluation, the distribution of a product involving six sequential ownership transfers, beginning with the manufacturer, was simulated. The manufacturer performed the initial product registration and shipping operations, while each subsequent participant executed two operations: receiving the product from the previous participant and shipping it to the next participant.

The smart contracts implementing the proposed protocol were developed using **Solidity version 0.5.11** [8]. Validation and testing were carried out using the **JavaScript Virtual Machine (JSVM)** provided by the Remix Integrated Development Environment (IDE) [9]. Zero-knowledge proofs were generated and verified using **ZoKrates** [10], an open-source toolkit for zk-SNARK implementation.

RESULTS AND DISCUSSION

The experimental results demonstrate that none of the blockchain addresses belonging to product owners could be retrieved from the information stored in the PMC or VC after multiple product transfers. This confirms the effectiveness of the proposed privacy-preserving mechanism. Furthermore, the manufacturer was able to correctly identify the legitimate product owner by decrypting the encrypted blockchain address stored in the PMC using its private key. Therefore, the proposed approach successfully achieves both privacy preservation and manufacturer-level traceability.

The transaction costs associated with the distribution process were also evaluated. Transaction fees were calculated by multiplying the gas consumption reported by Remix with the Ethereum gas price at the time of testing. On March 17, 2020, at 11:00 a.m. JST, the gas price was 1.1622×10^{-6} USD per gas unit. The resulting transaction fees for each participant are presented in Fig. 3.

***Corresponding Author:** Dr. V. R. Palanivelu

The observed variation in transaction fees between the manufacturer and the remaining participants is primarily due to the different operations executed by each role. In particular, the shipping operation performed by the manufacturer differs from that executed by subsequent supply chain participants because of the additional verification procedures involving zero-knowledge proofs. Consequently, gas consumption and transaction fees vary according to the participant's role and the smart contract functions executed.

The results indicate that the maximum transaction fee incurred by any participant is approximately **2.6 USD**. Although additional optimization could further reduce this cost, the current implementation is economically suitable for high-value products such as automobiles and household appliances. These products frequently require recall procedures when manufacturing defects are identified. However, conventional recall systems often suffer from limited consumer awareness and low response rates [11].

By utilizing the proposed protocol, only the manufacturer retains complete traceability of the product throughout the supply chain, enabling direct notification of the current owner whenever a product recall is issued. Consequently, the transaction fee of approximately 2.6 USD can be regarded not merely as a blockchain transaction cost but also as an investment toward extended product support, allowing owners to receive timely repair or replacement services when necessary.

CONCLUSION AND FUTURE WORK

This study proposed a novel privacy-preserving approach that simultaneously ensures product traceability by the manufacturer within a blockchain-based supply chain system. By integrating pairing-based cryptography (PBC) with blockchain technology, the proposed method achieves a balance between privacy protection and traceability, addressing one of the major challenges in decentralized supply chain management.

The proposed approach was implemented on the Ethereum blockchain, and experimental evaluation demonstrated its practical feasibility. The results showed that the maximum transaction fee incurred per participant was approximately 2.6 USD, indicating that the method is economically viable for medium- and high-value products and has strong potential for industrial adoption.

Despite these promising findings, two important challenges remain for future research.

The first challenge involves reducing transaction costs. A significant portion of the current transaction fee results from deploying a new Verifier Contract (VC) for every product distribution event. A possible improvement would be to allow manufacturers to deploy a shared VC only once, enabling all supply chain participants to reuse the same verification contract. Such an approach would substantially reduce gas consumption and transaction costs, making the proposed system practical for lower-value products as well.

The second challenge concerns extending the proposed framework to support more complex product lifecycles involving product assembly and disassembly. The current implementation is designed primarily for the linear distribution of individual products. However, modern supply chains frequently involve composite products assembled from multiple components or products that are later disassembled for recycling or reuse. Future work should therefore focus on supporting traceable multi-product transactions while maintaining both privacy preservation and verifiable ownership. Such enhancements would improve the applicability of the proposed approach to circular economy initiatives and reverse logistics systems.

In conclusion, the proposed method demonstrates that secure, privacy-preserving, and traceable product management can be achieved using blockchain technology. Future improvements aimed at reducing transaction costs and supporting more complex supply chain structures will further enhance the scalability, practicality, and industrial applicability of the proposed system.

REFERENCES

1. Organisation for Economic Co-operation and Development (OECD), & European Union Intellectual Property Office. (2019). *Trends in trade in counterfeit and pirated goods*. OECD Publishing. https://doi.org/10.1787/g2g9f533-en
2. Centers for Disease Control and Prevention. (2016, February). *Multistate outbreaks of Shiga toxin-producing Escherichia coli O26 infections linked to Chipotle Mexican Grill restaurants (Final update).* Retrieved March 17, 2020, from https://www.cdc.gov/ecoli/2015/o26-11-15/index.html
3. Toyoda, K., Mathiopoulos, P. T., Sasase, I., & Ohtsuki, T. (2017). A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. *IEEE Access, 5*, 17465–17477. https://doi.org/10.1109/ACCESS.2017.2720760
4. Kim, H. M., & Laskowski, M. (2018). Toward an ontology-driven blockchain design for supply-chain provenance. *Intelligent Systems in Accounting, Finance and Management, 25*(1), 18–27. https://doi.org/10.1002/isaf.1424
5. Huang, H., Zhou, X., & Liu, J. (2019). Food supply chain traceability scheme based on blockchain and EPC technology. In *Proceedings of Smart Blockchain* (pp. 32–42). Springer. https://doi.org/10.1007/978-3-030-05764-0_4

***Corresponding Author:** Dr. V. R. Palanivelu

6. GS1. (n.d.). *The global language of business*. Retrieved March 17, 2020, from https://www.gs1.org/
7. WhiteHat, B., Baylina, J., & Bellés, M. (n.d.). *Baby Jubjub elliptic curve*. Retrieved March 17, 2020, from https://iden3-docs.readthedocs.io/en/latest/downloads/33717d75ab84e11313cc0d8a090b636f/Baby-Jubjub.pdf
8. Solidity. (n.d.). *Solidity documentation*. Retrieved March 17, 2020, from https://solidity.readthedocs.io/
9. Remix Project. (n.d.). *Remix Ethereum IDE*. Retrieved March 17, 2020, from https://remix.ethereum.org/
10. ZoKrates. (n.d.). *ZoKrates* [Computer software]. GitHub. Retrieved March 17, 2020, from https://github.com/Zokrates/ZoKrates
11. Organisation for Economic Co-operation and Development (OECD). (2018, November). *Enhancing product recall effectiveness globally* (OECD Science, Technology and Industry Policy Papers No. 58). OECD Publishing. https://doi.org/10.1787/ef71935c-en.

***Corresponding Author:** Dr. V. R. Palanivelu