Kalpa Publications in Computing

Volume 19, 2024, Pages 41–52

Proceedings of 6th International Conference
on Smart Systems and Inventive Technology

kalpa Computing

Securing Supply Chains: Blockchain's Shield Against Counterfeit Products

Abhay Das[1], Aishwarya Krishnadas[1], Vaishakh S Krishnan[1], Anjali Thachankattil[2], and Abhishek Sujith[3]

[1] Department of Computer Science and Engineering, Amrita School of Computing, Amrita Vishwa Vidyapeetham, Amritapuri, India
abhaydas02@gmail.com
aish3399@gmail.com
vaishakhsk2052@gmail.com

[2] Department of Computer Science and Engineering, Amrita School of Computing, Amrita Vishwa Vidyapeetham, Amritapuri, India
anjalit@am.amrita.edu.com

[3] Rolls-Royce Inc, Bangalore, India
abhishekabi2002@gmail.com

Abstract

Globalization and advancements in trade facilitation have opened up new possibilities for polluting trade routes with counterfeits. Consequently, protecting goods and products against counterfeiting has become critical for intellectual property owners worldwide. Yet, conventional safeguards of adding protective elements and safety features have proven inadequate. Over the past decade, blockchain technology has emerged with a promising potential to become a veritable tool in safeguarding supply chain authenticity. The proposed system presents an effective counterfeit detection system using blockchain technology. The proposed framework of the blockchain leverages a three-entity model - manufacturers, sellers (distributors), and consumers, ensuring transparency and immutability. The efficiency of the proposed system is demonstrated through experiments performed on various data.

Keywords: Consumer Safety, Blockchain Technology, Smart Contracts, Real-world case studies

1 Introduction

Counterfeiting isn't just a problem; it represents a multi-trillion-dollar 'economy' with estimates indicating approximate annual sales between $1.7 trillion to $4.5 trillion. Counterfeiting emerges as a staggering economic force, potentially ranking it as the world's tenth-largest economy (Forbes, 2022). India, one of the largest rising economies in the world has seen an alarming increase in the number of counterfeit goods in a variety of industries. The situation has put both consumers and businesses at risk. The predominance of such goods affects consumer confidence in the market, harms brand reputation, and has serious repercussions for the stability of the

economy. While counterfeiting happens throughout a range of businesses, some have proven more susceptible than others to this illegal activity. Generally, counterfeit products can be segmented into deceptive and non-deceptive practices [1].

In the case of non-deceptive counterfeits, consumers can readily identify fake products based on their notably lower prices, inferior quality, and unconventional sales locations, like high-end branded items sold by street vendors at significantly reduced costs. Conversely, deceptive counterfeits closely resemble genuine products in price and packaging but fall short in quality. These deceptively similar counterfeits mislead unsuspecting consumers, who unknowingly purchase unsafe or life-threatening products. For example, the counterfeiting of pharmaceuticals presents a serious threat to public health and safety. Traditional safeguards like radio frequency identification (RFID) and watermarks fall short, as counterfeiters can replicate genuine product tags, and post-purchase, the removal of tags at sales counters nullifies the assurance of product authenticity[3].

Employing blockchain presents a promising solution. The proposed system examines how blockchain technology helps consumers feel more at ease about the legitimacy of their purchases and stop the spread of counterfeit goods. A blockchain is a chain of chronological blocks[5]. It functions as a decentralized system designed for storing and distributing digital data. Its decentralized nature ensures trust among the parties involved and reduces the risk of network failure. In 2018, IBM announced the Trust Chain initiative. It is a blockchain solution with technology specifically designed to trace the global origins of the raw materials in the diamond and jewelry industry. In 2021, VeChain recorded digitized COVID-19 vaccine passports in the form of NFT tokens. In Blockchain, information is structured into blocks each of which is transformed into a hash format. Every block contains data from the preceding block, and its hash value is computed based on the combination of the previous block's hash value and its details. This process continues sequentially, ensuring the interconnectedness of blocks. Any attempt to tamper with or modify data would disrupt the integrity of all subsequent blocks, preserving the immutability of the entire Blockchain network.

An efficient counterfeiting system is proposed, utilizing Blockchain technology, providing consumers with complete product histories from manufacturers to end-users. To trace the journey of products across the supply chain, QR codes are utilized within the application. At every stage of the chain, these chips require scanning to satisfy the criteria set by the smart contract. Subsequently, numerous autonomous blockchain nodes validate the information received. It ensures transparency and authenticity throughout the product supply chain. This innovative approach not only safeguards consumers but also elevates the overall knowledge and understanding of employing advanced technology to combat the pervasive issue of counterfeit goods.

2 Objective

The project initiative was prompted by the exponential rise of counterfeit products. While previous studies have mainly used blockchain for verification, our novel method applies a three-body entity type verification system to improve the supply chain's authenticity tracking. This new approach surpasses the traditional techniques by adding a tripartite validation process that includes the product and two other essential supply chain entities. The objectives of this project are:

1. To Design an Anti Counterfeit System using Blockchain.
2. To implement a three-entity verification system.

3 Related Work

This section explores research on the usage and applications of blockchain technology in counterfeit product detection systems.
"A Blockchain-based approach for detecting counterfeit products in supply chains" by H.M. Tharaka Thilina et al. (2021) [6] The system proposes a blockchain-based solution for detecting counterfeit products in supply chains. The technology traces products from manufacturing to consumption by integrating blockchain and the Internet of Things (IoT), effectively monitoring their route. The authors demonstrate the viability of their strategy in a pharmaceutical supply chain case study.
"Blockchain: case studies in food supply chain visibility" by Rogerson et al. (2020) [4] Nestle, a major player in the food and beverage sector, started a ground-breaking project to use blockchain technology to solve this problem. Chinese technology company Techrock and Nestle had joined together to create a mobile app with public blockchain platform. Parents were given the ability to confirm important aspects of NAN A2 using the blockchain platform and mobile app, including the components, their sourcing regions, the place of production, and even specifics about the packaging with accompanying photographs. Parents were able to make educated decisions and confirm the legitimacy and safety of the goods they were purchasing for their newborns because of the immutable and decentralised nature of blockchain technology.
"A secure blockchain-based approach for detecting counterfeit products in online marketplaces" by X. Zhang et al. (2020) [7] The paper proposes a safe blockchain-based solution for detecting counterfeit items in online markets. The technology examines product characteristics, images, and various data to identify probable counterfeit items by combining blockchain and machine learning.
The proposed research work involves the incorporation of traditional blockchain technology in combination with Quick Response Code (QR Code) technology for verification. It also suggests a more efficient system that employs three key entities - product, supplier, and distributor - to enhance the overall integrity and transparency of the supply chain. Through the addition of a tripartite validation process that includes the product and two other essential supply chain entities, this approach surpasses traditional techniques and creates a robust and all-encompassing framework.

4 Proposed Methodology

The system design is shown in the below Fig 1. This study describes a development and application process for a supply chain management system that uses a blockchain to monitor products. Through enabling transparent and safe tracking of products from makers through sellers and eventually to customers, the system makes use of QR codes, Metamask, Ganache, and Truffle [2]. The system applies a three-body entity type verification system, enabling a tripartite validation process to improve the supply chain's authenticity tracking. Through the extension of the verification scope to encompass the product, supplier, and distributor—these three interdependent entities—a strong and all-encompassing framework that greatly enhances the supply chain's overall integrity and transparency are developed.

Why Blockchain?

Blockchain is a collection of blocks that are linked together which stores information. It operates across a network of computers(nodes) and can record real data at each node in the entire

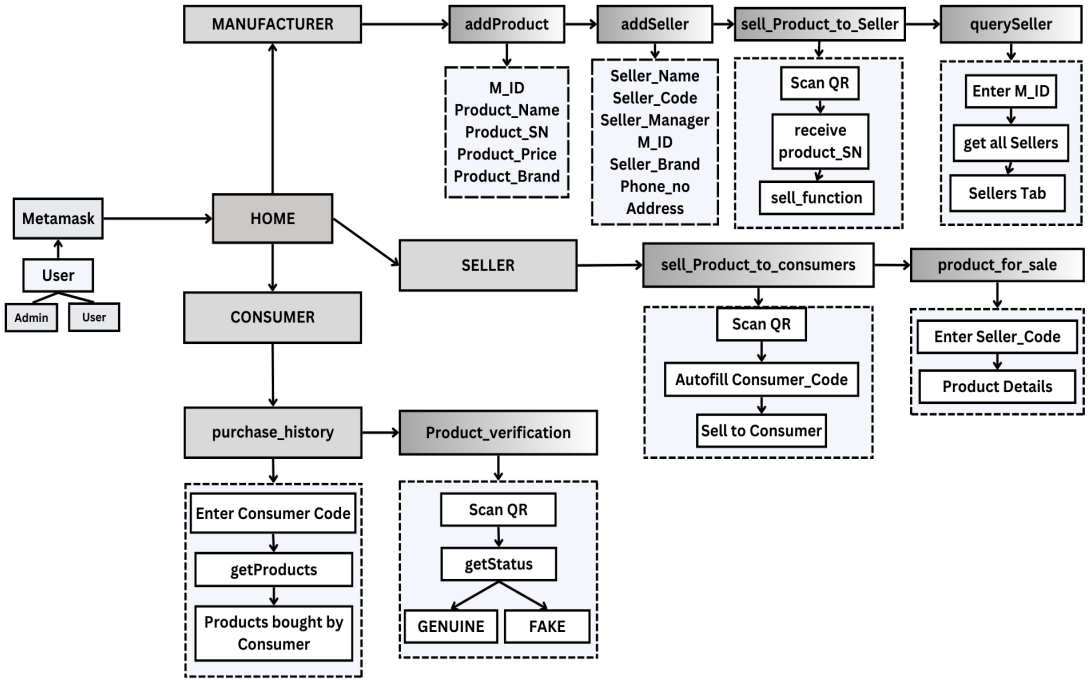

Figure 1: The system design

supply chain. Each block has a timestamp, transaction data and hash of its own and hash of previous block, so it is difficult to tamper with data. Blockchain is a decentralized system. It ensures that every new block added to the blockchain is the one and only true version that is agreed upon by all nodes in the Blockchain. It refers to the collective maintenance of a technical solution that maintains a continuous record file as a reliable database through decentralization. Throughout order to accomplish timely data exchange and complete traceability across the product life cycle of the supply chain, blockchain technology functions over a network of computers, or nodes. It can capture real data at each node throughout the entire supply chain. This, along with Blockchain's immutability and transparency properties, not only significantly increases supply chain management efficiency but also aids in resolving the issues of product traceability and responsibility. Naturally, prompt sharing of product circulation data via blockchain technology raises customer satisfaction, which boosts the competitiveness of the supply chain as a whole.

Because blockchain eliminates the need for third parties, it fosters greater trust. Smart contracts, which are essentially blockchain programs, only execute when specific requirements are satisfied. It gets more difficult to alter the blockchain with false information because every block saves its contents along with the hash of the previous block. The hash of a block changes if an attacker modifies its contents, while the hash of the subsequent block stays unchanged. Each block has transaction data, a timestamp, and a cryptographic hash of the block before it. A new transaction is broadcast to the network of nodes, or computers, when it is started, and these nodes confirm the transaction using pre-established standards. Upon verification, the transaction is added to a fresh block, which then establishes a cryptographic connection with the preceding block via its hash. A consensus method, such as Proof of Work or Proof of

Stake, ensures that all nodes agree on the current state of the ledger, facilitating the process of adding blocks to the chain. Because of its cryptographic connection, the linked blocks provide an immutable, tamper-evident record of every transaction. Any changes made to one block render all other blocks invalid.

A Metamask

By giving users control over Ethereum assets and facilitating communication with blockchain-based applications (dApps), MetaMask improves supply chain trust. Customers can access a blockchain system for tracking product data and authenticity by integrating with MetaMask. Fast product legitimacy verification is made possible by QR codes and unique identifiers that are verified by MetaMask.

B Ganache and Truffle Suite

Providing a private Ethereum network for supervised testing of smart contracts and decentralized applications (dApps), Ganache functions as a local blockchain emulator. When combined, these tools allow for the easy development, deployment, and testing of smart contracts that handle authentication and product tracking within the haven provided by Ganache's local blockchain emulation.

C Ethereum

Blocks are added to the decentralized blockchain through the proof-of-work consensus mechanism, which verifies nodes' computational efforts by solving mathematical equations. This procedure, called mining, makes sure that blocks are verified and recorded. Ethereum (ETH) sets itself apart from conventional brute force mining techniques by implementing a reward scheme for successful block additions.

D Smart Contracts

Programs called smart contracts are kept in blocks. Third-party participants are replaced with smart contracts. These essentially operate as protocols when the conditions are met. They remain constant, therefore nobody can alter the contract.

E Manufacturer

The manufacturer is capable of four tasks: sell`_Product_to_Seller`, addProduct, addSeller, and querySeller

1. addProduct: The manufacturer adds a new product to the blockchain, providing information on the item's name, unique identifier, and authenticity attributes to ensure transparency(Fig 2).

2. addSeller: Manufacturers use this feature to include approved sellers in the blockchain network and linked them to particular product categories or geographical areas, facilitating safe distribution routes(Fig 3).

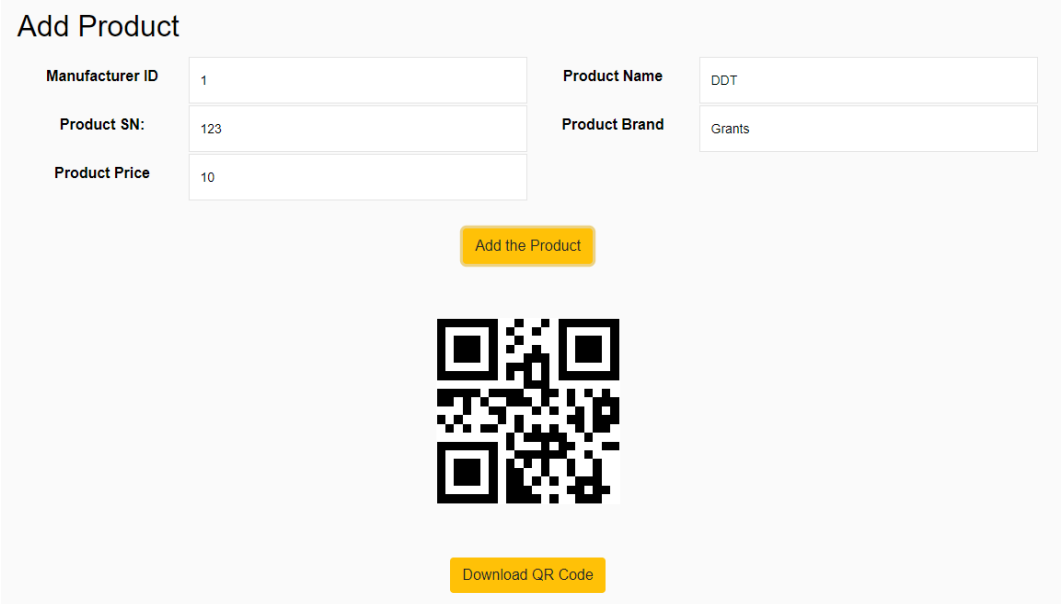

Figure 2: addProduct Function

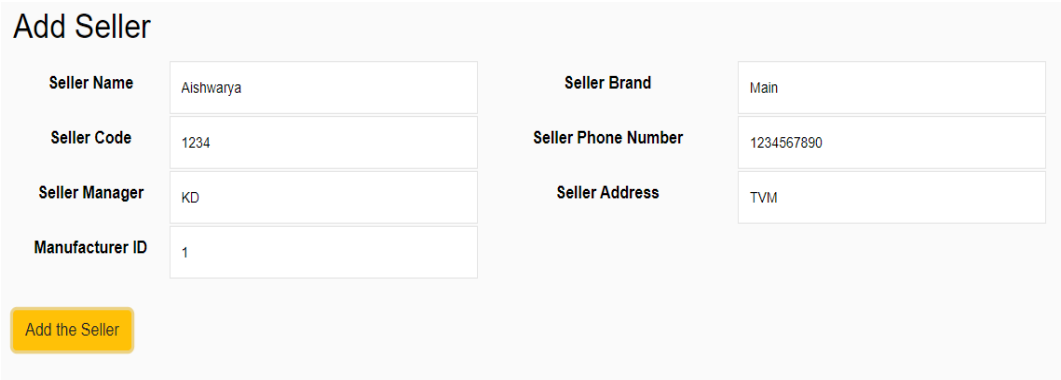

Figure 3: addSeller Function

3. sell_`Product_to_Seller`: The manufacturer can update the ownership and status of products sold to approved sellers while also keeping a clear record of all previous transactions.

4. querySeller: To help with the identification and tracking of counterfeit goods, manufacturers use this service to acquire details about a specific seller the product categories they are permitted to sell, and their transaction history.

F Seller

Seller: Seller scans the product's QR code.
Two tasks are available for the seller: sell_`Product_to_consumer`, product_`for_sale`

1. market_`Product_to_consumers`: When a seller scans a product's QR code, this feature enables them to complete a sale transaction, giving the consumer ownership of the scanned item while recording the transaction's specifics on the blockchain for accountability and transparency.

2. product_`for_sale`: This feature enables the seller to examine a list of items that are currently for sale from their inventory, assisting them in managing their offerings and updating product availability data, which is important for keeping a current and accurate product catalog.

G Consumer

1. purchase_`history`: Customers use this function to retrieve their purchase history, which offers a thorough record of all previous transactions. Consumers can study product specifications, pricing, and purchase dates, which improves their ability to keep track of their product purchases.

2. product_`verification`: Customers can scan a product's QR code or provide a special identifier to confirm the legitimacy and place of origin of the item. This promotes trust in the supply chain and lowers the risk of counterfeit goods by making sure that customers can reliably check the legality of the products they buy.

H Blockchain Security Measures Evaluation

1. Immutability: Verify that once the data has been written to the blockchain ledger, it cannot be removed or changed. This guarantees an unchangeable, long-lasting record of every item's travels.

2. Cryptographic Hashing: Evaluate the hashing algorithm's strength in order to safeguard data on the blockchain. Common metrics include the avalanche effect, which occurs when slight changes in data cause big hash changes, and collision resistance, which measures how difficult it is to construct identical hashes for different data.

3. Consensus Mechanism: Evaluate how well the selected consensus method (such as Proof-of-Work or Proof-of-Stake) protects the network from hackers trying to alter data. Block generation time, consumption of energy (in the case of Proof-of-Work), and stake distribution (in the case of Proof-of-Stake) are examples of metrics.

4. Smart Contract Security: Examine the code of the smart contract for security flaws such as reentrancy attacks, integer overflows, and access control problems. To find and fix possible security vulnerabilities, use penetration testing and static code analysis tools.

5. Key Management: Evaluate how securely private keys are kept and managed in order to communicate with the blockchain. This comprises protocols for access control, hardware security modules, and secure key creation.

5 Results and Discussion

A Security Considerations

The three-entity blockchain strategy for detecting fake goods is implemented with a number of security concerns thoughtfully examined and resolved. These factors are essential to guaranteeing the system's resilience and efficacy.

1. Data Integrity: Because traditional systems are frequently transparent, data manipulation can occur. The blockchain-based solution, on the other hand, makes use of a decentralized ledger to guarantee immutable records and maintain data integrity all the way through the supply chain.

2. Counterfeit Prevention: By giving each item a unique identification, blockchain technology enables thorough product tracking and discourages attempts at counterfeiting. The solution substantially lowers the possibility of counterfeit infiltration through continuous tracking from point of origin to point of destination.

3. Visibility Enhancement: The system offers absolute supply chain visibility and transparency by logging all transactions and movements on the blockchain. This improved visibility helps to preserve the integrity of the entire ecosystem by spotting anomalies and inefficiencies.

4. Auditing and Compliance: By providing clear, unchangeable records of every action taken across the supply chain, blockchain automates auditing procedures. This transparency greatly cuts down on the time and expense of auditing while streamlining compliance verification processes.

5. Data Security: By protecting sensitive data from potential cyberattacks and breaches, blockchain technology improves data security through the use of cryptographic algorithms and a distributed design. Because blockchain technology is decentralized, data is protected from single points of failure.

The 3-entity blockchain model proves to be a game-changer in anti-counterfeit efforts. Its decentralized nature, comprehensive verification approach, and end-to-end coverage provide a robust solution that surpasses traditional methods and standard blockchain approaches.

B 3-Entity Blockchain's Advantage in Combating Fakes

The three-entity blockchain model for fake product identification surpasses both traditional supply chain and standard blockchain verification methods in key aspects, such as demonstrated by our research findings.
In our proposed system, we address product counterfeiting through a multi-step verification process leveraging blockchain technology. Each product receives a unique identifier, like a QR code, linked to a central database containing detailed product information. Blockchain then stores a secure hash of this information, acting as a digital fingerprint. Suppliers include the QR code and a digitally signed record of the shipment on the blockchain using their unique account. Distributors can verify the product's authenticity by scanning the QR code, retrieving the original hash from the database, and recalculating it with the retrieved information. Any discrepancy between the two hashes exposes potential tampering or counterfeiting. This

Stakeholder	Blockchain benefit
Buyers, manufacturers, distributors, and sellers	Replaces paper documentation with digital fraud-proof certificates that are instantly verifiable
Third party logistics	Informed about the origin and destination of the product
Retailer	Can track all of the products and be assured that they are genuine from suppliers and logistics carriers without the need for third parties to continually check
Store	Can get full transparency on the product including the origin and standards
Customer	Can scan a QR code from their app and instantly get information on the origin of a product and other details

approach fosters transparency within the supply chain as all participants, including consumers, can verify product legitimacy at any stage. By readily scanning the QR code with a verification app on their smartphones, consumers gain immediate assurance of a product's authenticity, fostering trust and brand loyalty. Additionally, the cryptographic security of blockchain makes tampering with data highly improbable, increasing overall trust and consumer confidence in the authenticity of products.

C Traditional Supply Chain Limitations

Traditional supply chains lack transparency and rely on centralized records, making them vulnerable to fraud and counterfeiting. Information silos prevent comprehensive product tracking, hampering early detection of fake products infiltrating the system. The 3-entity model disrupts this by:

1. Decentralizing data: Blockchain distributes product information across a network of nodes, providing a tamper-proof audit trail accessible to all authorized entities.

2. Enabling real-time tracking: Every stage of the product the journey is documented on the blockchain, empowering continuous oversight and immediate identification of discrepancies.

D Standard Blockchain Verification Shortcomings

Standard blockchain verification systems often focus solely on product origin or specific checkpoints, leaving gaps in the verification process. Counterfeiters can exploit these gaps by bypassing certain checks or manipulating data at authorized points. The 3-entity model addresses these issues by:

1. Triple-layer verification: Manufacturer, processor, and distributor/retailer each contributes to the verification process, creating a multi-pronged defense against counterfeiting.

2. End-to-end coverage: Verification occurs at every step within the authorized supply chain, eliminating blind spots and creating a holistic picture of product authenticity.

Blockchain technology functions as a distributed ledger, meaning a copy of the entire transaction history is replicated across a network of computers. Any alterations to the data would need to be reflected consistently across all copies, an extremely challenging feat due to the network's decentralized nature.

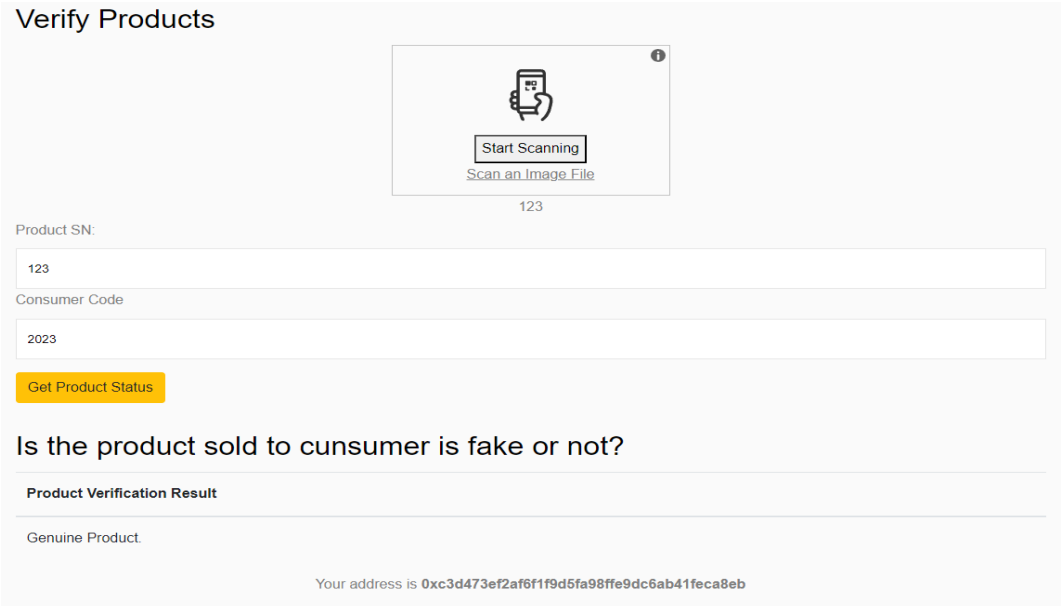

Figure 4: verifyProduct Function

Overall, the system successfully identified all test items that deviated from the authorized production flow and discriminated between real and counterfeit products. It highlighted its relevance by demonstrating scalability and practical usability through quick product verification. The system demonstrated remarkable accuracy and dependability in distinguishing between genuine and fake goods, demonstrating its high degree of precision. A comparison of Fraud Rates by Industry is shown in Figure 5.

6 Conclusion

In conclusion, the proposed blockchain-based system is a crucial step in combating counterfeit goods, safeguarding the supply chain, and preserving the thriving consumer market. The core tenets of blockchain technology, including its immutability, the execution of smart contracts, and the maintenance of data consistency, providing a solid framework for effective product verification. Additionally, the system's traceability empowers consumers with comprehensive information, enabling them to make informed choices.

However, our systemic approach presents conducting a feasibility test at a small scale, which is just one of numerous strategies. According to experts, it is widely acknowledged that blockchain has substantial room for improvement in terms of enhancing performance,

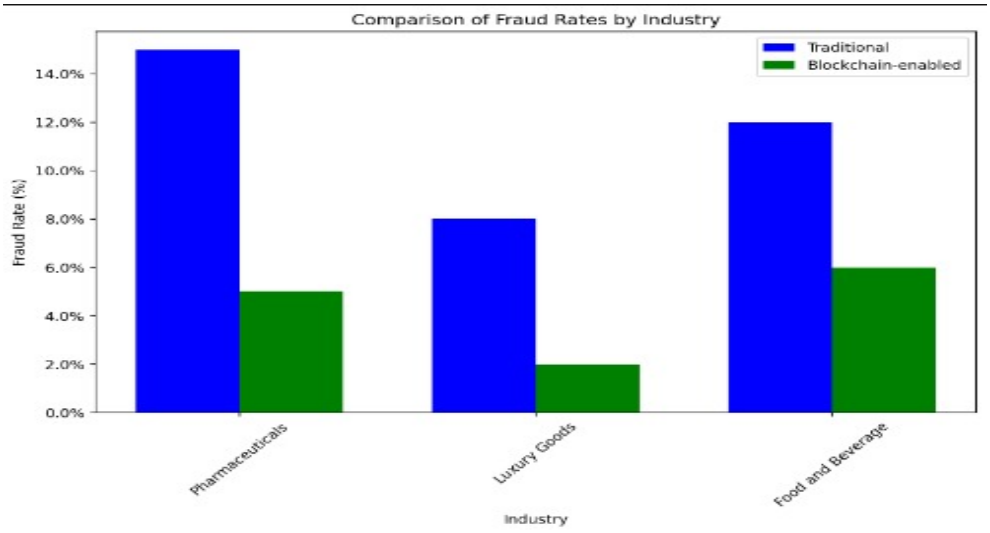

Figure 5: Comparison of Fraud Rates by Industry

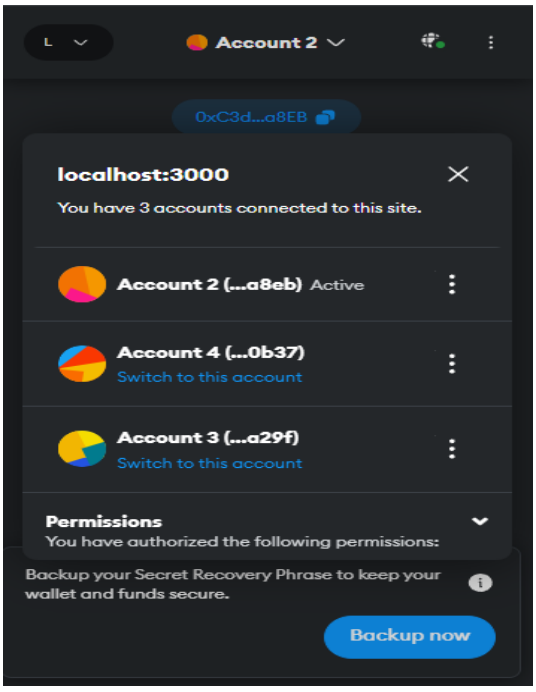

Figure 6: Connection of accounts to localhost site

particularly in areas like latency, throughput, and scalability. Nonetheless, as we progress, the proposed system holds promise in generating enduring effects on the integrity of supply chains, bolstering consumer trust, and contributing to the overarching economic welfare.

Acknowledgment

We would like to express our gratitude to our mentor, Assistant Professor Anjali T, and our guide, S Abhishek for their invaluable guidance, academic encouragement, and friendly critique. We would like to acknowledge that the research presented in this paper does not involve or utilize any data or resources from Rolls-Royce India Private Limited, Bangalore, India. The work presented here is based solely on independent research and publicly available data sources. We also acknowledge Amrita Vishwa Vidyapeetham for providing the necessary academic environment and resources.

References

[1] G. M. Grossman and C. Shapiro. Counterfeit-product trade, 1986.

[2] H. S. Hassan, R. Hassan, and E. K. Gbashi. Evoting system based on ethereum blockchain technology using ganache and remix environments. Published in Engineering and Technology Journal, Volume 41, Number 4, Pages 1–16, 2023.

[3] H. Pun, J. M. Swaminathan, and P. Hou. Blockchain adoption for combating deceptive counterfeits. Published in Production and Operations Management, Volume 30, Number 4, Pages 864–882, 2021.

[4] M. Rogerson and G. C. Parry. Blockchain: case studies in food supply chain visibility. Published in Supply Chain Management: An International Journal, Volume 25, Number 5, Pages 601–614, 2020.

[5] S. Saha, B. Jana, and J. Poray. A study on blockchain technology. SSRN 3477373, 2019.

[6] H. M. T. Thilina. A blockchain-based approach for detecting counterfeit products in supply chain, 2021.

[7] X. Zhang. A secure blockchain-based approach for detecting counterfeit products in online marketplaces, 2020.