INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Combating Counterfeit Products with Blockchain Technology to Enhance Trust and Authenticity in Consumer Markets

S Saraswathi[1]*, J Suresh[1], Digant Mehul Gandhi[2]

1 Associate Professor, Department of Computer Science and Engineering, SriSivasubramaniya Nadar College of Engineering, Kalavakkam, 603110, Tamilnadu, India
2 Department of Computer Science and Engineering, SriSivasubramaniya Nadar College of Engineering, Kalavakkam, 603110, Tamil Nadu, India

OPEN ACCESS

Received: 30-04-2024

Accepted: 16-07-2024

Published: 26-08-2024

Citation: Saraswathi S, Suresh J, Mehul Gandhi D (2024) Combating Counterfeit Products with Blockchain Technology to Enhance Trust and Authenticity in Consumer Markets. Indian Journal of Science and Technology 17(34): 3512-3521. https://doi.org/10.17485/IJST/v17i34.1449

* **Corresponding author**.

saraswathis@ssn.edu.in

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: Counterfeit products are becoming a global problem where consumers are fooled into buying fake goods without being able to verify their authenticity. By taking advantage of the secure and transparent nature of blockchain, this work aims to establish a system for consumers to verify the authenticity of products. **Methods:** Recently, blockchain has become more popular because it fosters trust between untrusted participants. A blockchain is a decentralized, distributed, and digital ledger that records transactions by means of blocks. It is a security technology that does not allow anyone to change or hack the block. Using blockchain technology, customers do not have to rely on third parties to confirm product originality. **Findings:** This work will show the effectiveness of blockchain. Blockchain creates a more secure and transparent system for product authentication. It helps in identifying counterfeit products entering the market and increases consumer confidence during purchase. The comparison of the transaction send rate and the average latency for each type of transaction is elaborated. The CPU consumption for each transaction type Add, Query, and Query-all are 1.81%, 1.11% and 1.27% respectively. The memory consumption by add, Query and Query all are respectively 53MB, 45MB and 92 MB. **Novelty:** Blockchain technology helps manufacturers to add real product serial numbers into the ledgers. The serial number stored in the ledger is protected from tampering. The stored serial number helps consumers check the authenticity of a product before buying it. To verify that a manufacturer or trader is genuine, consumers may also submit reviews of the products they purchase. The deeper integration of consumer reviews within the system offers a novel approach to enhancing trust and transparency in the verification process. We have also developed a user-friendly interface for manufacturers, sellers, and customers, enhancing the novelty of our solution.

Keywords: Counterfeit product; Blockchain; Supply chain; Product Authenticity; Trust

1 Introduction

A counterfeit product is a weaker imitation of the original with the main objective of imitating luxury goods at a lower price to stimulate savings for consumers. Nowadays, the quality of such products has rapidly developed over recent years, and today, they are almost in line with their original product. According to the Organization for Economic Cooperation and Development (OECD), worldwide trade in counterfeit goods has grown at a constant rate over the last few years. It is now accounting for 3.3%. Figure 1 lists the industries that are affected by counterfeit products and shows that the footwear and clothing industries are the most affected industries[1]. Counterfeits take away revenue from original brands and, depending on the type of products, like pharmaceuticals and beauty products, can seriously harm the health of consumers.

One of the biggest challenges in combating counterfeit products is identifying them. Counterfeiters have become increasingly sophisticated in their methods, making it difficult for consumers and regulators to distinguish fake products from genuine ones. Counterfeit items can be made to seem to be indistinguishable from real items, with just minor contrasts that are frequently challenging to recognize. As a result, consumers may purchase counterfeit goods without realizing it, which can have serious consequences. Due to a lack of trust, counterfeit goods are making consumers more reluctant to buy products on the internet. Authentic brands, on the one hand, are affected when they lose business[2].

On the other hand, uninformed consumers are helping counterfeit brands to make money while hurting legitimate brands' profitability and success. These problems have created a huge need for a reliable way to authenticate products before purchase, especially when they are exchanged between consumers. Fake goods have been a problem for a while on the global market. Given the rise in counterfeit goods on the market, it is now essential to have a safe and effective system for tracking products and ensuring their authenticity. By offering a decentralized and tamper-proof mechanism to distinguish and trace products from their starting place to their last objective, blockchain technology can play a critical part in tackling this issue.

Fig 1. Percentage of Counterfeiting in various sectors

In today's world, blockchain technology offers a dependable way to build a platform where customers can trust each other. Tracking and verifying the authenticity of products can be made easier and safer with the help of blockchain technology. Blockchain is a distributed ledger that securely and without permission records transactions. A distinct cryptographic hash connects each block of the blockchain to the block that came before it, resulting in an unbroken record chain. The immutability and security of the data that is stored on the blockchain are ensured by the fact that a block cannot be changed or deleted after it is added to the system. A blockchain platform is a medium through which users can interact with a blockchain and its network, whereas a blockchain network is a distributed ledger infrastructure. Blockchain platforms are designed to be scalable and act as extensions of existing blockchain infrastructure, enabling information exchange and service usage directly from within that framework. Developers can create tokens to represent any digital asset, track its ownership and perform its functions according to programming instructions. Each product is given a unique digital identifier that is recorded on the blockchain ledger in a system that is based on blockchains for product identification. This identifier can be utilized to confirm the validness of the item at each phase of the network. By comparing a product's digital identifier to the data stored on the blockchain, anyone with access to the blockchain can verify the product's authenticity.

There are many research contributions to combat counterfeit products. In the paper [3], the authors look at how blockchain can help to stop fake products that trick customers and suggest that government subsidies can make blockchain even more effective. It finds that supporting blockchain could be better for everyone than strict enforcement. Implementing blockchain technology could help customers avoid buying fakes and benefit society as a whole. This work considers only a single manufacturer. The authors in [4] suggest that blockchain can help stop fake goods in sustainable supply chains by using insights from interviews with experts, technology specialists, and case studies. They investigate the barriers to using blockchain and the ways to overcome them. They suggested a framework for improving traceability, authentication, and accountability. This work focuses on manufacturing and does not apply to other industries. A serious issue of counterfeit medicine is addressed in [5] and proposes a blockchain-based framework to combat it. The study includes interviews and content analysis to understand the problem, explore specific use cases, and find that the blockchain solution is secure, scalable, and user-friendly. This work relies on physical packaging for verification. Fake Product Identification for Small and Medium Firms (FPISMF), a blockchain-based solution using Hyperledger and AES encryption to help businesses detect counterfeit products and protect their brand reputation is proposed in [6]. Product and customer information is encrypted and stored on the blockchain, with the system using chaincode in a secure, containerized environment. The problem with this work is that the processing time could be higher.

TrustChain, a blockchain-based decentralized mobile application system [7], was designed for supply chain traceability across various manufacturing industries. TrustChain utilizes blockchain technology and decentralized storage to securely record product histories and help with product authentication and origin tracking. TrustChain offers a transparent solution for both companies and consumers to verify product authenticity and combat counterfeit products. This work relies on time-consuming manual QR code generation. The paper [8] talks about how fake products are a big problem in the textile industry, hurting both consumers and honest businesses. It suggests using blockchain technology to keep records secure and unchangeable. Blockchain can make sure products are real by tracking their journey from start to finish. This not only helps companies protect their reputation and helps customers stay safe, but it also makes it easy for people to verify if a product is genuine using their phone. Overall, all these papers are about using modern blockchain technology to fight counterfeit goods and make things better for humanity. In [9], the authors proposed a reliable Blockchain-based Biometric Authentication Solution (BBAS) for the Aadhar. They developed a hybrid scheme that uses a blockchain to store the hash value of the biometric and a trusted third party to store the original biometric file to enhance the security of the Aadhar-based verification system. The blockchain-based supply chain system may need more improvement, such as integration into existing supply chains, the ability to handle large-scale supply chains, interoperability between different blockchain systems, and data privacy. In summary the research shows that blockchain technology can effectively combat counterfeit in many fields like pharmaceuticals, food, textile, banking, insurance and Aadhar based verification. Researchers' opinion is that government subsidiaries, strict enforcement and integrating blockchain with existing systems can stop fake goods. This would benefit consumers and society more.

The adoption of blockchain offers incredible potential for each stage of the product and gives organizations tailor-made tools to deal with counterfeiting. They use distributed ledger technology to create a digital footprint for the entire supply chain. Automated platforms reduce the risk of fraud by streamlining the supply chain's flow of money and services [10]. Legacy systems can easily be integrated with blockchain-powered counterfeiting solutions. This makes blockchain technology a cost-effective solution for industries to combat counterfeiting. For example, legitimate manufacturers can claim primary ownership of their products, and this increases consumer confidence that they are buying genuine products. Overall, blockchain reduces fraud and improves anti-counterfeiting measures across supply chains.

To meet such requirements, we propose a new blockchain-based anti-counterfeiting system in this work. A full protocol is launched to allow any party, including manufacturers, sellers, and customers, to transfer and prove ownership of products. An important advantage of the proposed system is that consumers can review the products they receive and add reviews to the system for a specific product. Table 1 highlights the comparative analysis of existing work with the proposed one. Most of the works related to blockchain are study-based, and papers that discuss the implementation are considered for comparative analysis.

Table 1. Comparative Analysis with Existing Work

Work	Industry	Scalability	Blockchain platform	Limitations Identified	Reviews incorporated
Framework to prevent medicine counterfeit [5]	Medicine	No	Private	Not a cost-effective solution	No
FPISMF [6]	Small and Medium industry	Yes	Private	More complexity as it uses encryption methods	No
TrustChain [7]	General	Yes	Private	Not a cost-effective solution, as gas(payment term) is used as cost for transactions	No
Framework for counterfeiting in Textile [8]	Textile	No	Private	Complexity	No
Proposed framework	General	Yes	Public	-	Yes

2 Methodology

2.1. System model

The proposed architecture given in Figure 2 shows how the participant applies and becomes a member. It also shows the transaction and ledger management. The elaboration is given in the following subsection.

2.2. Proposed Work

Our application involves three major participants: The Manufacturer, The Seller, and The Consumer. The admin provides the manufacturer, seller and consumer with the required credentials to access the system.

1. Manufacturer: The manufacturer has the authority to add products they produce and information on the sellers to whom they are selling, ensuring no counterfeiting. The manufacturer can also retrieve information on all consumers who have bought their products.
2. Seller: The seller can add information on the consumer to whom the product is being sold. The seller can also retrieve the information related to the list of consumers and products.
3. Consumer: The consumer can authenticate whether a product is genuine before buying it and provide reviews on the products they have purchased.

The system architecture consists of a Membership Service Provider (MSP) that creates three different types of network participants: Manufacturer, Seller, and Consumer. The participants' roles determine their login credentials, which are validated by the Certificate Authority. The MSP ensures that all participants, including consumers, sellers, and manufacturers, are authorized to add and query transactions. The MSP also enrolls new participants after verifying their identities. It generates and supplies cryptographic keys and assigns appropriate permissions to the participants. When a participant accesses the website, an endpoint is triggered that connects the system to the network. The system authorizes the user by checking if the user is enrolled in the network and then allows the participant to perform various operations depending on their role.

Backend initiation involves creating orders and adding them to the channel using the Raft Consensus Algorithm. Shell scripts facilitate peers joining the channel, deploying the chaincode, and initializing smart contracts. Smart contracts, written in Go, link various system functionalities with the blockchain. These functionalities include adding products, adding orders, querying products, querying consumers, checking product authenticity, and reviewing products by consumers. Each smart

contract trigger adds a transaction to the blockchain and updates the world state database. We use CouchDB to manage our database operations. As the default state database for the Hyperledger Fabric network, CouchDB is a NoSQL document-oriented database that stores the data in JSON format and is highly scalable and resilient.

The Hyperledger Fabric network consists of the transaction management system and the ledger management system. The transaction management system facilitates the transfer of products between the manufacturer, seller, and customers. Transactions are digitally signed using cryptographic techniques to ensure authenticity and integrity. Before a transaction is added to the blockchain, it undergoes validation. Once validated, transactions are included in a block and require confirmation by the network, with the number of confirmations indicating transaction security. Our Raft consensus algorithm supports this process. Raft ensure all nodes agree on the ledger's state before and after adding a transaction. It manages the ordering service, creating transactions, and forming blocks. The consensus process involves leader election, where a node is randomly elected as the leader and other nodes become followers. The leader validates and proposes transactions to the followers. Once the majority of followers acknowledge the transactions, the leader adds them to the ledger. The transactions are then verified and committed to the block. The ledger management system records all transactions, such as adding and querying products. Transactions are validated, added, and maintained by a network of distributed nodes. Our design is a decentralized and tamper-proof system to ensure the authenticity of products and increase consumer trust.

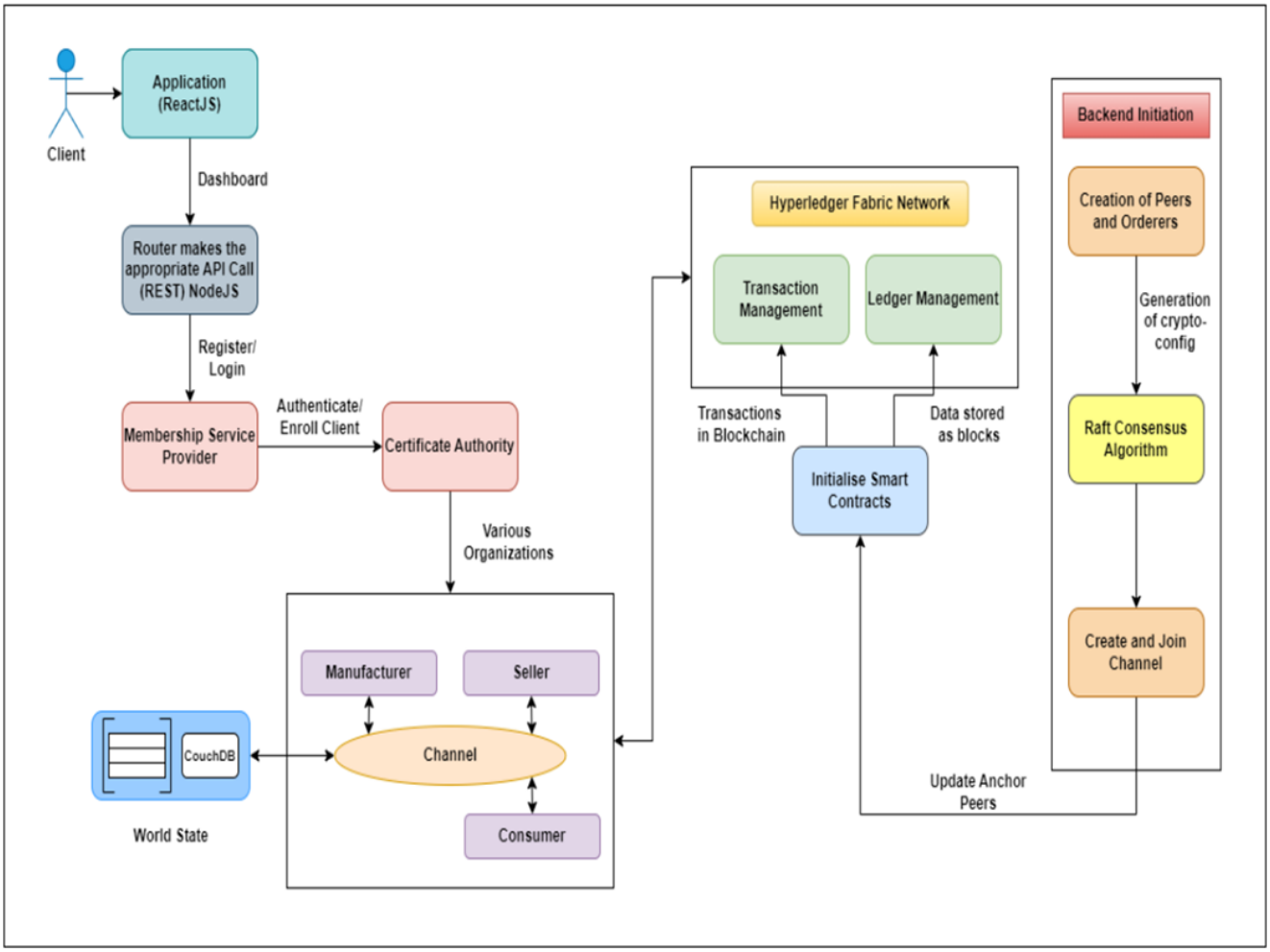

Fig 2. Architecture of Proposed framework

Table 2. Add Product, Seller and Consumer

Algorithm 1 Add Product	**Algorithm 2** Add Seller	**Algorithm 3** Add Consumer
Input: Product Id, Product Name, Brand, Colour, Price, Size, Owner, Seller Id **Function:**createProduct() this.ProductId ← Product Id this. Product Name ← Product Name this.Brand ← Brand this.Colour ← Colour this. Price ← Price this.Size ← Size this.Owner ← Owner this. Seller Id ← Seller Id **if** Arguments == 8 **then** Product []Product.JSON Add Product.JSON into the ledger **else** Throw error**end if**	**Input:**SellerId, Seller Name, Manager Name, ManagerId, Brand **Function** createSeller() this.SellerId ←Seller Id this.Seller Name ← Seller Name this.Manager Name← Manager Name this.ManagerId← ManagerId this.Brand← Brand **if** Arguments == 5 then Seller ←Seller.JSON Add Seller.JSON into the ledger **else**Throwerror**end if**	**Input**:ProductId, Product Name, Consumer Name, Address, Phone Number, Mail, Seller Id, Seller Name **Function**: createConsumer() this.ProductId← ProductId this.ProductName ← Product Name this.Consumer Name ←Consumer Name this.Address← Address this.PhoneNumber ← Phone Number this.Mail← Mail this.Seller Id ←Seller Id this.Seller Name ← Seller Name **if**Arguments == 8 then consumer ←onsumer.JSON Add consumer.JSON into the ledger **else**Throwerror**end if**
Algorithm 4 Query Products	**Algorithm 5** Query Sellers	**Algorithm 6** Query Consumers
Function: query AllProducts() Product[]+= get(Items From Ledger) return product; Input:Item Number **Function:** query Product() product←get(Item Number) return product:	**Function**: query AllSellers() seller[]+= get(sellersFrom Ledger) return sellers; **Input:**Seller Number **Function:**querySeller() seller←get(Seller Number) return seller:	**Function:** query AllConsumers() Consumer[]+= get(Consumers From Ledger) return consumer; **Input:**Consumer Number **Function:**queryConsumer() consumer get(Consumer Number) return consumer:
Algorithm 7 Change Product Owner	**Algorithm 8** Add Review	**Algorithm 9** Query Reviews
Input: Item Number, Owner **Function :** change ProductOwner() ProductIdGetStateByKey(ProductId) Set this.Owner Owner **if** Arguments == 2 **then** product product.JSON Add new product.JSONinto the ledger **else**Throwerror e**nd if**	**Input:** Product Name, Seller Name, Rating **Function:** add review() this.Product Name ← Product Name this.Seller Name ← Seller Name this.Rating ← Rating **if**Arguments == 3**then** review review.JSON Add review.JSON into the ledger **else**Throwerror**end if**	**Input:**Product Name **Function :**queryreview() Product Name ← GetStateByKey (Product Name) **if** Product Name.hasFound()**then** Display all the review ratings of the product return true; **else**returnfalse;**end if**

2.3. Smart Contracts and Chaincode

The smart contract for adding and querying the product, seller, and customer is elaborated in this section. Adding a product, a manufacturer must create a distinctive digital record of the product on the blockchain network to add it to the network. The product's name, product ID, brand, price, size, and any other pertinent information are all included in this record. The first step would be for the manufacturer to log in using the admin-provided credentials, which are authenticated. The second step includes adding a new transaction to the blockchain that contains the product identifier as well as any other crucial information. The manufacturer would then have to broadcast this transaction to the network so that other users could confirm it. Upon confirmation of the transaction, the item's digital record will be added to the blockchain. Adding Seller, the seller's name, seller ID, manager name, manager ID, and brand are included in this record. The manufacturer would then have to broadcast this transaction to the network and get it verified by the neighboring nodes within the confines of the smart contract defined below; upon confirmation of the transaction, the seller record would be added to the blockchain. Adding Consumer: a seller must create a unique digital record of the consumer on the blockchain network to add it to the network. The consumer's name, email address, phone, and other pertinent information are all included in this record. The first step would be for the seller to log in using the authenticated admin-provided credentials. The second step includes adding a new transaction to the blockchain that contains the consumer identifier as well as any other crucial information. The seller would then have to broadcast this transaction to the network so that other users could confirm it by agreeing upon the smart contracts defined. Upon confirmation of the transaction, the consumer's digital record would be added to the blockchain. The algorithm for adding product, seller and consumer is given in Table 2: algorithm 1, 2, and 3. Query Product/Query Consumer/Query Seller: While querying on the network, a specific search identifier is asked for, and the application search tool would then return the relevant data, which

includes product, seller, and consumer details, stored on the blockchain. The smart contract will retrieve the data, iterate it and send it to the front-end. The algorithm for querying the product, seller, and consumer are given in Table 2: algorithm 4, 5, 6.

Our blockchain system provides a transparent and immutable record of the contract's execution and state changes as they occur. The product moves from one hand to another in the chain, which requires transparency and security. A high level of security and transparency in contract execution can be achieved with blockchain smart contract authentication, which takes the unique identifier as input and gives out the details of the product if registered with the blockchain's immutable records. The smart contract would create a new transaction on the blockchain connecting the previous transactions which were held by the preceding owner. The typical process would involve verifying the current owner; once verified; transfer it to the new owner by adding the new transaction and getting it verified by the neighboring nodes. Once verified, the transaction is updated in the product record. The process also includes the option for the customer to review the product they have purchased in order to recommend other consumers to buy the product from the particular seller or not. The algorithm to change owner, add review and query review are given in Table 2: algorithms 7, 8, 9. The process typically involves identifying the asset that needs to be queried and then querying the blockchain with the help of the smart contract. Once the verified records are retrieved, iterate through all the records and display them on our front-end application. Query Purchase History of Consumer query uses the consumer's contact number to find the products that the consumer has purchased.

2.4. Client Application

The user- friendly interface for manufacturer, seller and customers is very essential[11] for a supply chain system. The user interface is often referred to as the client application for our blockchain fake product identification application. The users can interact with the blockchain using this application. Different tasks like adding products, sellers, customers, product reviews, and querying are carried out using this application interface. Upon redirecting to different pages and providing the required inputs, endpoints are triggered in the backend, which gives back the response for a valid query to be rendered on the front end. Manufacturers, as they log in, can add product details and seller details as well as view consumers who have bought their products. Sellers, as they log in, can add consumers, query the products they have, and view the list of products and consumer details. Consumers who log in can authenticate the product they have bought and check if the product has really come from the manufacturer by checking its history. They can also drop in the reviews of the product and query them. The manufacturer dashboard, seller dashboard and consumer dashboard are given in Figures 3 and 4, and Figure 5, respectively. The products, sellers, consumers and reviews, added using smart contracts, are stored in the ledger and are queried from **the ledger.**

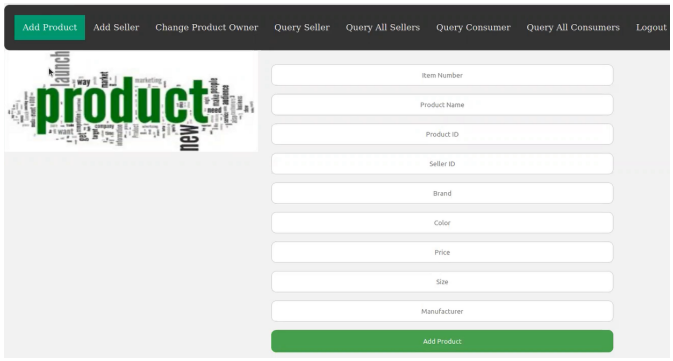

Fig 3. Manufacturer Dashboard for adding and querying

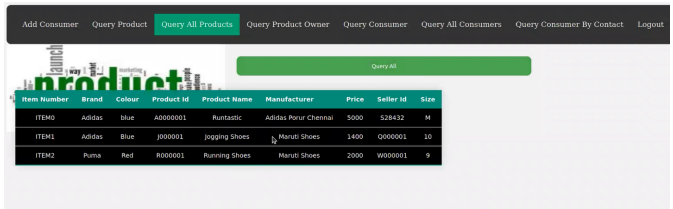

Fig 4. Seller Dashboard for adding and querying

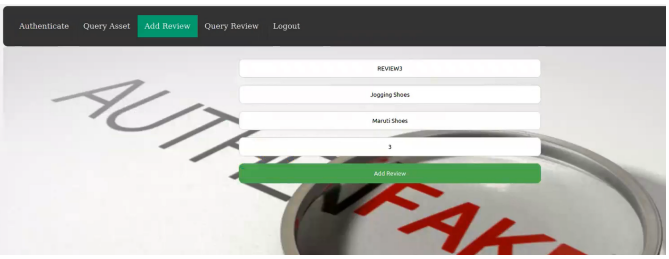

Fig 5. Consumer Dashboard for adding and querying .

3 Results and discussion

A system for identifying fake products using blockchain technology may be an efficient way to deal with the rising issue of counterfeit goods[12]. The blockchain-based security systems can be applied to any application, such as cross-border e-commerce systems[13] integrated circuits (IC)[14], pharmaceutical supply chains[15], and many others. A secure and unchangeable record of the complete supply chain, from the manufacturer to the final consumer, can be provided via our end-to-end blockchain system[16] [17] [18].

By using blockchain technology, our fake product identification system can offer several advantages, like - increased transparency and accountability in the system, as manufacturers, Sellers and consumers can access and verify the product information; Improved traceability, as the blockchain records can provide a complete history of the product's journey from the manufacturer to the consumer using our query history product feature with which any of the consumers can trace the roots of the product.

With the RAFT consensus algorithm, the security aspect is taken care of, as in raft, the immutable and the requirement for consensus from neighboring nodes of the blockchain ensures that the product information is tamper-proof. By introducing a token for login for users, the risks of fraud and counterfeiting have been reduced, as the blockchain-based system can detect and prevent any attempts to introduce fake products into the supply chain in case the token is invalid. We measure all successful transactions for a test cycle.

We also measure the time it takes for an issued transaction to be completed and for a response to be available to the application that issued the transaction. The maximum, minimum and average latency for the test cycle is provided inFigure 6. In our system, we have three major types of transactions: insert or add a new transaction onto the block, query the already existing blocks and query all the transactions based on the given attribute. We compare the Transaction Send Rate vs the Average Latency for each one of them, and the comparison is shown in Figure 7.

CPU consumption for Add, Query and Query-all are respectively 1.81%, 1.11% and 1.27%. CPU usage statistics are obtained using the command docker stats, which provides real-time resource usage statistics.

Memory consumption for Add Query and Query all are respectively 53MB, 45MB and 92 MB. Memory usage can be recorded periodically to evaluate the resource utilization and efficiency of the blockchain framework. Proposed work adopts a minimalist approach by utilizing minimal services and optimizes memory usage and allocates resources more efficiently by avoiding unnecessary or redundant services. Additionally, ledger is maintained in a JSON format, a lightweight data-interchange format that is easy to parse and consumes less memory than other formats such as XML. The proposed work minimizes the memory requirements for storing and processing the ledger information by storing the ledger data in JSON format.

4 Conclusion

This study introduces a novel approach to combating counterfeit products by using blockchain technology which provides a user friendly interface for the manufacturer, seller and customer. The consumer can submit a review on the product they purchased. This review, which is stored on the blockchain, can be used by other sellers and consumers to verify that a manufacturer is genuine. The deeper integration of consumer reviews within the system offers a novel approach to enhancing trust and transparency in the verification process. Our study details the transaction send rate and average latency for different transaction types. CPU consumption for Add, Query, and Query-all transactions is 1.81%, 1.11%, and 1.27%, respectively, while memory consumption is 53MB, 45MB, and 92MB, respectively. Our current implementation involves only three parties—manufacturers, consumers, and sellers—excluding second-hand buyers. Future efforts will address this limitation by expanding the system to include second-hand buyers, making it more user-friendly and effective.

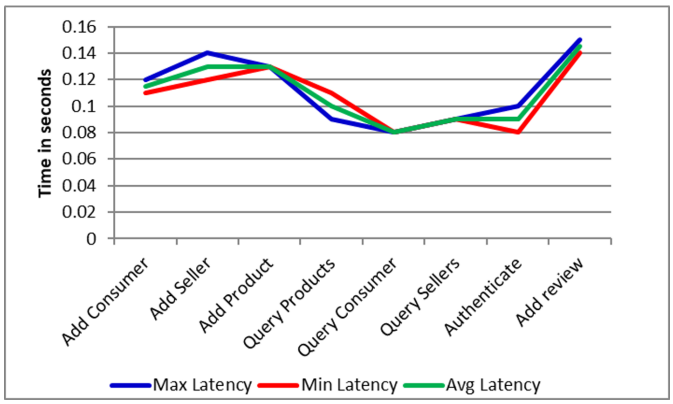

Fig 6. Maximum, minimum and average latency for the type of transactions

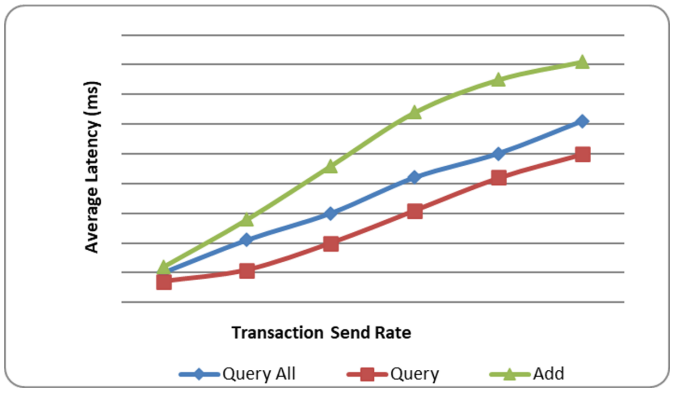

Fig 7. Transaction Send Rate vs the Average Latency

References

1) Kumar TA, Kumar V, Pal R, Wang L, Chen Y. Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry. *Computers & industrial engineering*. 2021;107130. Available from: https://doi.org/10.1016/j.cie.2021.107130.
2) Tfl. 2021. Available from: https://www.thefashionlaw.com/?cat=&s=Nearly+1+in+10+EU+Consumers+Have+Mistakenly+Purchased+a+Counterfeit+Product+Over+the+Past+Year.Dateaccessed:23/04/2024.
3) Pun H, Swaminathan JM, Hou P. Blockchain adoption for combating deceptive counterfeits. *Production and Operations Management*. 2021;30:864–82. Available from: https://doi.org/10.1111/poms.13348.
4) Onu P, Mbohwa C, Pradhan A. Blockchain-Powered Traceability Solutions: Pioneering Transparency to Eradicate Counterfeit Products and Revolutionize Supply Chain Integrity. *Procedia Computer Science*. 2024;232:1420–1427. Available from: https://doi.org/10.1016/j.procs.2024.01.140.
5) Islam I, Islam MN. A blockchain based medicine production and distribution framework to prevent medicine counterfeit. *Journal of King Saud University-Computer and Information Sciences*. 2024;36(1):101851–101851. Available from: https://doi.org/10.1016/j.jksuci.2023.101851.
6) Gupta S, Kuchipudi R, Sohail M, Singh K, Mahalakshmi J, Sarabu A. Fake Product Identification for Small and Medium Firms (FPISMF) Using Blockchain Technology. *Measurement: Sensors*. 2024;p. 101164–101164. Available from: https://doi.org/10.1016/j.measen.2024.101164.
7) Mohammed M, Alzahrani M, Hejjou A, Alharby M. TrustChain: Trusted Blockchain-Based System for Supply Chain Traceability. *Arabian Journal for Science and Engineering*. 2024;23:1–9. Available from: https://doi.org/10.1007/s13369-024-08900-2.
8) Cammillus S, Balakrishnan M, Gopinath B, Sm TK. A Blockchain-Based Solution for Counterfeiting in Textile Industry. *Journal of Systems Engineering and Electronics*. 2024;34(4):1671–1793. Available from: https://doi.org/10.1007/978-981-13-0080-6_10.
9) Pradeep R, Sunitha NR. A Reliable Blockchain Based Biometric Authentication Solution for Aadhar. *Indian Journal of Science and Technology*. 2022;15(41). Available from: https://doi.org/10.17485/IJST/v15i41.658.
10) Das TM, Khan MM, Kaur M, and AZ. Smart supply chain management using the blockchain and smart contract. *Scientific programming*. 2021;2021:1–12. Available from: https://doi.org/10.1155/2021/6092792.
11) Dayma N, Badwane S, Bhole C, Mahajan M. Fake Product Detection using Blockchain. In: 6th International Conference on Advances in Science and Technology (ICAST). 2023;p. 223–228. Available from: https://doi.org/10.1109/ICAST59062.2023.10454928.
12) Tyagi I, Gupta R, Upadhyay D, Dubey AK, Jabbar MA, Tiwari S, et al. Blockchain - A Secure and Transparent Solution to Detect Counterfeit Products. *Machine Learning and Data Analytics* . 2024. Available from: https://doi.org/10.1007/978-3-031-55486-5_4.
13) Lee H, Yeon C. Blockchain-based traceability for anti-counterfeit in cross-border e-commerce transactions. *Sustainability*. 2021;13(19):11057–11057. Available from: https://doi.org/10.3390/su131911057.

14) Aniello L, Halak B, Chai P, Dhall R, Mihalea M, Wilczynski A. Anti-BlUFf: towards counterfeit mitigation in IC supply chains using blockchain and PUF. *International Journal of Information Security*. 2021;20:445–60. Available from: https://doi.org/10.1007/s10207-020-00513-8.
15) Kordestani A, Oghazi P, Mostaghel R. Smart contract diffusion in the pharmaceutical blockchain: the battle of counterfeit drugs. *Journal of Business Research*. 2023;158:113646–113646. Available from: https://doi.org/10.1016/j.jbusres.2023.113646.
16) Hald K, Sundtoft A, Kinra. How the blockchain enables and constrains supply chain performance. *International journal of physical distribution & logistics management*. 2019;49:376–397. Available from: https://doi.org/10.1108/IJPDLM-02-2019-0063.
17) Kumar A, Liu R, Shan Z. Is blockchain a silver bullet for supply chain management? Technical challenges and research opportunities. *Decision Sciences*. 2020;51(1):8–37. Available from: https://doi.org/10.1111/deci.12396.
18) Ali O, Jaradat A, Kulakli A, Abuhalimeh A. A comparative study: Blockchain technology utilization benefits, challenges and functionalities. *IEEE Access*. 2021;9:12730–12749. Available from: https://doi.org/10.1109/ACCESS.2021.3050241.