SECURE COUNTERFEIT PRODUCT DETECTION SYSTEM USING BLOCKCHAIN

Enroll No. (s) - 19803021, 19103061, 19803025

Name of Student(s) - Pranav Gupta, Aditya Kesarwani, Divyanshu Tiwari

Name of Supervisor(s) - Dr. Sangeeta Mittal

April 2023

Submitted in partial fulfillment of the Degree of

Integrated Master of Technology

in

Computer Science Engineering

Department Of Computer Science Engineering & Information Technology

Jaypee Institute of Information Technology

TABLE OF CONTENTS

DECLARATION

We hereby declare that this submission is our own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material that has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where the acknowledgement has been made in the text.

Place: Noida, U.P. **Signature:**

Date: 25-05-23 **Name:** Pranav Gupta, Aditya Kesarwani, Divyanshu Tiwari

Enrollment No: 19803021, 19103061, 19803025

CERTIFICATE

This is to certify that the work titled **" Secure Counterfeit Product Detection System Using Blockchain"** submitted by **Pranav Gupta (19803021), Aditya Kesarwani (19103061), and Divyanshu Tiwari (19803025),** in partial fulfillment for the award of the degree of Bachelor of Technology of the Jaypee Institute of Information Technology, Noida, has been carried out under my supervision. This work has not been submitted partially or wholly to any other university or institute for the award of this or any other degree or diploma.

Signature of Supervisor	……
Name of supervisor:	Dr. Sangeeta Mittal
Designation:	Associate Professor
Date:	09th November 2022

ACKNOWLEDGEMENT

It gives us immense pleasure to express our most profound sense of gratitude and sincere thanks to our most respected and esteemed guide, Dr. Sangeeta Mittal, for her valuable guidance, encouragement, and help in completing this work. Her useful suggestions for this whole work and her cooperative behavior are sincerely acknowledged. We would like to express our sincere thanks to her for giving us this opportunity to undertake this project. We would also like to express our indebtedness to our parents and the family members, whose blessings and support have always helped us face the challenges ahead.

Date: 09-12-22

Name: Pranav Gupta **Signature:** ……. **Enroll:** 19803021

Name: Aditya Kesarwani **Signature:** ……. **Enroll:** 19103061

Name: Divyanshu Tiwari **Signature:** ……. **Enroll:** 19803025

SUMMARY

The project will be a viable solution to this issue of blockchain-based skill verification because it offers a transparent, reliable, and independent platform and speeds up the process of product verification flawlessly. With blockchain, any user can enter their credentials and verify if their product was authentic. The allocation of product is done at various levels so as to prevent the fraud and counterfeiting. This ensures that all levels are covered under the blockchain and can be verified for secure transit of the product within the ecosystem.

Enrollment No.: 19803021 Name: Pranav Gupta
Enrollment No.: 19103061 Name: Aditya Kesarwani
Enrollment No.: 19803025 Name: Divyanshu Tiwari

Date: 02nd May 2023

Signature of Supervisor ……

Name of supervisor: Dr. Sangeeta Mittal

Designation: Associate Professor

Date: 09th November 2022

AuthentiFi

LIST OF FIGURES

AuthentiFi

LIST OF TABLES

LIST OF SYMBOLS AND ACRONYMS

1. NFT - Non fungible tokens
2. ATS - Applicant Tracking System
3. SSD - Solid State Drive
4. CSRF - Cross Site Request Forgery
5. XSS - Cross Site Scripting
6. DOM - Document Object Model

1. INTRODUCTION

This section gives a brief information about the necessity of detecting counterfeit goods as well as a brief introduction to the governmental organizations working on the above mentioned issue. Then the keywords are highlighted related to the blockchain niche so as to facilitate the ease of understanding. Then the comparison of various approaches is analysed to find the gaps in the previous studies.

1.1 General Introduction

The risk considerations like counterfeiting and duplication are always present when a technology or product is developed globally; these elements can have an impact on the reputation of the organization, its revenue, and the wellbeing of its customers. The supply chain contains a huge number of products. to verify whether the product is genuine or not. Manufacturers are suffering the worst difficulties and the greatest losses as a result of counterfeit or phony goods. We can use blockchain technology to determine whether a product is authentic or not.

Blockchain is a system for storing data that makes it challenging or difficult to alter, hack, or defraud the system. A blockchain is essentially a network of computer systems that copy and distribute a digital record of transactions across the whole network. Several transactions are included in each block of the chain, and each time a new transaction takes place on the blockchain, a record of that transaction is added to the records of all participants. Distributed Ledger Technology (DLT) refers to the decentralized database that is controlled by several users (DLT). Transactions on a blockchain are recorded with an immutable cryptographic signature known as a hash.

Blockchain technology aids in addressing the issue of product counterfeiting. Technology based on blockchain is more secure. A chain will be constructed for that product's transactions once it is stored on the network, making it possible to keep all transaction records for both the product and its present owner. In the blockchain, all transaction histories will be kept as blocks. With the suggested system, each product is given a generated QR code that the end user can scan to learn

all there is to know about that product. We can tell whether a product is genuine or phoney by scanning the QR code.

Risk factors like forging and duplication frequently accompany the global enhancement of a product or innovation. The reputation of the company and the well-being of the customer can both be affected by forging. Nowadays, finding fake items is the biggest test. False goods have a serious negative effect on the organization and the clients' welfare. As a result, product makers are facing severe hardship. India and other countries are fighting against such phony and counterfeit goods. The suggested framework generates QR codes by employing blockchain technology. Blocks are used to hold exchange records in this innovation. Data stored in these squares cannot easily be accessed or changed. A QR code can be used to identify bogus goods.

1.2 Problem Statement

To make a decentralized counterfeit product detection system and a tamper-proof data storage system to store product details and get the consumers to verify the same. The primary objective of this problem statement is to detect if a malicious/ unauthenticated user is selling the product. And, if an invalid/ ineligible user is detected, then the registration/transaction must be blocked by the contract itself. It does this with the help of a new emerging technology, namely, Solidity, which has the provisional or conditional execution of functions. The functions get executed only by authenticated users and even authenticated users can perform authenticated operations

1.3 Significance and novelty of the problem

The Importance of Counterfeiting Detection in today's scenario: Counterfeiting is the act of producing fake or imitation goods or currency with the intent to deceive or defraud. Counterfeiting is a significant issue that affects various industries, including fashion, electronics, pharmaceuticals, and even currency. In the current environment, detecting counterfeiting is crucial for a number of reasons:

1) Consumer protection: Since counterfeit products are often of lower quality, using them can have serious negative effects, including health hazards and financial loss.

Additionally, it is possible for sophisticated quality items to damage goodwill because consumers cannot tell the difference between an original and an imitation simply by looking at the product. Companies can shield consumers from these dangers by spotting counterfeit goods.

2)Brand protection: Products that are counterfeit hurt businesses and their brands' reputations. Losses in revenue, market share, and consumer loyalty may result from them. Businesses may safeguard their brands and preserve their reputation by spotting counterfeiting and taking appropriate action.

3) Revenue protection: Both businesses and governments lose money as a result of counterfeiting. Both businesses and governments lose money when their items are imitated since counterfeiters don't pay taxes. Businesses and governments can safeguard their sources of income by spotting counterfeits.

4) Protection of intellectual property : By replicating trademarks, patents, and copyrights, counterfeiters frequently violate intellectual property laws. Companies may safeguard their intellectual property and stop further violations by identifying counterfeit goods.

5) National security: Counterfeit currency is a significant threat to national security. It can be used to finance terrorism, the trafficking of illegal substances, and other wrongdoing. Governments can protect their citizens and uphold national security by spotting counterfeit money.

For a variety of reasons, including the protection of customers, brands, revenue, intellectual property, and national security, it is crucial to find counterfeit goods nowadays. Governments and businesses alike must make investments in the tools and methods that help identify and stop counterfeiting.

In addition to defending the reputation and financial success of companies who manufacture and sell legitimate products, the relevance of counterfeit product identification rests in protecting customers from potentially hazardous and subpar products. Following are some justifications for the significance of fraudulent product detection:

1.4 Empirical Study

Not just India, Counterfeiting is a problem existing worldwide. Thus, there are several governmental bodies that coordinate counterfeit detection efforts worldwide. A few of them are listed here:

Interpol: The International Criminal Police Organization, or Interpol, coordinates global police cooperation against counterfeiting and other forms of transnational crime. It provides a central platform for exchanging information and conducting joint operations to disrupt counterfeiting networks. Interpol

Europol: The European Union's law enforcement agency, Europol, works to combat counterfeiting and other types of organized crime within the EU. Europol provides support to national law enforcement agencies and facilitates cross-border cooperation and information sharing. Europol

U.S. Customs and Border Protection (CBP): The CBP is responsible for securing U.S. borders and facilitating lawful trade and travel. It works to prevent the entry of counterfeit goods into the U.S. by intercepting suspicious shipments and conducting targeted enforcement actions.

The number of organisations spread worldwide emphasises on the importance of counterfeiting detection. Even in India, Many bodies look into this matter, but there is still no independent body that is solely responsible for the counterfeiting. Thus it becomes even more important for the firm to stop these activities. USCBP

In India, there are several government bodies responsible for detecting counterfeit goods. Some of the major ones are:

Central Board of Indirect Taxes and Customs (CBIC) - CBIC is responsible for enforcing customs and excise laws in India. They have a specialized wing called the Directorate of Revenue Intelligence (DRI) that deals with detecting and preventing smuggling and counterfeit goods. CBIC

Department for Promotion of Industry and Internal Trade (DPIIT) - DPIIT is a department under the Ministry of Commerce and Industry that is responsible for promoting and regulating industrial development in India. They have a cell called the Cell for IPR Promotion and Management (CIPAM) that focuses on protecting and enforcing intellectual property rights, including the prevention of counterfeit goods. DPIIT

Indian Patent Office (IPO) - The IPO is responsible for granting patents and trademarks in India. They have the power to take action against the infringement of patents and trademarks, which includes the sale of counterfeit goods. IPO

Food Safety and Standards Authority of India (FSSAI) - The FSSAI is a statutory body under the Ministry of Health and Family Welfare that regulates food safety and standards in India. They have the power to take action against the sale of counterfeit food products. FSSAI

State Police - State police forces are responsible for maintaining law and order within their respective states. They often collaborate with other government bodies to detect and prevent the sale of counterfeit goods.

Qualitative analysis is required for some research experiments because quantitative methods are inapplicable. In many instances, detailed information is required, or a researcher may need to watch the behaviour of a target audience; as a result, descriptive results are required. Results from qualitative research won't be prescriptive; they'll be more descriptive. It gives the researcher the chance to develop or support theories for potential quantitative study in the future. In such a case, a conclusion is drawn to support the theory or hypothesis under study using qualitative research methodologies. The subsequent field study was conducted

What is Blockchain

In contrast to traditional server-oriented architectures, blockchain has evolved as a trustworthy and robust technology. Blockchain is a method of storing and committing data that makes it extremely impossible to manipulate, edit, hack, or influence the system. A blockchain is a distributed digital ledger of transactions that is duplicated at every node and spread over the whole blockchain network of computer systems.

The Genesis block is the initial block, and each subsequent block carries the previous block's hash address. Each block includes data about transactions, timestamps, and hash addresses of its own block and the block before it, as well as other information. The following block will have the same unaltered hash as the previous block, disregarding this block and all succeeding blocks, even though the data has been changed. The blocks in the networks are kept in a Merkle tree, and each block has the appropriate Merkle root hash. It uses the idea of proof of work to prevent tampering, which delays the generation of new blocks and requires a significant amount of computer power to find the next valid block hash.

Solidity:

Solidity is a smart contract programming language native to Ethereum. Due to its potential to implement smart contracts on blockchains, it has been a hot topic for a while. Solidity programming uses a language that is comparable to C or C++ and JavaScript to solve real-world challenges in a straightforward manner. Right now, smart contracts may be created using Solidity programming for a variety of purposes, including voting, crowdfunding, blind auctions, and multi-signature wallets.

Smart Contract:

Simply put, smart contracts are blockchain-based programmes that execute when certain criteria are met. They are often used to automate the implementation of an agreement so that all parties can be certain of the conclusion right away, without the need for an intermediary or additional delay. They can also automate a workflow such that when circumstances are met, the following action is executed.

Truffle Compile & Test:

Truffle includes an automated testing framework as standard to make it simple to test our contracts. We may create small, manageable tests using this framework in a variety of ways.

Migrate to local Blockchain Ganache: A virtual blockchain called Ganache, formerly known as Testrpc, creates 10 default Ethereum addresses, complete with private keys, and pre-loads each one with 100 simulated ethers. It then instantly confirms any transaction that comes its way.

The ability to deploy smart contracts, play around, call functions, and then tear it all down for more simulation or new tests while returning all addresses to their starting state of 100 Ether makes it possible to use iterative development.

MetaMask Wallet Connection: A software cryptocurrency wallet called MetaMask is used to communicate with the Ethereum network. Users can utilise a browser extension or mobile app to access their Ethereum wallet, which can then be used to connect with decentralised applications. ConsenSys Software Inc., a blockchain software business that specialises in Ethereum-based infrastructure and tools, is the company behind MetaMask.

1.5 Brief Description of the solution Approach

Our technology for detecting fake products is intended to address the market's rising counterfeiting issue. We have developed a safe and decentralised platform using blockchain technology that enables producers, sellers, and buyers to confirm the legitimacy of products.

Each product is given a distinct digital signature when it is manufactured, which is how the system functions. An unchangeable record of the product's origin and legitimacy is then created and kept with this signature on the blockchain.

When a customer buys something, they can use their smartphone to scan the QR code, which will then ask the blockchain for the product's signature. The customer can be sure that the product is genuine if the signature is valid.

Similar to retailers, suppliers can utilise the system to confirm the legitimacy of the goods they receive from them. They can verify that the goods are authentic and unaltered by scanning the QR codes on the products.

Overall, our system for verifying counterfeit products offers a safe and effective means of addressing the issue of illegally produced commodities on the market. We can establish a transparent and reliable supply chain that benefits producers, retailers, and customers by utilising the potential of blockchain technology.

1. Blockchain-based authentication: The usage of blockchain technology is the cornerstone of our strategy for product authentication. Every item included on the blockchain has a

distinct digital signature. A collection of distinctive identifiers, such as a product serial number, batch number, and production location, is used to form the signature encrypted using a private key. This establishes an immutable record of the product's origin and legitimacy that can be accessed by anybody with access to the blockchain.

2. Decentralized platform: The blockchain works on the concept of decentralization that means there is no centralized entity working for the maintenance of the project hence avoids the possibility of centralised attack mechanisms like DOS attack, DDOS attack and other possible attacks.
3. QR code scanning: Each product has a unique QR code printed on its packaging to make it easier for customers and retailers to access the blockchain and verify product legitimacy. Consumers and retailers can use their smartphone's camera to scan the code, which will then query the blockchain for the product's signature. The product is regarded authentic if the signature matches the product's unique identifiers.
4. Transparency and traceability: One of the solution's primary advantages is the transparency and traceability it delivers across the supply chain. Every transaction on the blockchain is recorded and accessible to all participants. This provides an audit trail of the product's path from manufacture to sale. Furthermore, any attempts to tamper with the product's signature or change the product's information will be recognised immediately by the blockchain.
5. Improved security: This solution improves security in order to address the problem of counterfeit goods. By creating an immutable record of a product's authenticity, counterfeiters find it considerably more difficult to recreate the goods and pass it off as genuine. Additionally, the decentralized nature of the platform and the usage of encryption and private keys make it much tougher for hackers to interfere with the blockchain.

1.6 Comparision of existing approaches to the problem framed

There are various possibilities when examining current methods for the issue of counterfeit goods detection. To guarantee the validity of the goods, one strategy is to employ conventional

authentication techniques like serial numbers, holograms, and other physical security measures. However, these techniques are frequently not reliable and are simple for counterfeiters to copy. Another strategy involves using blockchain technology to produce a tamper-proof history of the product. It is possible to guarantee that a product is real and unaltered by putting information about it on the blockchain. However, this strategy needs a lot of infrastructure and might be challenging to put into practise.

The decentralised, Solidity-based counterfeit product detection system suggested in this research provides a number of advantages over these current methods. It combines the immutable record-keeping capabilities of blockchain technology with the conditional execution of Solidity functions to guarantee that only authenticated users can carry out authorised system actions. The method also makes it simple for customers to confirm the legitimacy of the item they are buying. Overall, this method provides a more decentralised and safe solution to the issue of detecting fake goods.

2. Literature Survey

This section highlights previous work done in the area that has been published in a number of research papers that have been presented at conferences and publications. This aided in assessing the drawbacks of earlier efforts and provided insight into potential techniques, filling in the gaps left by earlier studies.

2.1 Summary of Papers Studied

Table 2.1.1: Paper 1

Paper Title	A Blockchain-Based Fake Product Identification System

Author	Dabbagh, Yasmeen, and Khoja, Reem and AlZahrani, Leena and AlShowaier, Ghada and Nasser, Nidal
Publisher	2022 5th Conference on Cloud and Internet of Things (CIoT)
Year	2022
Summary	This research paper proposes a novel approach to combat the problem of counterfeit products using blockchain technology. Counterfeit products are a significant problem that affects consumers, businesses, and the economy as a whole. Current methods of identifying counterfeit products are often inadequate, as they rely on physical labels or serial numbers that can be easily replicated. The paper describes the implementation of the proposed system using the Hyperledger Fabric blockchain framework. The authors also conduct a security analysis of the system to ensure its robustness against various attacks. The proposed system has several advantages over traditional methods of counterfeit detection, including its ability to track products throughout the supply chain, its resistance to tampering, and its decentralized nature. The system can also provide valuable data to manufacturers and regulators to help identify and prevent counterfeiting.

Table 2.1.2: Paper 2

Paper Title	Optimized Combination of e-commerce Platform Sales Model and Blockchain Anti-Counterfeit Traceability Service Strategy

Author	Guo, Fangfang and Ma, Deqing and Hu, Jinsong and Zhang, Lu
Publisher	IEEE Access
Year	2021
Summary	The research paper proposes a new strategy for combating counterfeiting in e-commerce using a combination of blockchain technology and an optimized sales model. The authors begin by discussing the prevalence of counterfeiting in e-commerce and the limitations of current anti-counterfeiting measures. The proposed strategy involves using blockchain technology to create a transparent and traceable supply chain, allowing customers to verify the authenticity of products. The authors also propose an optimized sales model that incentivizes legitimate suppliers and discourages counterfeiters. The authors evaluated the effectiveness of the proposed strategy using a simulation model and compared it with traditional anti-counterfeiting measures. The results showed that the proposed strategy was more effective in reducing the prevalence of counterfeit products and increasing customer trust in the e-commerce platform. The research paper presents a promising new strategy for combating counterfeiting in e-commerce using blockchain technology and an optimized sales model. The proposed strategy addresses the limitations of current anti-counterfeiting measures and has the potential to increase customer trust in e-commerce platforms.

Table 2.1.3: Paper 3

Paper Title	An Ethereum based Fake Product Identification System using Smart Contract
Author	S, Balasubramani and Pramanick, Soumen and Singh, Rohit and Kumar, Dhananjay
Publisher	2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS)
Year	2022
Summary	This research paper proposes an Ethereum-based solution for identifying and combating counterfeit products using smart contracts. The use of smart contracts ensures that the system operates autonomously, without any intervention from intermediaries. The paper highlights the problem of counterfeit products, which not only poses a threat to consumers but also affects the reputation of the manufacturers and the economy as a whole. The system is implemented using the Ethereum blockchain framework and smart contracts. The smart contract acts as an intermediary between the manufacturer and the consumer, allowing them to exchange product information securely and transparently. The paper discusses the implementation of the proposed system and its security analysis. The system provides several benefits, such as real-time product tracking, transparency, and tamper-proof data storage.

Table 2.1.4: Paper 4

Paper Title	Fabrication of Dynamic Holograms on Polymer Surface by Direct Laser Writing for High-Security Anti-Counterfeit Applications
Author	Miao, Jiahao and Ding, Xinghuo and Zhou, Shengjun and Gui, Chengqun
Publisher	IEEE Access
Year	2019
Summary	The authors begin by discussing the importance of anti-counterfeit measures in various industries, such as currency, passports, and consumer goods. They also highlight the limitations of current anti-counterfeit measures, such as holographic stickers, which can be easily replicated. The proposed method involves using direct laser writing to create dynamic holograms on polymer surfaces. The holograms are created by varying the thickness of the polymer surface using the laser, which creates a pattern that changes with viewing angle. The authors evaluated the effectiveness of the proposed method by comparing it with traditional holographic stickers and conducting experiments to test the durability and security of the holograms. The results showed that the holograms created using the proposed method were more secure and durable than traditional holographic stickers. The holograms were also able to display dynamic images and could be customized for specific applications. The research paper presents a promising new method for creating high-security holograms on polymer surfaces using direct laser writing. The method addresses the limitations of current anti-counterfeit measures and

	has the potential to be used in various industries to increase security and prevent counterfeiting.

Table 2.1.5: Paper 5

Paper Title	A Survey on Supply Chain Security: Application Areas, Security Threats, and Solution Architectures
Author	Hassija, Vikas and Chamola, Vinay and Gupta, Vatsal and Jain, Sarthak and Guizani, Nadra
Publisher	{IEEE Internet of Things Journal
Year	2021
Summary	The paper covers the various application areas of supply chain security, including logistics, manufacturing, and retail. It also explores the different types of security threats that can occur within a supply chain, such as theft, counterfeiting, and cyber attacks. The authors present various solution architectures that can be implemented to mitigate these threats and enhance the security of the supply chain.

	The paper concludes by highlighting the need for more research in the area of supply chain security and the importance of collaboration among various stakeholders to ensure a secure and resilient supply chain. This paper offers valuable insights into the current state of supply chain security and potential solutions for enhancing supply chain security in the future.

Table 2.1.6: Paper 6

Paper Title	Blockchain smart contracts: Applications, challenges, and future trends
Author	Shafaq Naheed Khan, Faiza Loukil, Chirine Ghedira-Guegan
Publisher	Peer-to-Peer Netw. Appl. 14
Year	2021
Summary	• This research paper presented a comprehensive survey of blockchain-enabled smart contracts from both technical and usage points of view. • Thus, it introduced a taxonomy of existing blockchain-enabled smart contract solutions, categorized and discussed the existing smart contract-based studies. Based on the findings from the survey, both smart contract challenges and open issues are identified to be addressed in further studies. And also it discussed future trends of smart contracts. This study provides informational support to stakeholders interested in the research of smart contracts.

Table 2.1.7: Paper 7

Paper Title	Security with holographic barcodes using Computer generated holograms
Author	Divya P.S and Sheeja M.K
Publisher	2013 International Conference on Control Communication and Computing (ICCC)
Year	2013

Summary	There is immense evolution of different technologies and methods used for product authentication and anti-counterfeiting measures. The use of holograms for product authentication has been around for several decades and involves applying a unique holographic label or seal to a product to verify its authenticity. Holograms are difficult to replicate and can provide a visual indication of the product's authenticity. Later, the use of databases was introduced, which allows for the storage and retrieval of product information. This enables companies to track products throughout their supply chain and verify their authenticity by comparing the information stored in the database. With the advancement of artificial intelligence (AI), machine learning algorithms can be used to analyze data and detect patterns that may indicate counterfeit products. AI can also be used to develop predictive models to identify potential counterfeiting threats before they occur. Now, blockchain technology is being used to provide a secure and decentralized platform for tracking and verifying product authenticity. The use of blockchain provides an immutable and transparent record of a product's entire supply chain, making it difficult for counterfeiters to tamper with the product's information.

Table 2.1.8: Paper 8

Paper Title	Exploring Web3 From the View of Blockchain
Author	Qin Wang, Rujia Li, Qi Wang, Shiping Chen
Publisher	arXiv

Year	2022
Summary	• Web3 is an emerging concept prevailing in the entire crypto-world. • Applications and services in the Web3 space, with non-custodial nature, allow users to control their data and obtain rewards. However, no clear definitions of such a buzzword have formed. • In this tech report, we fill the gap by investigating a large corpus of in the wild projects titled with Web3. • We dig into this topic by decoupling existing systems supporting blockchain-based Web3 services into separate core components, and accordingly discussing related features and properties for each potential combination.

Table 2.1.9: Paper 9

Paper Title	An IoT-Based Anti-Counterfeiting System Using Visual Features on QR Code
Author	Yan, Yulong and Zou, Zhuo and Xie, Hui and Gao, Yu and Zheng, Lirong
Publisher	IEEE Internet of Things Journal
Year	2021

Summary	The authors discuss the growing problem of counterfeit goods and the need for effective anti-counterfeiting measures. They propose a system that uses a QR code with visual features to provide a secure and reliable method of identifying genuine products. The system is based on the Internet of Things (IoT) technology, which enables real-time monitoring and tracking of products throughout the supply chain. The paper presents the architecture of the proposed system, which includes a visual feature extraction module, an IoT gateway, and a cloud platform. The visual feature extraction module uses a deep learning algorithm to extract unique features from the QR code, while the IoT gateway collects and transmits data to the cloud platform. The authors conducted experiments to evaluate the effectiveness of the proposed system, and the results show that it can accurately identify genuine products and detect counterfeit products with a high level of accuracy. So, the authors suggest that their proposed anti-counterfeiting system using visual features on QR code has the potential to be an effective solution to the growing problem of counterfeit goods, and can provide a reliable method of identifying genuine products throughout the supply chain. The paper offers valuable insights into the development of anti-counterfeiting measures and the use of IoT technology in supply chain management.

Table 2.1.10: Paper 10

Paper Title	Optimized Combination of e-commerce Platform Sales Model and Blockchain Anti-Counterfeit Traceability Service Strategy
Author	Guo, Fangfang and Ma, Deqing and Hu, Jinsong and Zhang, Lu

Publisher	IEEE Access
Year	2021
Summary	The paper presents the architecture of the proposed solution, which includes an e-commerce platform sales model, a blockchain-based anti-counterfeit traceability service, and an optimized combination strategy. The e-commerce platform sales model is designed to ensure the efficient and effective sale of goods, while the blockchain-based anti-counterfeit traceability service enables the secure and transparent tracking of goods throughout the supply chain. The authors conducted experiments to evaluate the effectiveness of the proposed solution, and the results show that it can effectively detect and prevent the sale of counterfeit goods, while also ensuring the efficient and effective sale of genuine goods. So, the authors suggest that their proposed optimized combination of e-commerce platform sales model and blockchain anti-counterfeit traceability service strategy has the potential to be an effective solution to the growing problem of counterfeit goods in e-commerce. The paper offers valuable insights into the development of anti-counterfeiting measures and the use of blockchain technology in supply chain management.

2.2 Integrated Summary

There is immense evolution of different technologies and methods used for product authentication and anti-counterfeiting measures.The use of holograms for product authentication has been around for several decades and involves applying a unique holographic label or seal to a product to verify its authenticity. Holograms are difficult to replicate and can provide a visual

indication of the product's authenticity. In essence, holograms are a matrix of dots used to create a collection of nanostructures. To set it apart from the others, they employ texture, color density, and light refraction. They have both overt and covert features; overt features can be seen and verified with the unaided eye and rely on optical tricks. The concealed characteristics, however, can only be read by specialized tools like the Engage ™ app.

This strategy's main drawback was that it only used physical means of verification; also, as technology develops, it becomes easier to replicate the hologram. There is yet another issue involving the digital items. Digital objects cannot be covered in holograms.

Information about products may now be stored and retrieved thanks to databases, which were later developed. By comparing the data saved in the database, this enables businesses to monitor products along their supply chain and confirm their legitimacy. But If the network is slow, and all the data is at one location. The searching process takes much time. All databases would be lost in the event of a central server failure. As all data is kept in one location, many users accessing it simultaneously could lead to numerous issues.When multiple records are accessed from the same location simultaneously, a collision will occur.

With the advancement of artificial intelligence (AI), machine learning algorithms can be used to analyze data and detect patterns that may indicate counterfeit products. AI can also be used to develop predictive models to identify potential counterfeiting threats before they occur.

Now, we have proposed a blockchain technology based approach that is being used to provide a secure and decentralized platform for tracking and verifying product authenticity. The use of blockchain provides an immutable and transparent record of a product's entire supply chain, making it difficult for counterfeiters to tamper with the product's information.

3. Requirement Analysis and Solution Approach

The overall description, several types of requirements, including functional and non-functional, hardware and software, as well as the suggested solution, will be presented in this section to help organise the activities that need to be completed while developing the structure of the project..

3.1 Overall description of the project

Because the project provides a transparent, dependable, independent platform and expedites the completion of competency testing, it will be a potential solution to the problem of counterfeit product identification. Using blockchain, every user may enter their credentials, check the history of purchases, and have those credentials openly verified by the manufacturers, sellers, and businesses at their respective ends. The project employs a three-level hierarchy between the manufacturer, the seller, and the customer. Products and merchants could only be added to the ecosystem by the manufacturer. The product is then sold by the manufacturer to the appropriate sellers. Then merchants (sellers) offer those goods for sale to potential customers. Customers may scan the product and enter their unique consumer codes to authenticate it, making it verified. Integrity checks are incorporated at each step to guarantee that only authorized individuals may carry out the transaction. Yet, the consumer is not linked to a specific account for the sole purpose of enhancing the convenience of authenticating from any location and using any technology. Yet, only the customers who are a part of the ecosystem could do this.

3.2 Requirement Analysis (Functional/Non-Functional/Logical Database requirements)

The initiative was implemented using Ethereum which is considered modular with fast execution as compared to others (Bitcoin). The following section shows the libraries/requirements for the project.

3.2.1 Software Requirements

- Operating System: Linux (Ubuntu), Windows, MacOs
- Node.js (https://nodejs.org/en/) & NPM installed
- Ganache (Remix IDE for contract finalization)
- Metamask Extension installed and running on your browser
- Supported Internet browser: Chrome - Latest version, or the penultimate version

3.2.2 Hardware Requirements

- CPU: 2 GHz processor (minimum)
- Computer Processor: Intel i5 or i7 core
- Computer Memory:
    1. Ram: 2GB or more
    2. HDD: 10 GB or more
- Graphics Hardware: Not required
- Network:
    1. A broadband internet connection with at least 2 Mbps upstream bandwidth.
    2. Firewall - to mask the control and command server from direct attacks and block unauthorized traffic to the monitoring dashboard.

3.2.3 Functional Requirements

1. The Manufacturer must be able to add the product and generate/download QR code after successfully completing the transaction.
2. The Manufacturer must be able to add the Seller after successfully completing the transaction.
3. The Manufacturer must be able to sell the registered products to the authenticated sellers.
4. The Manufacturer must be able to view all the authenticated/registered sellers.
5. The Seller must be able to sell product to the registered consumers.
6. The Seller must be able to see all the available products which are currently under his ownership.
7. The registered consumer must be able to verify the authenticity of the product.
8. The registered consumer must be able to see his/her purchase history that displays all the products bought so far.

3.2.4 Non-Functional Requirements

1. The system should facilitate ease of navigation around the site.
2. The system should use simple colors and fonts, keeping in mind the formal theme of the business world.
3. The system should integrate technical controls such as anti malware, anti denial and intrusion detection.
4. The response to a query should not take more than 10 seconds to load on the screen.
5. The system should provide portability i.e... it must be adoptable to Windows, Linux and MacOS and it must be compatible with the apps running in the background.

3.3 Solution Approach

There is an immense evolution of different technologies and methods used for product authentication and anti-counterfeiting measures. The use of holograms for product authentication has been around for several decades and involves applying a unique holographic label or seal to a product to verify it's authenticity. Holograms are difficult to replicate and can provide a visual indication of the product's authenticity. In essence, holograms are a matrix of dots used to create a collection of nanostructures. To set it apart from the others, they employ texture, color density, and light refraction. They have both overt and covert features; overt features can be seen, and verified with the unaided or naked eye and rely on optical tricks. The concealed characteristics, however, can only be read by specialized tools like the Engage ™ app.

The earlier strategy's main drawback was that it only used physical means of verification; also, as technology develops, it becomes easier to replicate the hologram. There is yet another issue involving the digital items. Digital objects cannot be covered in holograms, and with the advent of technology, digital goods are quite in fashion these days. Like the emerging NFT or digital goods like cryptowallets etc.

Information about products may now be stored and retrieved thanks to databases, which were later developed. By comparing the data saved in the database, this enables businesses to monitor products along their supply chain and confirm their legitimacy. But If the network is slow, and all the data is at one location. The searching process takes much time. All databases would be lost in

the event of a central server failure. As all data is kept in one location, many users accessing it simultaneously could lead to numerous issues.When multiple records are accessed from the same location simultaneously, a collision will occur. After proper research and analysis it was quite evident that physical means of verification was not sufficient in today's scenario as it was designed keeping in mind the technologies available in those times, but with current set of technologies, it is just a matter of seconds to imitate the holograms and security designs using digital art devices. Then other physical means of verifications were used which included the embedded holograms that make use of patterns and refraction of light at various angles to verify the genuineness but most of the time the customer fails to detect those minor specifications and gets trapped by the attacker.

The first and foremost challenge was the selection of available technologies to solve the above-mentioned problem. Artificial Intelligence or Machine learning wasone of the apt technologies but it carries with itself an implicit requirement of data from various users which might be a breach of privacy for various users and infact we need forged or counterfeited products to train our model on the dataset. The first mentioned issues after appropriate research was resolved using federated learning which means only the results are shared instead of the data, so there is no such data privacy. But for new firms the trianind data was not available and even for old firms training data for new products wasn't available.

Furthermore if a product is added on the blockchain network, it is quite difficult to mutate the blockchain. Almost 51% of majority consensus is required for the blockchain network to tamper. It made use of the solidity contracts which was the most appropriate as we can set up a new chain for products even if it's newly launched. It acts as an additional layer of security over the existing physical means of security.

Solidity smart contracts were developed to implement the product verification and registration functionality. The smart contracts were deployed on the Ethereum blockchain, which provided the necessary tamper-proof nature and decentralization. As Ethereum has switched to proof of Stake from proof of work. It lays even more exponential penalty in case an attacker tries to attack the ecosystem.

4. Modelling and Implementation Details

In this section, various design diagrams along with the implementation details of the main modules are presented so as to get a jist of the overall project in action and understand how the important functions are providing an additional layer of security with the use of require keyword.

4.1 Design Diagrams

4.1.1 Use Case Diagram :

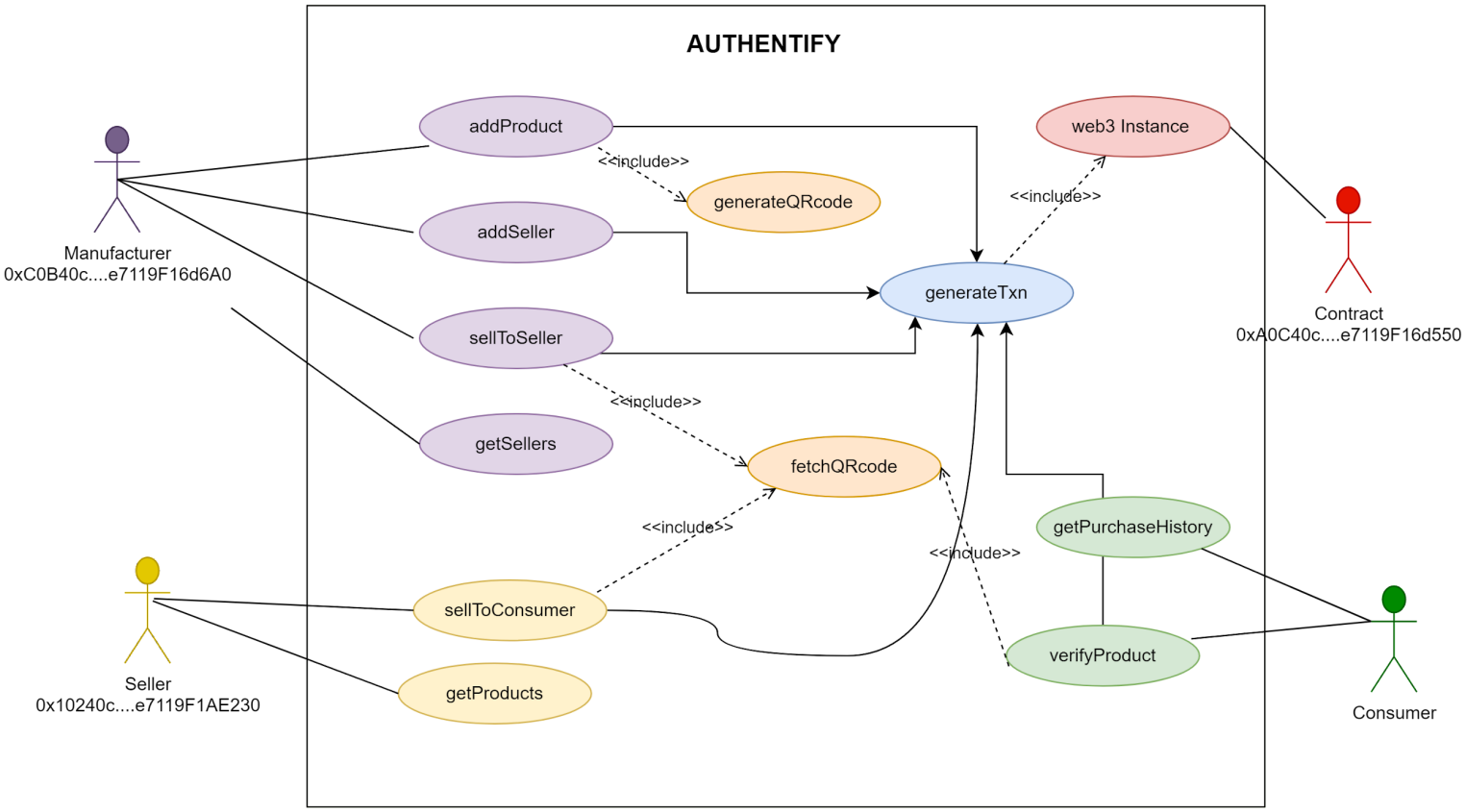

Figure 4.1.1 Use Case Diagram

4.1.2 Sequence Diagram

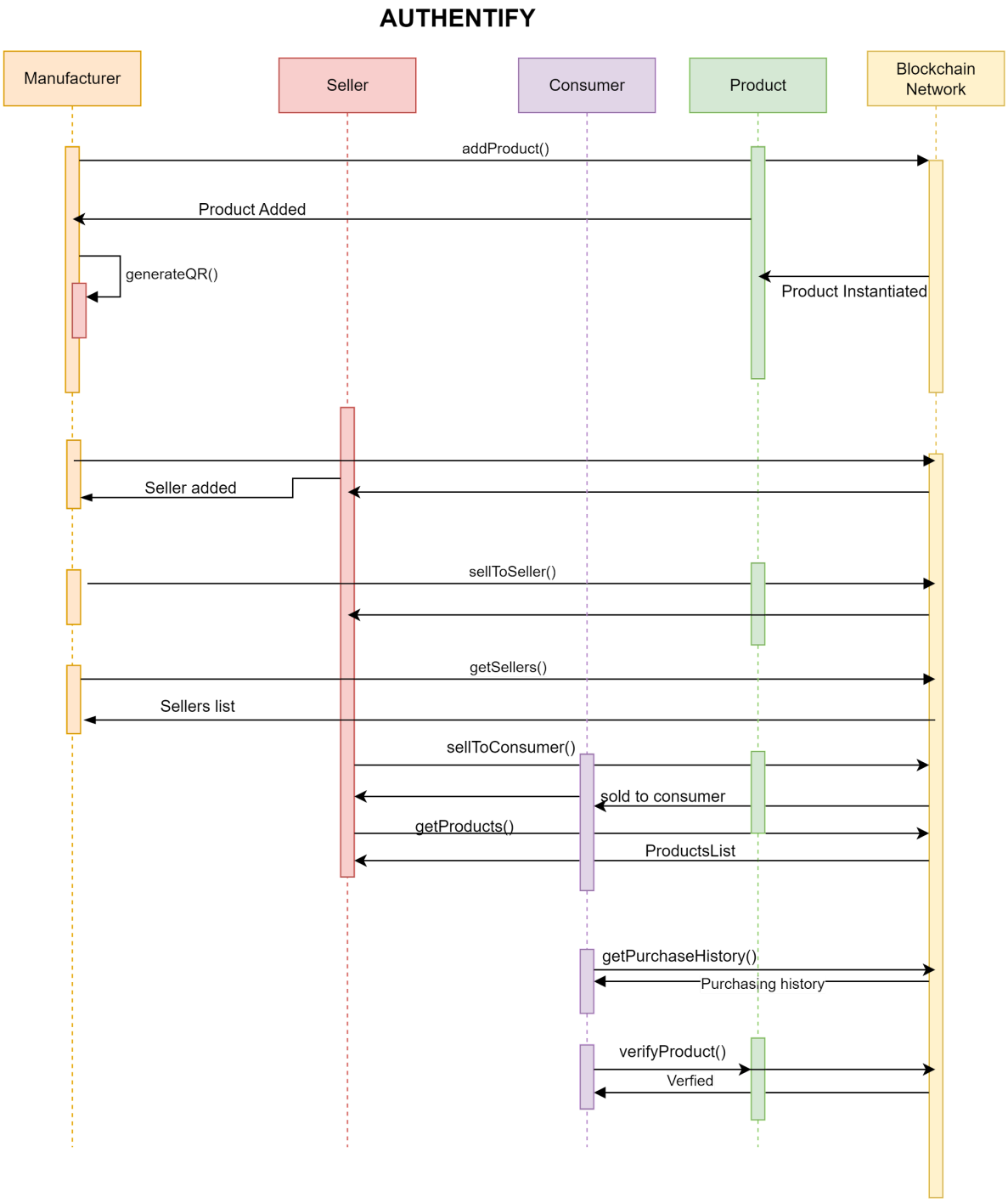

Figure 4.1.2 Sequence Diagram

4.1.3 Process Diagram

The Decentralized Counterfeit Product Detection and Tamper-Proof Data Storage System was implemented using the Ethereum blockchain and Solidity smart contracts. The following are the

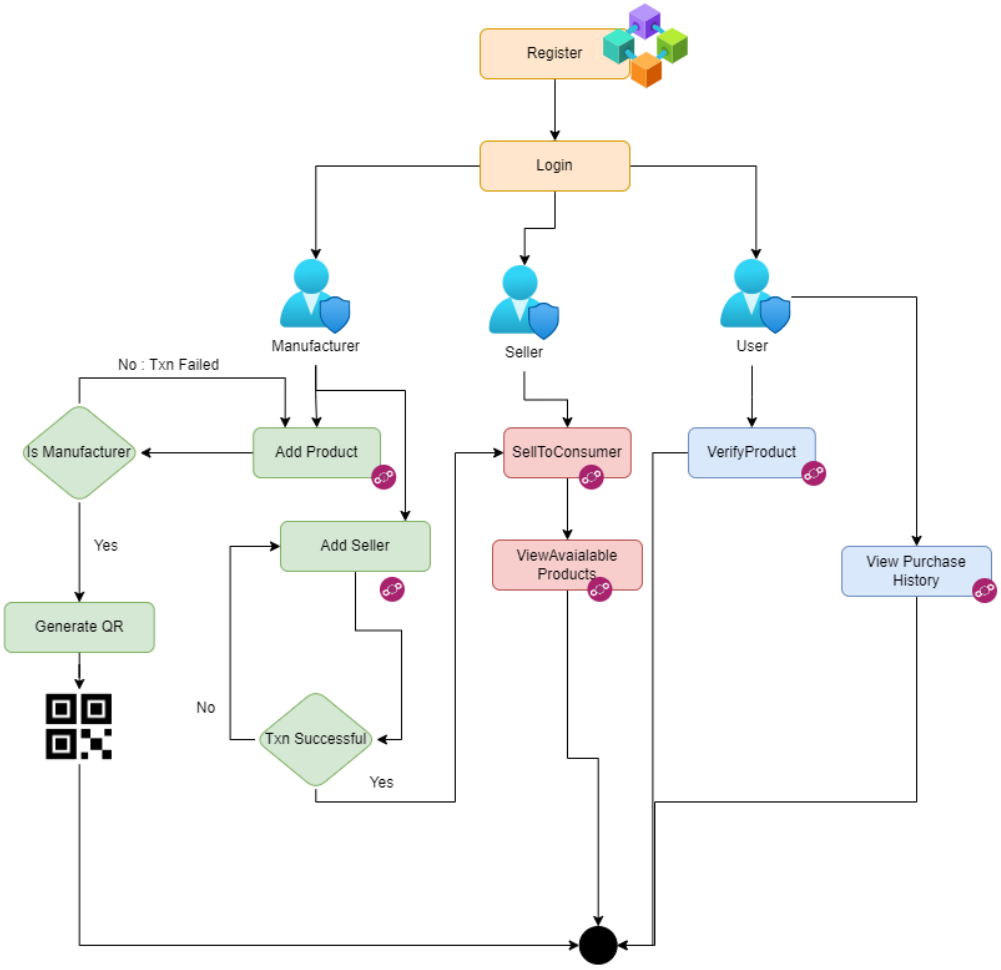

Figure 4.1.3 Process Flow Diagram

4.2 Implementation details and issues

implementation details and issues faced during the development process:

Here is the module wise description of the Project:

1. addProduct(): This function makes use of the security provided by the require function. This leaves a scope of penalty even when the transaction for a user fails. Thus if a user from unauthenticated account tries to add the product, the transaction would be considered as failed. Even if the registered user tries to add a product that has already been registered, transaction would again fail leading to recurring gas fees.
2. sellerSellProduct(): This function first checks whether or not the seller exists in the ecosystem. Then it checks if the seller who has been associated with the product is the one who is selling the product.

   require(sellerFound == true, "Seller does not exist in the ecosystem");

   require(sellers[b].sellerAddress == msg.sender, "Wrong Account Selected");

   Then further required mappings are done so as to associate a product with the consumer.

3. verifyProduct(): This function checks whether the product whose Serial no is scanned is sold to the same consumer verifying the product or not. require(strcmp(productsSold[_productSN], _consumerCode), "Counterfeit Alert!! : Invalid Serial Number Or Consumer Code"); Then based on the output of the above decision is made about whether or not the product is authentic.
4. returnProduct(): This function is invoked by the customer incase he doesn't likes the product and wishes to return the product back to the seller. This erases the existing mapping in the process and thus the product can be resold to the users.
5. consumerSellProduct(): The consumer can sell the second hand products to other consumers depending on the resellability of the product.
6. Apart from this other getter and setter functions are made so as to facilitate only the limited access to the crucial entities like seller or manufacturer or the product itself.

7. Another dependency is on web3 that is used for the interaction between the frontend and the solidity contract. In solidity direct comparison is not possible so the data is sent in form of bytes and received in form of bytes and decoded using web3.toAscii() or web3,FromAscii() to ease the comparison and hashing.
8. Another dependency is on the qr-library function that is used to generate and scan qr to simplify the process of product scanning and registration.

Issues faced:

The following are some of the significant issues faced:

Complexity of Blockchain Technology: The use of blockchain technology in the project introduced complexities that were not present in traditional software development projects. The team had to learn new technologies, such as Solidity and smart contracts, which required extensive research and learning.

Integration with Existing Systems: The project required the integration of the system with existing product authentication and counterfeit detection systems. This integration proved to be a challenging task as the team had to ensure that the system was compatible with different systems, which may have different requirements and specifications.

Limited Resources: The team faced a significant challenge of limited resources, including time and financial resources. The development process required extensive research, development, and testing, which required significant time and financial resources.

Security: The project involved the storage of sensitive information on the blockchain, which required careful consideration and implementation of security measures to prevent unauthorized access and tampering.

Screenshots:

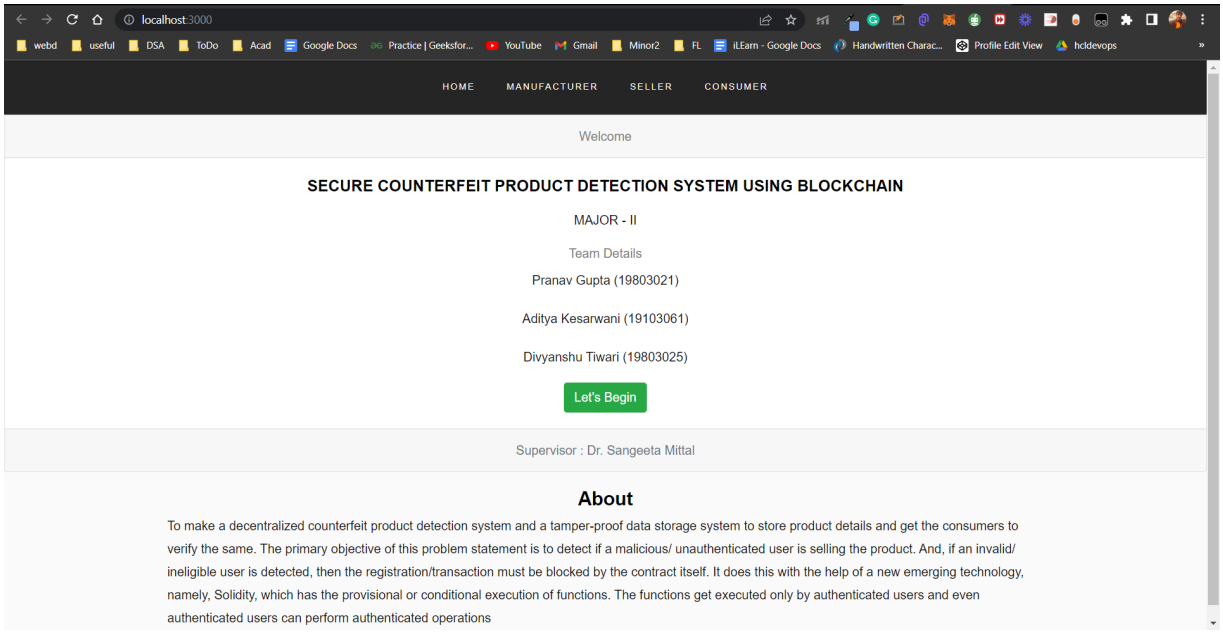

Fig 4.2.1 Landing Page

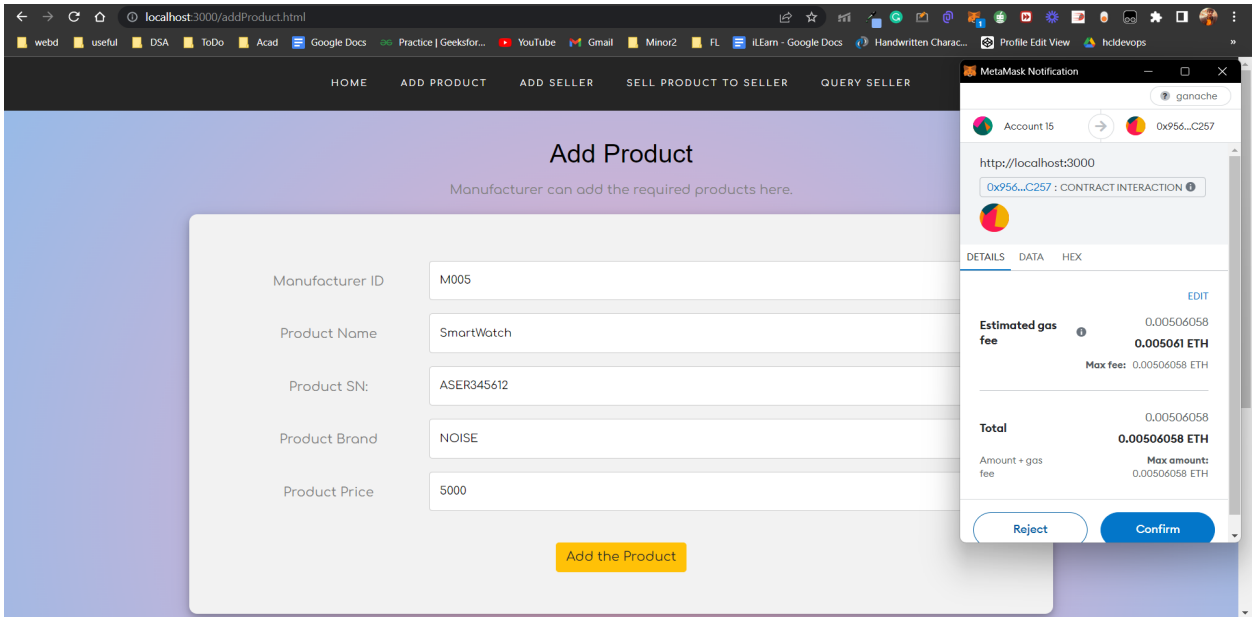

Fig 4.2.2 Manufacturer Dashboard: Add Product

This panel is for adding products by manufacturer on blockchain network after completing txn.

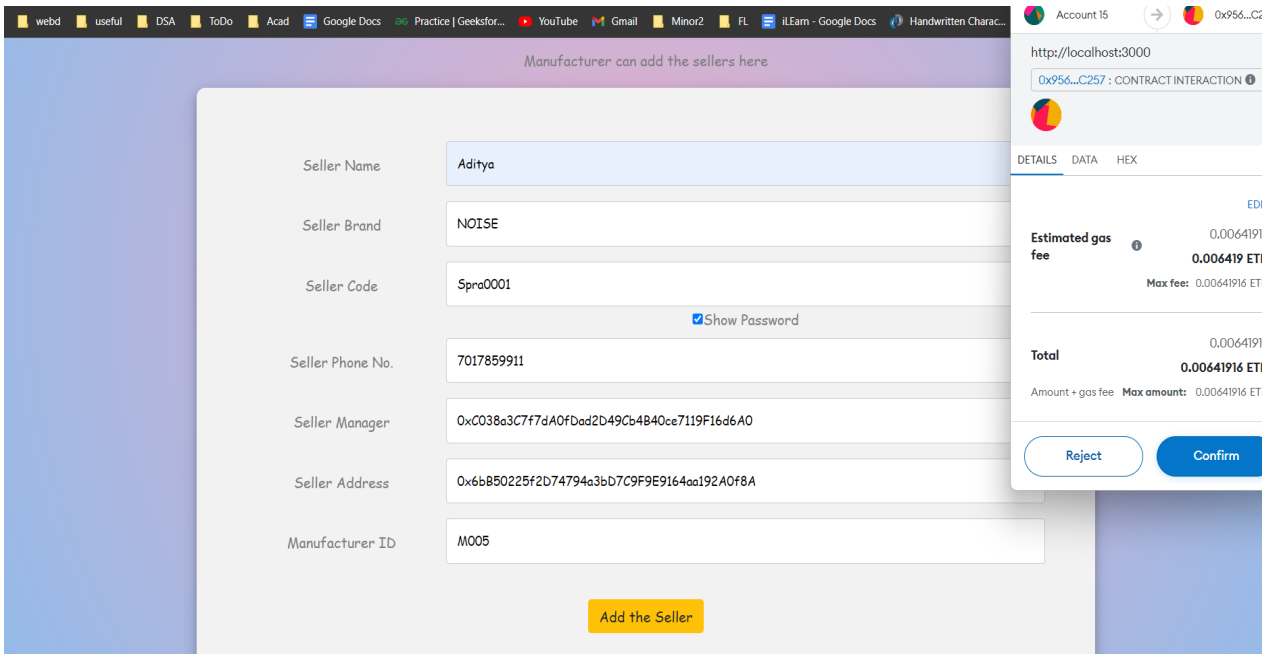

Fig 4.2.3 Manufacturer Dashboard: Add Seller

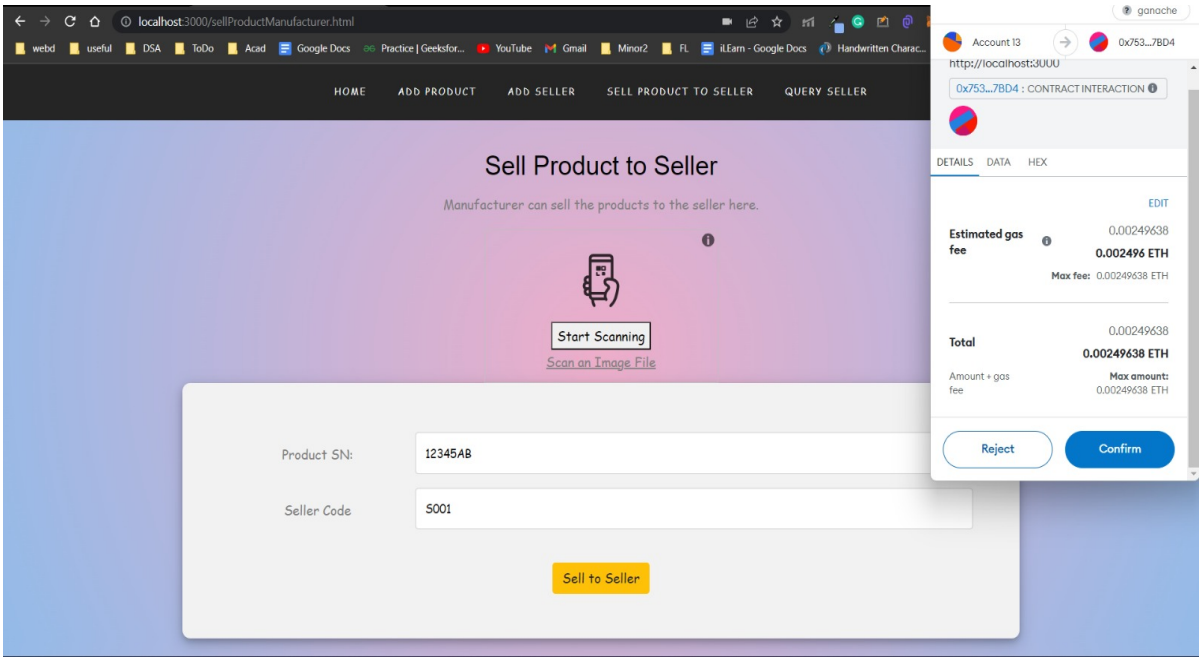

Fig4.2.4 Manufacturer Dashboard: Sell Product To Seller

The above panels are for adding the sellers and sell products to seller after scanning the qr code.

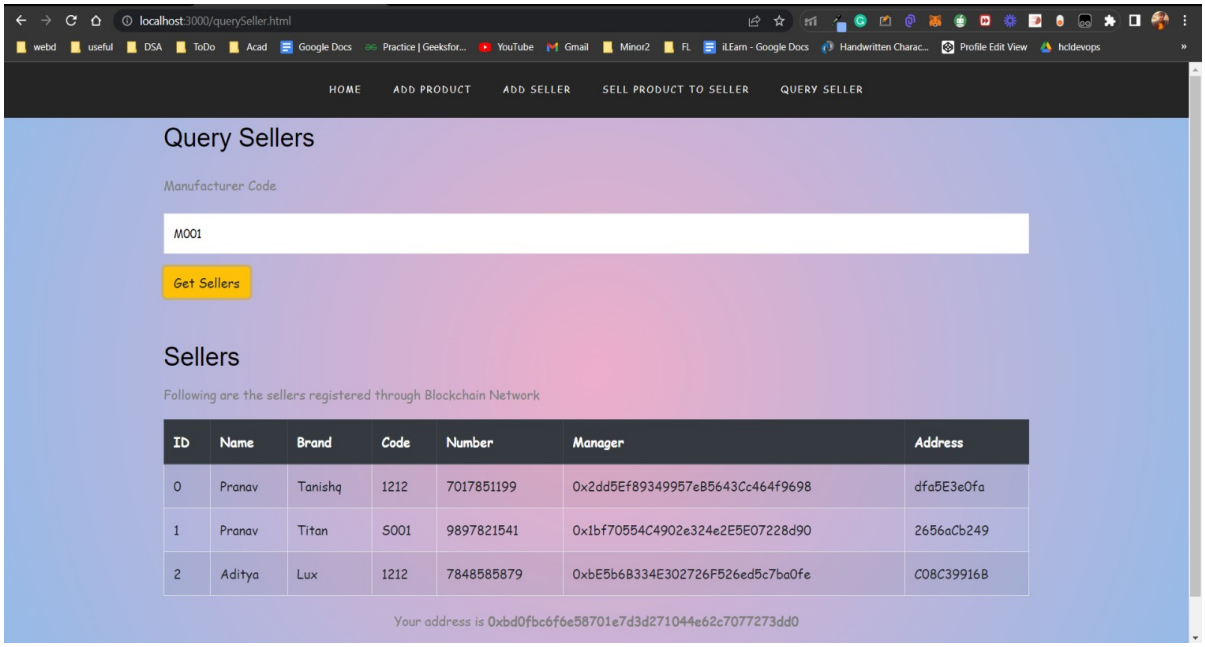

Fig 4.2.5 Manufacturer Dashboard: Query Sellers

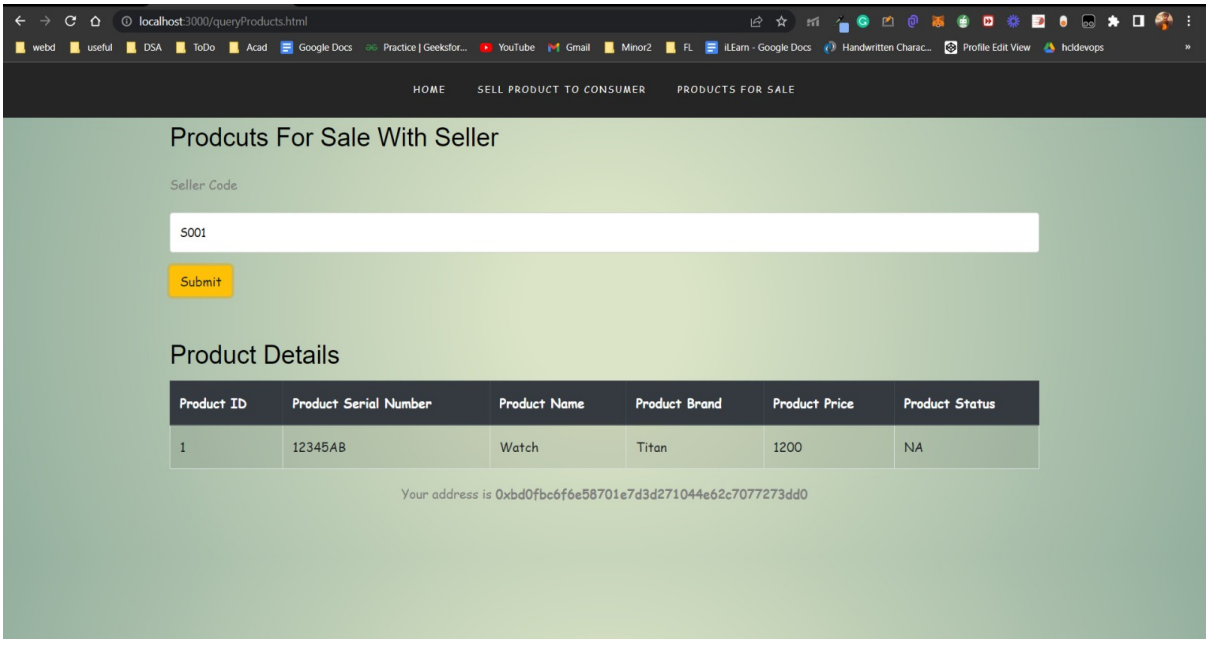

Fig 4.2.6 Seller Dashboard: Products For Sale

The above panels are for querying available sellers and fetch products on sale.

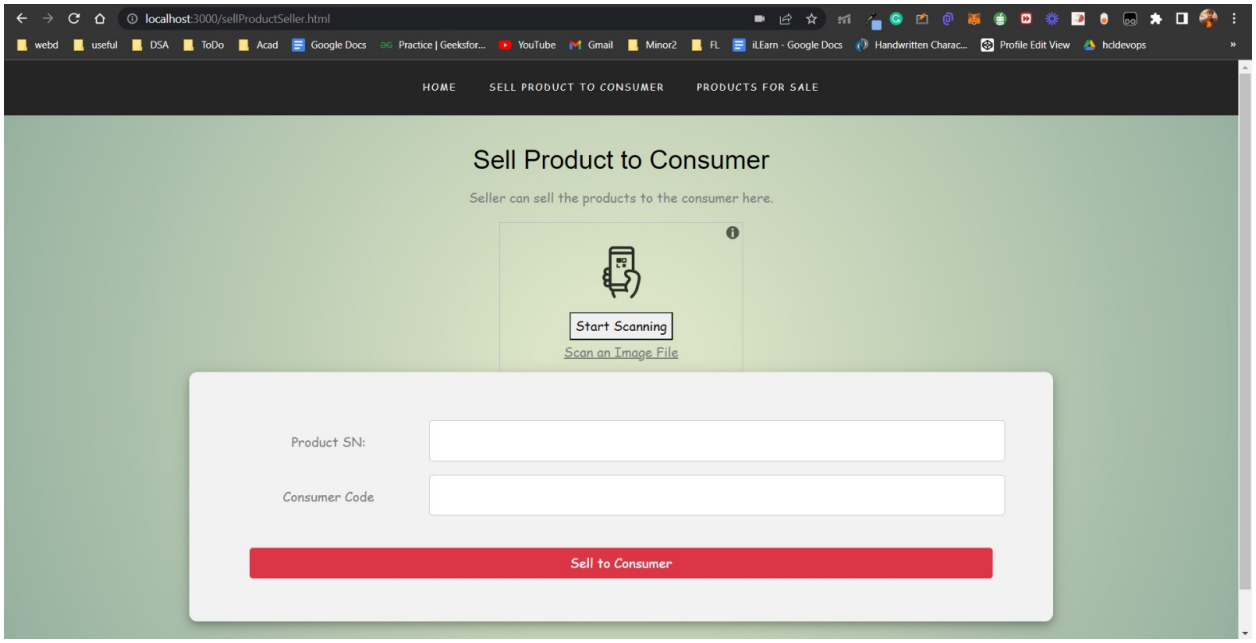

Fig 4.2.7 Seller Dashboard: Sell Product To Consumer

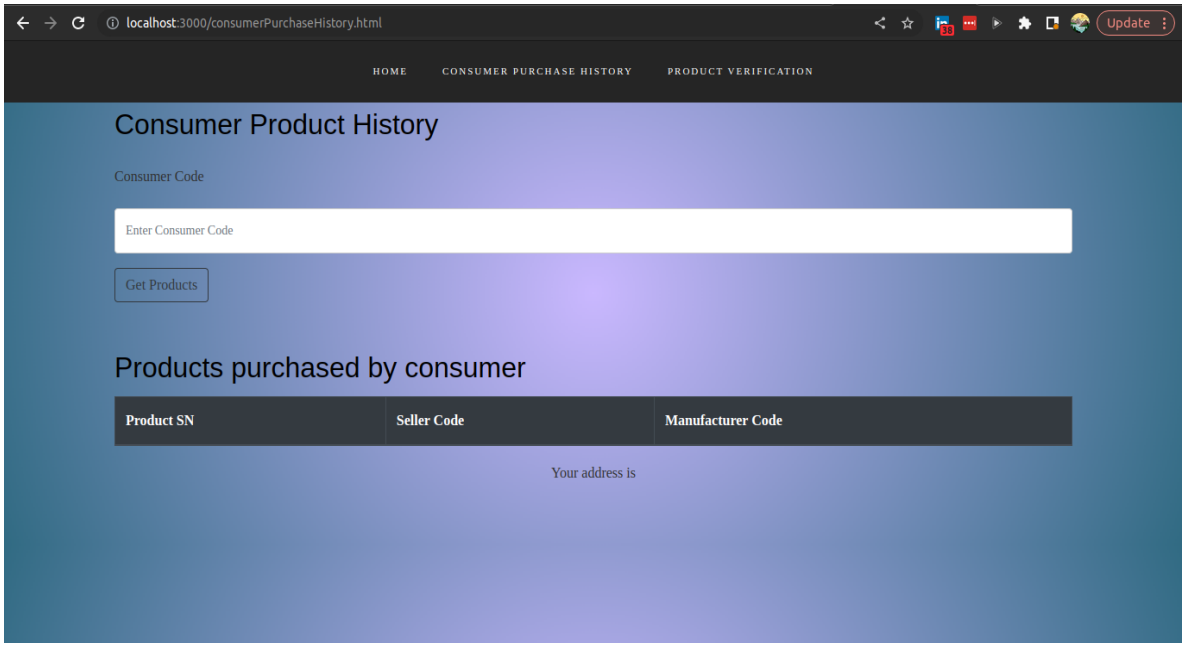

Fig 4.2.8 Consumer Dashboard: Consumer Product History

The above panels are for selling product to consumer by seller and view the purchase history .

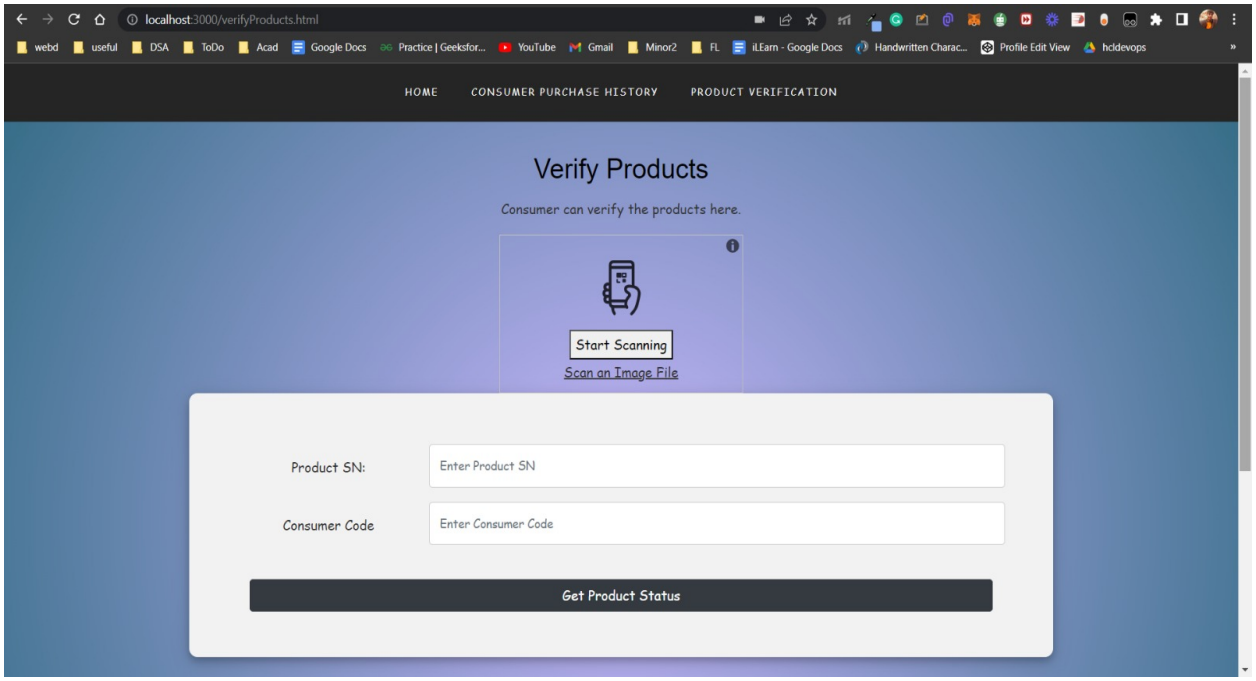

Fig 4.2.9 Consumer Dashboard: Verify Products

The above panel is the concluding among the all it verifies the transactions made at various levels that is manufacturer and seller and then verifies if the product is fake or not. If the product is a genuine one the respective message is displayed on the portal.

This concludes the overall working of the project and thus we can say that we can prevent the counterfeiting of goods to a better extent due to the security protocols laid by the blockchain protocols and the overhead security provided by the keyword require embedded in various functionalities while designing the contract. Along with the basic checks input validation is also used so as to prevent user being a threat to vulnerable attacks such as brute force guessing. This prevents the user from falling prey to the social engineering evils and setting a simpler code for themselves, especially for sellers who are frequently unaware of the technical aspects of security and brute force password guessing and end up keeping simple and easily guessable passwords.

4.3 Risk Analysis and Mitigation

Table 4.3.1: Risk Analysis

Risk_ID	Classification	Description of Risk	Risk Area	Impact
Risk_1	Design	Due to regular read and write operation on disk which takes time as data is written from primary to secondary memory. The performance depends on the disk seek time of the HDD or SSD used.	Performance	Moderate (M)
Risk_2	Engineering Specialties	Since each write and calculation is done separately, this means in case of any error or crash, the affected files might be written partially and no rollback will be available.	Reliability	Low (L)

Risk_3	Requirements	Solidity has minimum run time requirements, however the libraries are required which can be installed very easily on any system.	Completeness	Low (L)

5. Testing

5.1 Testing Plan

The project mainly boils down to three functionalities which are anti-disassembly, anti-debugging and anti-tampering, their functionalities are described above, the testing plan is to test each individual component and make the application more robust and failproof.

Table 5.1.1 Types of Testing

Type of Test	Test Performed	Comments/Explanations	Software Component
Requirements Testing	Yes	Solidity version must be greater than or equal to 0.5.1 Windows 10 OS, 4 GB RAM, 10 GB free space	Solidity Contract Node.js

Unit	Yes	All the individual webpages are working correctly.	addProduct.html addSeller.html consumerPurchaseHistory.html queryProducts.html querySeller.html sellProductManufacturer.html sellProductSeller.html verifyProducts.html
Integration	Yes	The solidity contract compiled and worked successfully. The contract was successfully deployed on Ganache and Metamask (connected to Ganache).	Metamask, Ganache
Performance	Yes	Tested on computer using various network speeds and on local environment	LT Browser
Compliance	Yes	Only the authorized person(Manufacturer) can access the respective job records	Manufacturer.html
Security	Yes	tracked the requests and responses sent via the tool to see the possible vulnerabilities.	BurpSuite

```
divyanshu@divyanshu-Ideapad:~/Desktop/major-2/Major-II$ truffle migrate

Compiling your contracts...
===========================
> Everything is up to date, there is nothing to compile.


Starting migrations...
======================
> Network name:    'development'
> Network id:      5777
> Block gas limit: 6721975 (0x6691b7)


1_initial_migration.js
======================

   Replacing 'Migrations'
   ----------------------
   > transaction hash:    0x1aee23b3066e6f35fa2bf6bce39478ca16eb80c6c42bd1b16a6ec812e8127148
   > Blocks: 0            Seconds: 0
   > contract address:    0xEfd4Ce56Db1D3d6C2eE8bAbcEE40732AFd1c79d5
   > block number:        21
   > block timestamp:     1682434888
   > account:             0xFdF8d1609aa94143bF7d4f7053A1cfD324B7b7B0
   > balance:             99.99502316
   > gas used:            248842 (0x3cc0a)
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.00497684 ETH

   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
```

```
   > Saving artifacts
   -------------------------------------
   > Total cost:          0.00497684 ETH


2_deploy_contract.js
====================

   Replacing 'product'
   -------------------
   > transaction hash:    0x82199d500f52e1fc15e894803504cef1ad32275c5ee8d7431db8a0df17a59e38
   > Blocks: 0            Seconds: 0
   > contract address:    0x62ea9f2CbBd1D13c8b63e01b8b18646a5CeEa395
   > block number:        23
   > block timestamp:     1682434890
   > account:             0xFdF8d1609aa94143bF7d4f7053A1cfD324B7b7B0
   > balance:             99.95413056
   > gas used:            2002117 (0x1e8cc5)
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.04004234 ETH

   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:          0.04004234 ETH

Summary
=======
> Total deployments:   2
> Final cost:          0.04501918 ETH
```

Figure 5.1.1 Contract Compiled Successfully

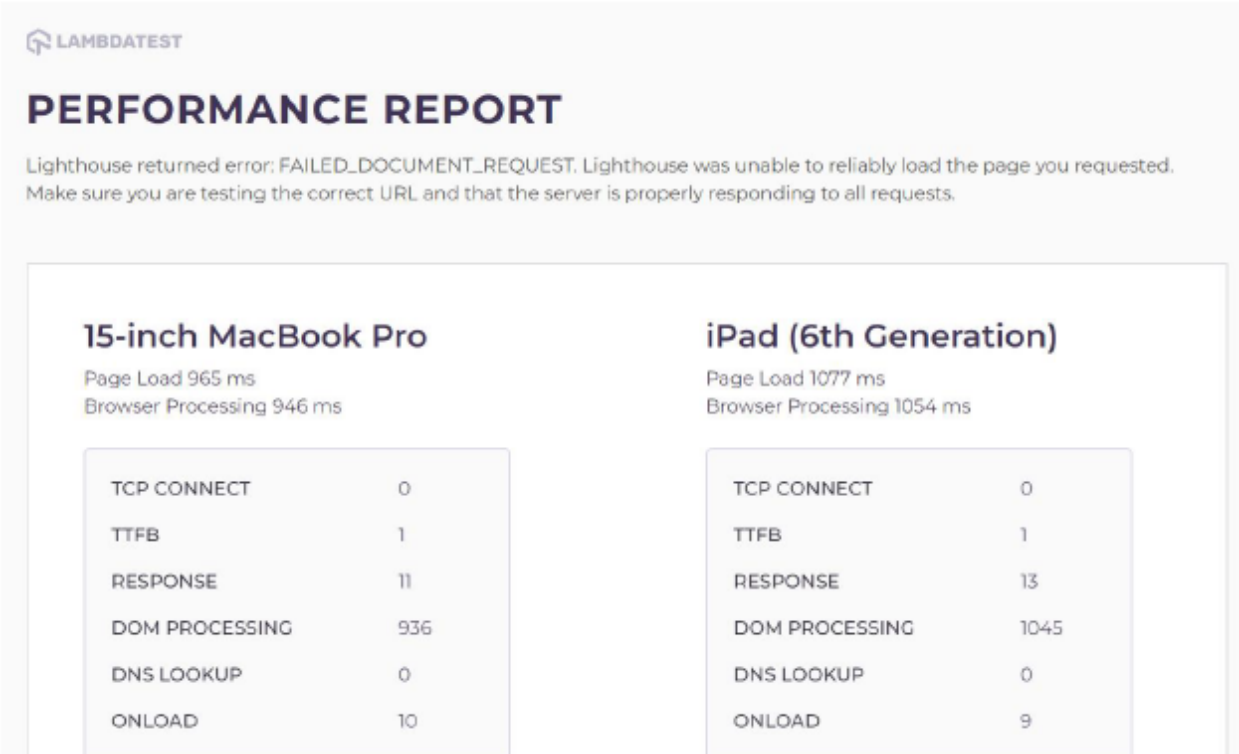

Figure 5.1.2 Testing on Lambda Test

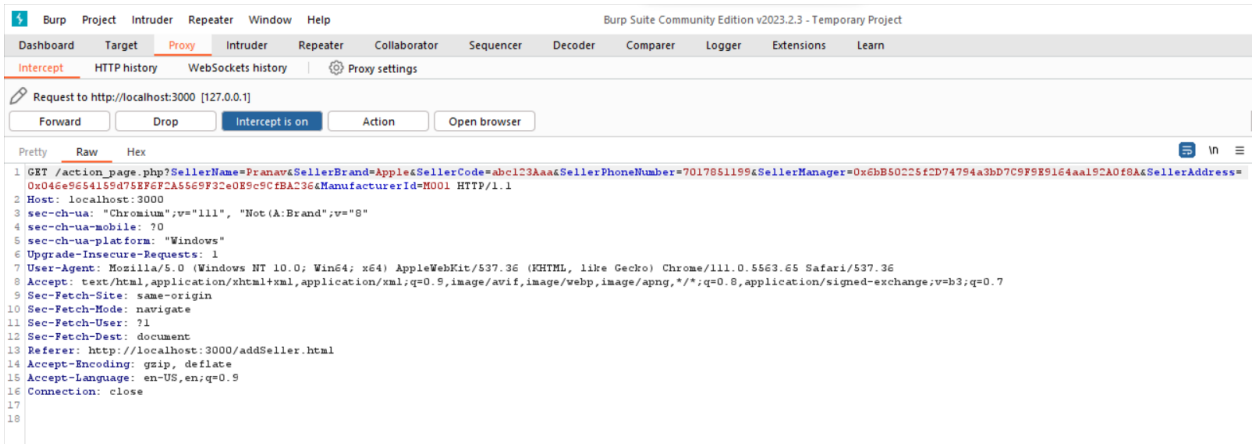

Figure 5.1.3 Request forwarding using BurpSuite Community Edition

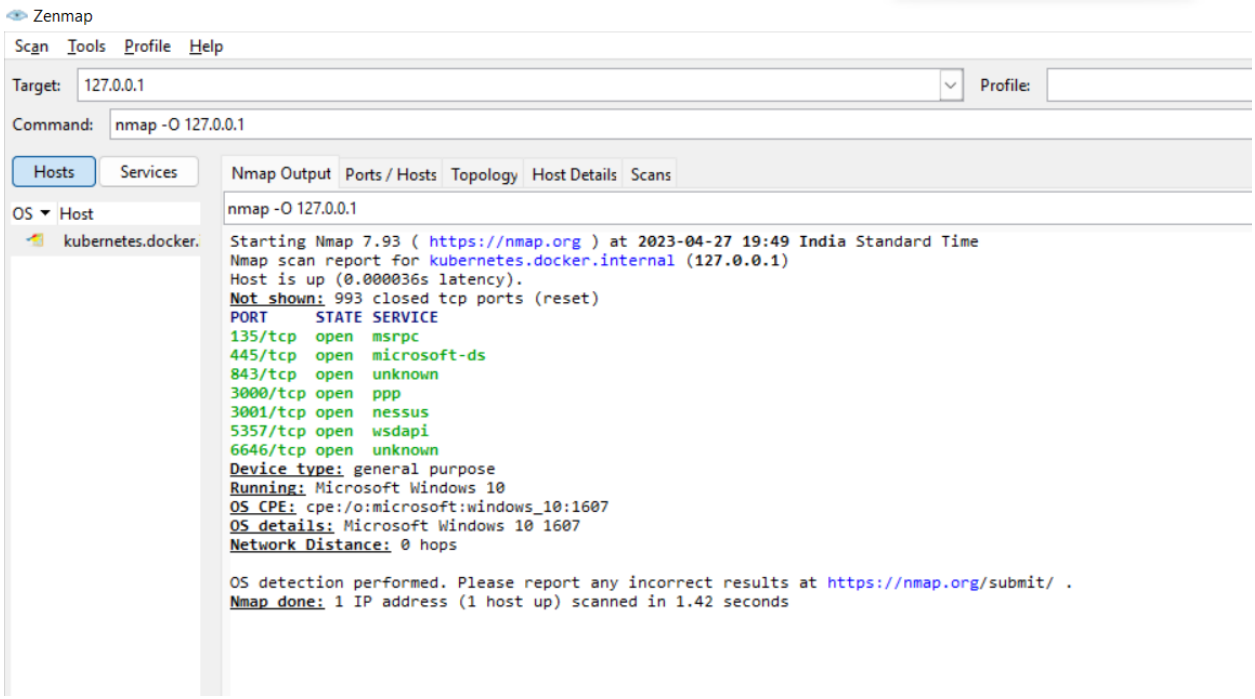

Figure 5.1.4 OS Detection using nmap tool

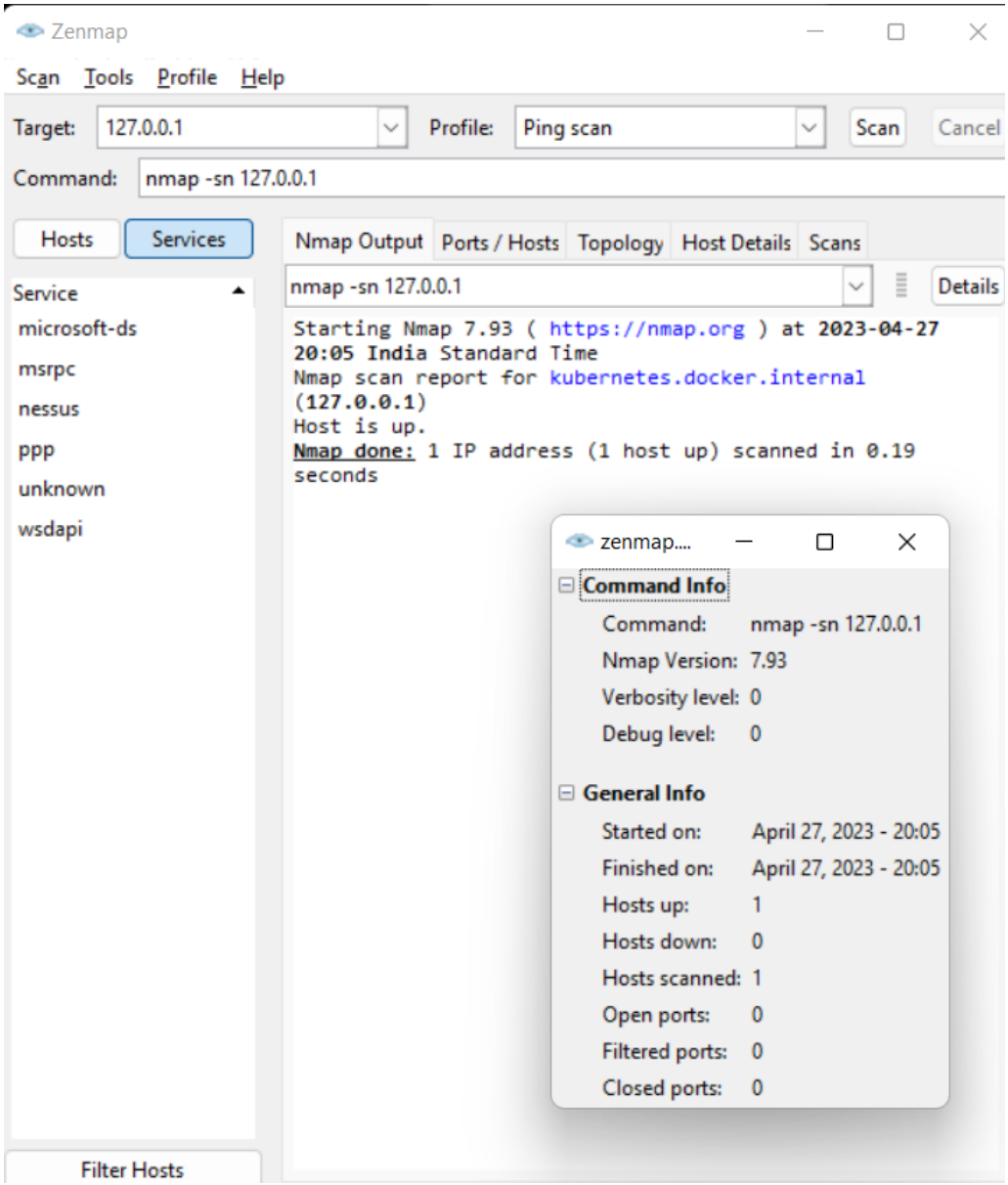

Figure 5.1.5 Ping Scanning using nmap tool

5.2 Component Decomposition and Type of Testing Required

Table 5.2.1: Component Decomposition and Identification of Tests required

S.No	List of Various Components (modules) that require testing	Type of Testing Required*	Technique for writing test cases**
1	addProduct.html	Unit Testing	Negative testing, Error guessing, Boundary value analysis
2	addSeller.html	Unit Testing	Negative testing, Error guessing
3	consumerPurchaseHistory.html	Unit Testing	Negative testing, Error guessing
4	queryProducts.html	Unit Testing	Negative testing, Error guessing
5	querySeller.html	Unit Testing	Negative testing, Error guessing
6	sellProductManufacturer.html	Unit Testing	Negative testing, Error guessing
7	sellProductSeller.html	Unit Testing	Negative testing, Error guessing
8	verifyProducts.html	Unit Testing	Negative testing, Error guessing

Table 5.2.2 Test cases for component addProduct.html(price)

Test Case id	Input	Expected Output	Status
1.	2000	Pass	Pass
2.	1000	Pass	Pass
3.	0	Invalid price	Pass
4.	-200	Invalid price	Pass

Table 5.2.3 Test cases for component addSeller.html(Seller Code)

Test Case id	Input	Expected Output	Status
1.	aAbB25Nn	Pass	Pass
2.	aabb25nn	Include Uppercase letter as well	Pass
3.	AABB25NN	Include Lowercase letter as well	Pass
4.	aAbBNnKk	Include a Number as well	Pass
5.	aAbB25N	Include minimum 8 characters	Pass

Table 5.2.3 Test cases for component addSeller.html(Seller Phone No.)

Test Case id	Input	Expected Output	Status
1.	9891710335	Pass	Pass
2.	9891710	Enter at least 10 digits	Pass

3.	abc9821323	Not a number	Fail

Table 5.2.4 Test cases for component sellProductManufacturer.html(image)

Test Case id	Input	Expected Output	Status
1.	P001.png	Pass	Pass
2.	P002.png	Invalid QRcode	Fail
3.	P003.jpg	Fail	Fail

Table 5.2.5 Test cases for component querySeller.html(Manufacturer Code)

Test Case id	Input	Expected Output	Status
1.	M001	Registered sellers' detail	Pass
2.	M002	No seller registered	Pass
3.	<null>	Fail	Fail

Table 5.2.6 Test cases for component sellProductSeller.html(image)

Test Case id	Input	Expected Output	Status
1.	P001.png	Pass	Pass
2.	P002.png	Invalid QRcode	Fail
3.	P003.jpg	Fail	Fail

Table 5.2.7 Test cases for component queryProducts.html(Seller Code)

Test Case id	Input	Expected Output	Status
1.	S001	Product details	Pass
2.	S002	No product found	Pass
3.	<null>	Fail	Fail

Table 5.2.8 Test cases for component consumerPurchaseHistory.html(Consumer code)

Test Case id	Input	Expected Output	Status
1.	C001	Consumer Purchase history	Pass
2.	C002	No purchases found	Pass
3.	<null>	Fail	Fail

Table 5.2.9 Test cases for component verifyProducts.html(image)

Test Case id	Input	Expected Output	Status
1.	P001.png	Pass	Pass
2.	P002.png	Invalid QRcode	Fail
3.	P003.jpg	Fail	Fail

Table 5.2.10 Test cases for component verifyProducts.html(Product SN)

Test Case id	Input	Expected Output	Status
1.	P001.png	Genuine Product	Pass
2.	P002.png	Fake product	Pass
3.	P003.jpg	Fail	Fail

5.3 Type of Test Explanation Software Component

5.1.1 Unit Testing:

A unit test is a way of testing a unit - the smallest piece of code that can be logically isolated in a system. In most programming languages, that is a function, a subroutine, a method or property.

5.1.2 Integration Testing:

It is defined as a type of testing where software modules are integrated logically and tested as a group. A typical software project consists of multiple software modules, coded by different programmers and software developers, The purpose of this level of testing is to identify bugs in the interaction between these software functionalities when they are put together. Integration testing can be generally coupled with/on top of unit testing and can be bundled with the unit test written by the developer but rather it comes on top of the unit testing and thus easing the developers to filter out the content before going for unit testing.

According to the previous rule as unit testing on each individual component now every permutation of these unit tests will be constructed and then testing will be individually performed on every permutation and tested as a whole new component this will helps in minimizing the

failure risk when the individual components are integrated together and then tested again because when these will be considered as together there will be numerous scenarios generated.

5.1.3 Security testing:

Application security testing (AST) is the process of making applications more resistant to security threats, by identifying security weaknesses and vulnerabilities in source code analysis is important to perform to make sure, that the application does not break any legal securities check or if it doesn't expose any sensitive or confidential information which the project contains on which the project is currently working.AST started as a manual process, But then a lot of automated scripts and tools have been incorporated to increase the throughput, Also it should be automated as there are a large no of open source projects and proprietary software in action and thus Most organizations use a combination of several application security tools.

Static Application Security Testing (SAST)

SAST tools use a white box testing approach, in which testers inspect the inner workings of an application. SAST inspects static source code and reports on security weaknesses.

Static testing tools can be applied to non-compiled code to find issues like syntax errors, math errors, input validation issues, and invalid or insecure references. They can also run on compiled code using binary and byte-code analyzers.

Dynamic Application Security Testing (DAST)

DAST tools take a black-box testing approach. They execute code and inspect it in runtime, detecting issues that may represent security vulnerability. This can include issues with query strings, requests, and responses, the use of scripts, memory leakage, anti-tampering, anti-debug check functionality, cookie and session handling, also other security attacks based on authentication, such as CSRF, XSS, SQL injection execution of third-party components, data injection, and DOM injection.

DAST tools help in conducting large-scale scans which in turn helps a lot of organizations to find bugs in a densely scaled environment.

5.4 Error and Exception Handling:

Debugging technique used

Table 5.2.3 Test cases for component addSeller.html(Seller Phone No.)

Test Case id	Input	Debugging technique
1.	abc9821323	Print debugging

Table 5.4.1 Test cases for component sellProductManufacturer.html(image)

Test Case id	Input	Debugging technique
1.	P002.png	Backtracking
2.	P003.jpg	Backtracking

Table 5.4.2 Test cases for component querySeller.html(Manufacturer Code)

Test Case id	Input	Debugging technique
1.	<null>	Backtracking

Table 5.4.3 Test cases for component sellProductSeller.html(image)

Test Case id	Input	Debugging technique
1.	P002.png	Backtracking
2.	P003.jpg	Backtracking

Table 5.4.4 Test cases for component queryProducts.html(Seller Code)

Test Case id	Input	Debugging technique
1.	<null>	Backtracking

Table 5.4.5 Test cases for component consumerPurchaseHistory.html(Consumer code)

Test Case id	Input	Debugging technique
1.	<null>	Backtracking

Table 5.4.6 Test cases for component verifyProducts.html(image)

Test Case id	Input	Debugging technique
1.	P002.png	Backtracking
2.	P003.jpg	Backtracking

Table 5.4.7 Test cases for component verifyProducts.html(Product SN)

Test Case id	Input	Debugging technique
1.	P003.jpg	Backtracking

The overall application code will be wrapped in try-catch blocks to handle traffic in order to prevent a sudden application failure, which could then break the end application and cause

malfunctions in the source code, which could then lead to improper testing of the end-user application.

Chapter 6 (Findings, Conclusion and Future Work)

6.1 Findings

A reliable method for identifying fake goods and guaranteeing their validity is the Decentralised Counterfeit Product Detection and Tamper-Proof Data Storage System. By utilising the tamper-proof properties of the Ethereum blockchain, the solution offers a high level of security. Decentralised storage of product data makes it challenging for unauthorised users to change or manipulate the data.

Authentication: By using private and public keys for user authentication, the system is protected from unauthorised users. This lessens the likelihood of security breaches and unauthorised access.

Transparency: The system gives consumers transparency by enabling them to confirm the legitimacy of the item they are buying. As a result, there is a greater level of trust between consumers and manufacturers, which may boost customer loyalty and sales.

Efficiency: The use of smart contracts, which automate numerous operations and lessen the need for user interaction, makes the system extremely efficient. This makes it easier to identify fake goods and ensure product authenticity while using less time and resources.

Cost-effectiveness: Using a decentralised system eliminates the need for middlemen and can lower the price of authenticating products and finding counterfeits.

Scalability: The system is suited for usage across a variety of industries since it is easily scaled to support a large number of items and users.

6.2 Conclusion

The Decentralised Counterfeit Product Detection and Tamper-Proof Data Storage System, in conclusion, is a reliable method for identifying fake goods and confirming their authenticity. The technology uses the tamper-proof characteristics of the Ethereum blockchain and smart contract technology to offer a safe, decentralised, and effective solution.

The method deals with the crucial problem of counterfeit goods and gives customers the means to confirm the legitimacy of the product they are buying. Consumers and manufacturers can develop a stronger sense of trust as a result, which may boost sales and customer loyalty. Additionally, the system is appropriate for usage in a variety of businesses due to its openness and affordability.

The Decentralised Counterfeit Product Detection and Tamper-Proof Data Storage System is highly effective, scalable, and economical, according to the results of our research and development. These results illustrate the system's potential to address the problem of counterfeit goods and attest to the system's effectiveness.

6.3 Future Work

Despite the success of the Decentralised Counterfeit Product Detection and Tamper-Proof Data Storage System, the following areas still have room for development and future work:

6.3.1 Integration with Existing Systems: To offer a more complete and reliable solution, the system can be integrated with current product authentication and counterfeit detection systems. The effectiveness and efficiency of the system may be improved by this integration.

6.3.2 Mobile Application: To give customers a quick and easy way to confirm the legitimacy of the product they are buying, a mobile application can be created. Additionally, this application may aid in raising consumer interest and awareness.

6.3.3 Expansion to Other Industries: The system's current field of use can be expanded to other industries. This can contribute to addressing the problem of fake goods in other industries and offering a more complete solution.

The system can be linked with supply chain management systems to enable end-to-end visibility of the product's path from production to the point of sale. The effectiveness and transparency of the system may be further improved by this integration.

There is room for growth and development for the Decentralised Counterfeit Product Detection and Tamper-Proof Data Storage System. Future work in these areas may improve the system's effectiveness, adoption, and efficiency while offering a more all-encompassing answer to the problem of fake goods.

REFERENCES

[1] Y. Dabbagh, R. Khoja, L. AlZahrani, G. AlShowaier and N. Nasser, "A Blockchain-Based Fake Product Identification System," 2022 5th Conference on Cloud and Internet of Things (CIoT), Marrakech, Morocco, 2022, pp. 48-52, doi: 10.1109/CIoT53061.2022.9766493.

[2] M. C. Jayaprasanna, V. A. Soundharya, M. Suhana and S. Sujatha, "A Block Chain based Management System for Detecting Counterfeit Product in Supply Chain," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, pp. 253-257, doi: 10.1109/ICICV50876.2021.9388568.

[3] B. S, S. Pramanick, R. Singh and D. Kumar, "An Ethereum based Fake Product Identification System using Smart Contract," 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2022, pp. 292-296, doi: 10.1109/ICICCS53718.2022.9788449.

[4] R. Jadhav, A. Shaikh, M. A. Jawale, A. B. Pawar and P. William, "System for Identifying Fake Product using Blockchain Technology," 2022 7th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2022, pp. 851-854, doi: 10.1109/ICCES54183.2022.9835866.

[5] P. M. Lavanya et al., "Fake Product Detection using Blockchain," 2021 4th International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, 2021, pp. 133-137, doi: 10.1109/ICCCT53315.2021.9711899.

[6] Khan, S.N., Loukil, F., Ghedira-Guegan, C. et al. Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-Peer Netw. Appl. 14, 2901–2925 (2021). https://doi.org/10.1007/s12083-021-01127-0

[7] Divya P.S and Sheeja M.K, "Security with holographic barcodes using Computer generated holograms," 2013 International Conference on Control Communication and Computing (ICCC), Thiruvananthapuram, India, 2013, pp. 162-166, doi: 10.1109/ICCC.2013.6731643.

[8] Qin Wang, Rujia Li, Qi Wang, Shiping Chen, Dragan. “Exploring Web3 From the View of Blockchain (2022)”. 2022 Arxiv, doi: 10.1109/Blockchain55522.2022.00021.