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

December 2022

Submitted in partial fulfillment of the Degree of

Bachelor Of Technology

in

Computer Science Engineering

Department Of Computer Science Engineering & Information Technology

Jaypee Institute of Information Technology

TABLE OF CONTENTS

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

1. INTRODUCTION

1.1 General Introduction

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 organisation, 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 phoney goods. We can utilise 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 decentralised 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

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:

Consumer protection: Fake goods may not adhere to safety regulations or contain potentially harmful substances. Finding these items and taking them off the market can stop harm, disease, or even death.

Quality assurance: As fake products might not be as good as real ones, they might leave customers unhappy and harm a company's reputation. Companies may guarantee that their customers receive the high-quality products they anticipate by identifying and removing bogus products.

Intellectual property protection: Fake goods violate the intellectual property rights of real

companies, costing them money and harming their reputation. Protecting intellectual property rights and avoiding economic loss can both be achieved by spotting and halting the manufacturing and sale of counterfeit goods.

Legal compliance: In the majority of nations, it is forbidden to produce and sell counterfeit goods. Businesses can adhere to pertinent rules and regulations by identifying and halting the sale of counterfeit goods.

Economic effects: Manufacturing and selling counterfeit goods can have a big impact on the economy, costing real companies sales and lowering tax collections for governments. Businesses and governments can contribute to the protection of their financial interests by identifying and halting the sale of counterfeit goods. In general, fraudulent product identification is crucial for consumer protection, assuring product quality, sustaining economic interests, and defending intellectual property rights.

1.4 Empirical Study

Some research experiments need to be analyzed qualitatively, as quantitative methods are not applicable there. In many cases, in-depth information is needed or a researcher may need to observe a target audience's behavior, hence the results needed are in a descriptive form. Qualitative research results will be descriptive rather than predictive. It enables the researcher to build or support theories for future potential quantitative research. In such a situation qualitative research methods are used to derive a conclusion to support the theory or hypothesis being studied. The following field study has been done

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.

Every block contains the hash address of the previous block, with the Genesis block being the first. Each block contains information on transactions, timestamps, the hash address of its own block, and the hash address of the block before it. If the data is changed, the hash of the block is modified as well, however, the following block will have the same unaltered hash as the preceding block, discarding this block and all subsequent blocks. A Merkle tree is used to store the blocks in the networks and the corresponding Merkle root hash is stored in the block. To avoid tampering, it employs the notion of proof of work, which postpones the formation of new blocks and necessitates a large amount of computational power to find the next valid block hash.[7]

Solidity:

Solidity is a smart contract programming language native to Ethereum.It has been a buzzword for quite some time now thanks to its ability to implement smart contracts on blockchains. Solidity programming tackles real-world solutions with a simplistic approach using a language that is similar to C or C++ and JavaScript. Currently, Solidity programming can generate smart contracts for various uses, including blind auctions, voting, crowdfunding, and multi-signature wallets.

Smart Contract:

Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss. They can also automate a workflow, triggering the next action when conditions are met.

Truffle Compile & Test:

Truffle comes standard with an automated testing framework to make testing our contracts a breeze. This framework lets us write simple & manageable tests in different ways.

Migrate to local Blockchain Ganache: Ganache, previously Testrpc, is a virtual blockchain which sets up 10 default Ethereum addresses, complete with private keys and all, and pre-loads

them with 100 simulated Ether each, it immediately confirms any transaction coming its way. This makes iterative development possible - we can write unit tests for our code which execute on this simulated blockchain, deploy smart contracts, play around, call functions, and then tear it all down for further simulation or new tests, returning all addresses to their initial state of 100 Ether.

MetaMask Wallet Connection:

MetaMask is a software cryptocurrency wallet used to interact with the Ethereum blockchain. It allows users to access their Ethereum wallet through a browser extension or mobile app, which can then be used to interact with decentralized applications. MetaMask is developed by ConsenSys Software Inc., a blockchain software company focusing on Ethereum-based tools and infrastructure.

1.5 Brief Description of the solution Approach

Our counterfeit product verification system is designed to combat the growing problem of counterfeit goods in the market. Using blockchain technology, we have created a secure and decentralized platform that allows manufacturers, retailers, and consumers to verify the authenticity of products.

The system works by assigning a unique digital signature to each product at the time of manufacture. This signature is then stored on the blockchain, creating an immutable record of the product's origin and authenticity.

When a consumer purchases a product, they can scan the product's QR code using their smartphone, which will then query the blockchain for the product's signature. If the signature is valid, the consumer can be assured that the product is authentic.

Similarly, retailers can use the system to verify the authenticity of the products they receive from their suppliers. By scanning the products' QR codes, they can confirm that the products are genuine and have not been tampered with.

Overall, our counterfeit product verification system provides a secure and efficient way to combat the problem of counterfeit goods in the market. By leveraging the power of blockchain technology, we can create a transparent and trustworthy supply chain that benefits manufacturers, retailers, and consumers alike.

1. Blockchain-based authentication: The core of your solution is the use of blockchain technology to authenticate products. Each product has a unique digital signature that is recorded on the blockchain. The signature is created by using a combination of unique identifiers, such as a product serial number, batch number, and manufacturing location, and encrypted with a private key. This creates an immutable record of the product's origin and authenticity that can be accessed by anyone with access to the blockchain.
2. Decentralized platform: The blockchain-based platform is decentralized, meaning that there is no central authority controlling the system. This makes the platform more resilient to attacks and tampering. Additionally, it allows all parties involved in the supply chain, such as manufacturers, retailers, and consumers, to access the blockchain and verify the authenticity of a product.
3. QR code scanning: To make it easy for consumers and retailers to access the blockchain and verify product authenticity, each product has a unique QR code printed on its packaging. Consumers and retailers can scan the code using their smartphone's camera, which will then query the blockchain for the product's signature. If the signature matches the product's unique identifiers, the product is considered authentic.
4. Transparency and traceability: One of the main advantages of your solution is the transparency and traceability it provides throughout the supply chain. Each transaction on the blockchain is recorded and can be accessed by all parties involved. This provides a complete audit trail of the product's journey from manufacturing to sale. Additionally, any attempts to tamper with the product's signature or alter the product's information will be immediately detected by the blockchain.

5. Enhanced security: Your solution provides enhanced security to combat the problem of counterfeit goods. By creating an immutable record of a product's authenticity, it becomes much harder for counterfeiters to replicate the product and pass it off as genuine. Additionally, the decentralized nature of the platform and the use of encryption and private keys make it much harder for hackers to tamper with the blockchain.

1.6 Comparision of existing approaches to the problem framed

When comparing existing approaches to the problem of counterfeit product detection, there are several options available. One approach is to use traditional authentication methods such as serial numbers, holograms, and other physical security measures to ensure the authenticity of the product. However, these methods are often not foolproof and can be easily replicated by counterfeiters.

Another approach is to use blockchain technology to create a tamper-proof record of the product's history. By storing information about the product on the blockchain, it is possible to ensure that the product is authentic and has not been tampered with. However, this approach requires a significant amount of infrastructure and can be complex to implement.

A third approach is to use machine learning and artificial intelligence to analyze data and detect patterns that may indicate counterfeit products. This approach can be highly effective but requires a large amount of data and may be vulnerable to false positives.

In comparison to these existing approaches, the decentralized counterfeit product detection system proposed in this project using Solidity has several advantages. It combines the tamper-proof record-keeping of blockchain technology with the conditional execution of functions in Solidity, ensuring that only authenticated users can perform authorized operations on the system. Additionally, the system allows for consumers to easily verify the authenticity of the

product they are purchasing. Overall, this approach offers a more secure and decentralized solution to the problem of counterfeit product detection.

2. Literature Survey

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	A Blockchain based Management System for Detecting Counterfeit Product in Supply Chain
Author	Jayaprasanna, M.C. and Soundharya, V.A. and Suhana, M. and Sujatha, S.
Publisher	2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)
Year	2021
Summary	This research paper proposes a blockchain-based solution to combat the problem of counterfeit products in the supply chain. Counterfeit products have become a significant problem that affects consumers, businesses, and the economy as a whole. Current methods of detecting counterfeit products are often inadequate, as they rely on physical labels or serial numbers that can be easily replicated. The proposed system consists of three main components: a product registry, a blockchain network, and a mobile application for end-users.

	The paper describes the implementation of the proposed system using the Ethereum 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 2.1.3: 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	System for Identifying Fake Product using Blockchain Technology
Author	Jadhav, Roshan and Shaikh, Altaf and Jawale, M. A. and Pawar, A.B. and William, P.
Publisher	2022 7th International Conference on Communication and Electronics Systems (ICCES)
Year	2022
Summary	This research paper proposes a blockchain-based solution for identifying and preventing fake products in the supply chain. The paper highlights the problem of counterfeit products, which poses a significant threat to consumers, businesses, and the economy as a whole.

	The application allows consumers to scan a product's QR code and verify its authenticity by accessing the product's information stored on the blockchain network. The paper discusses the implementation of the proposed system and its security analysis. The system provides several benefits, such as transparency, real-time product tracking, and tamper-proof data storage. The use of blockchain technology ensures that the system operates autonomously, without any intervention from intermediaries.

Table 2.1.5: Paper 5

Paper Title	Fake Product Detection using Blockchain
Author	Lavanya, P.M. and Ananthi, N. and Kumaran, K. and Abinaya, M. and Kalaivani, B. and Krithika, V. and Rahul, S. Shanjai
Publisher	2021 4th International Conference on Computing and Communications Technologies (ICCCT)
Year	2021

Summary	The authors argue that counterfeit products are a significant problem that affects businesses, consumers, and governments, and current detection methods are not efficient enough to tackle the issue. The proposed solution uses a blockchain-based system that stores information about the product's authenticity and tracks the product's entire supply chain. The system maintains a decentralized ledger that stores the product's information, including the manufacturer, distributor, and retailer information. The blockchain network can also verify the physical characteristics of the product, such as its serial number, barcode, and packaging. The authors implemented a prototype of their proposed solution and evaluated it using a case study involving the detection of counterfeit smartphones. The results of the study demonstrate that the proposed solution can accurately and efficiently detect fake products.

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	Complexity Analysis of Decentralized Application Development Using Integration Tools
Author	-Patrik Rek, Blaz Podgorelec, And Muhamed Turkanovi C
Publisher	CEUR Workshop Proceedings
Year	2019

Summary	Decentralized applications developers must be acquainted with the Solidity programming language, with which smart contracts on the Ethereum platform are developed. Smart contracts also represent the fundamental building blocks of decentralized applications. If we look from the traditional web application development perspective, smart contracts can be considered as a back-end logic of decentralized applications. Therefore, it is also necessary to know how to connect the aforementioned smart contracts within a blockchain network (eg. permissioned or permissionless) with the end user in a user-friendly way, i.e. with decentralized applications.

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

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

3.3.1 Smart Contract Development:

The system will be developed using Solidity, a programming language for writing smart contracts on the Ethereum blockchain. Several smart contracts will be developed to perform specific functions such as user authentication, product data storage, product verification, and invalid user detection.

3.3.2 Authentication:

To ensure that only authenticated users can access the system, users will be required to provide a private key that matches their public key. The smart contract will verify that the key is valid before allowing the user to access the system.

3.3.3 Product Data Storage:

Product data such as the product's unique identification number, manufacturing date, expiry date, and other relevant information will be stored in a tamper-proof manner on the Ethereum blockchain. This will ensure that the data is secure and cannot be altered by unauthorized users.

3.3.4 Product Verification:

To allow consumers to verify the authenticity of the product they are purchasing, a QR code will be generated for each product. Consumers can scan the QR code or enter the product's unique identification number to verify the product's authenticity.

3.3.5 Invalid User Detection:

To prevent invalid/ ineligible users from accessing the system, the smart contract will check the user's credentials before allowing them to perform any authorized operations on the system. If the user's credentials are invalid, the transaction will be blocked by the contract itself.

4. Modelling and Implementation Details

4.1 Design Diagrams

4.1.1 Use Case Diagram :

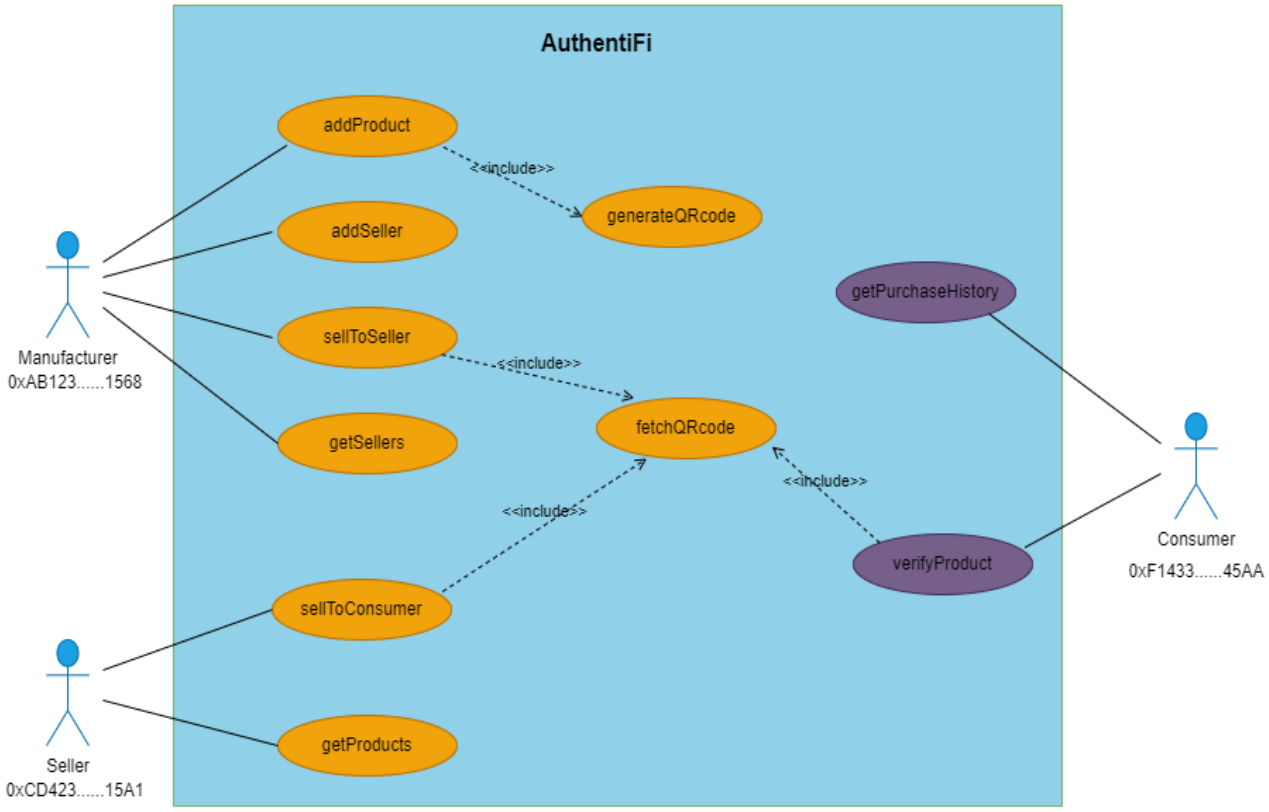

Figure 4.1.1 Use Case Diagram

4.1.2 Sequence Diagram

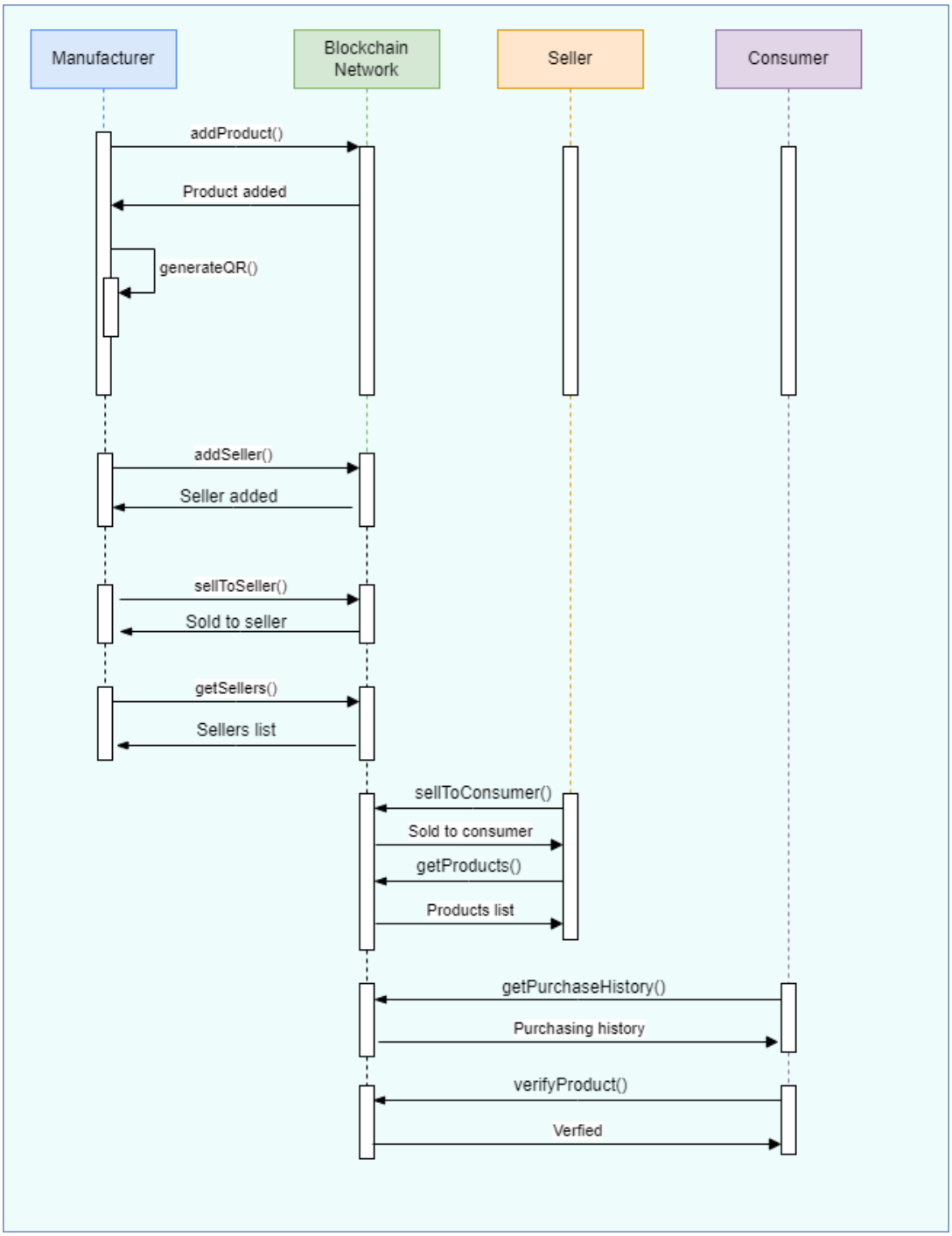

Figure 4.1.2 Sequence Diagram

4.1.3 Process Diagram

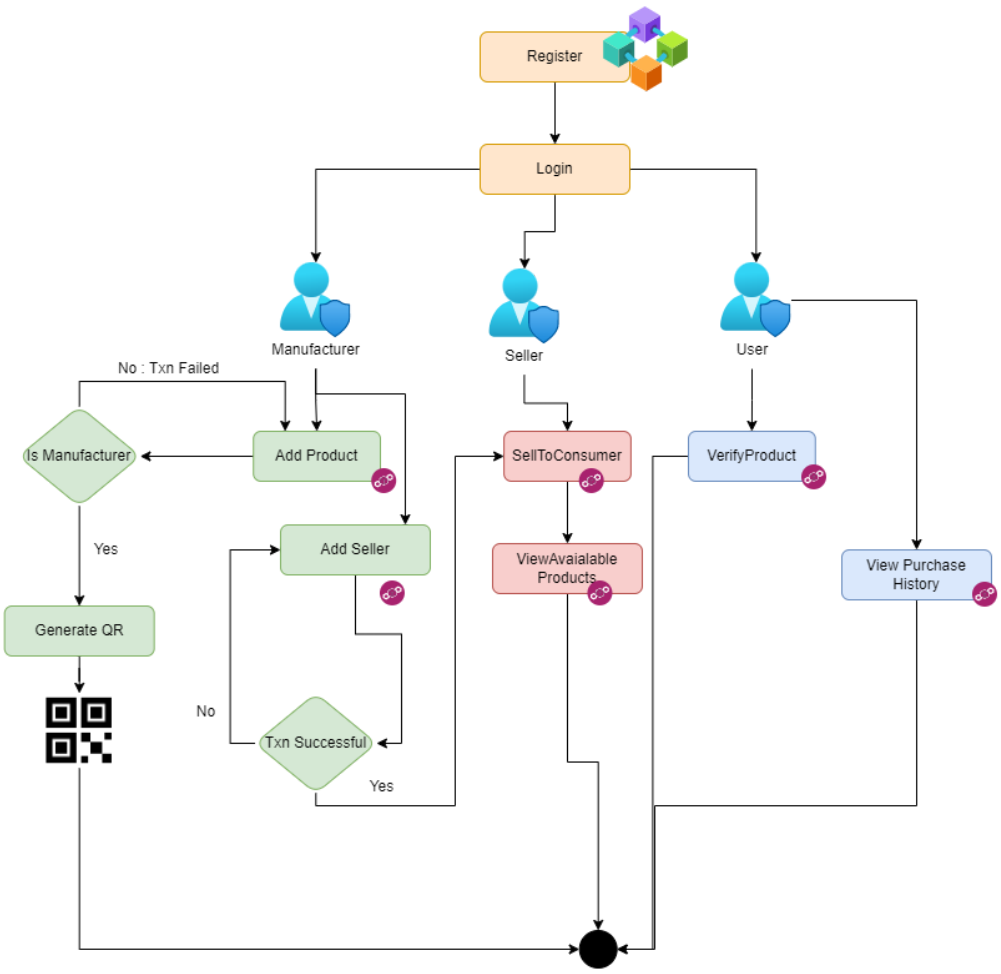

Figure 4.1.3 Process Flow Diagram

4.2 Implementation details and issues

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 implementation details and issues faced during the development process:

Smart Contract Development:

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.

User Authentication:

Product Verification:

Product verification was implemented by registering product details on the blockchain, such as the manufacturer, product name, and serial number. Consumers could verify the product's authenticity by checking the product details against the blockchain record.

User Interface:

The system's user interface was developed using web technologies, such as HTML, CSS, and JavaScript. The user interface provided a user-friendly way for users to access the system and verify product authenticity.

Scalability:

One of the significant issues faced during the implementation was scalability. The Ethereum blockchain's current limitations make it challenging to handle large volumes of transactions, leading to network congestion and increased transaction fees.

Security:

The system's security was a critical consideration during the implementation. Smart contracts were thoroughly tested to ensure there were no vulnerabilities or loopholes that could be exploited by malicious actors.

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.

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

Figure 5.1.1 Contract Compiled Successfully

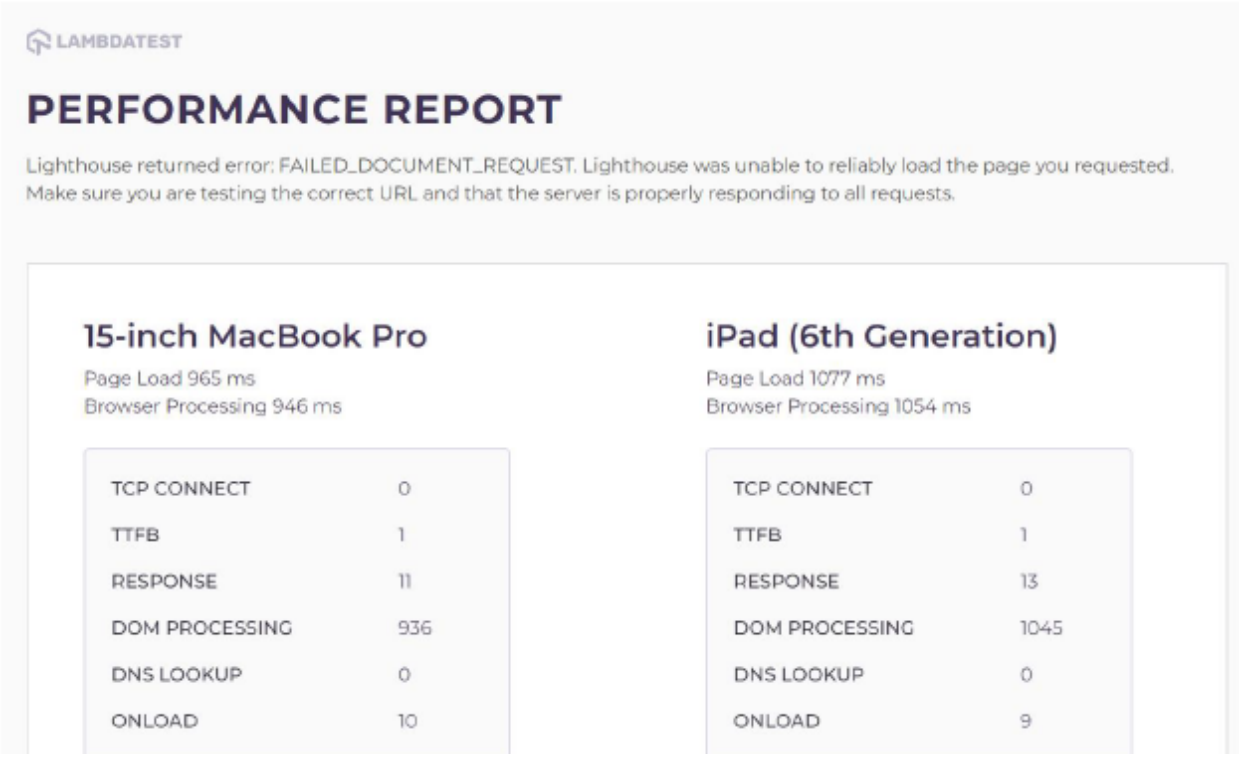

Figure 5.1.2 Testing on Lambda Test

vercel.app

Updated 3 days ago

Domain Information

Domain:	vercel.app
Registrar:	Tucows Domains Inc
Registered On:	2020-01-28
Expires On:	2023-01-28
Updated On:	2022-02-14
Status:	ok
Name Servers:	a.zeit-world.co.uk b.zeit-world.org e.zeit-world.com f.zeit-world.net

Figure 5.1.3 Domain Test on whois.com

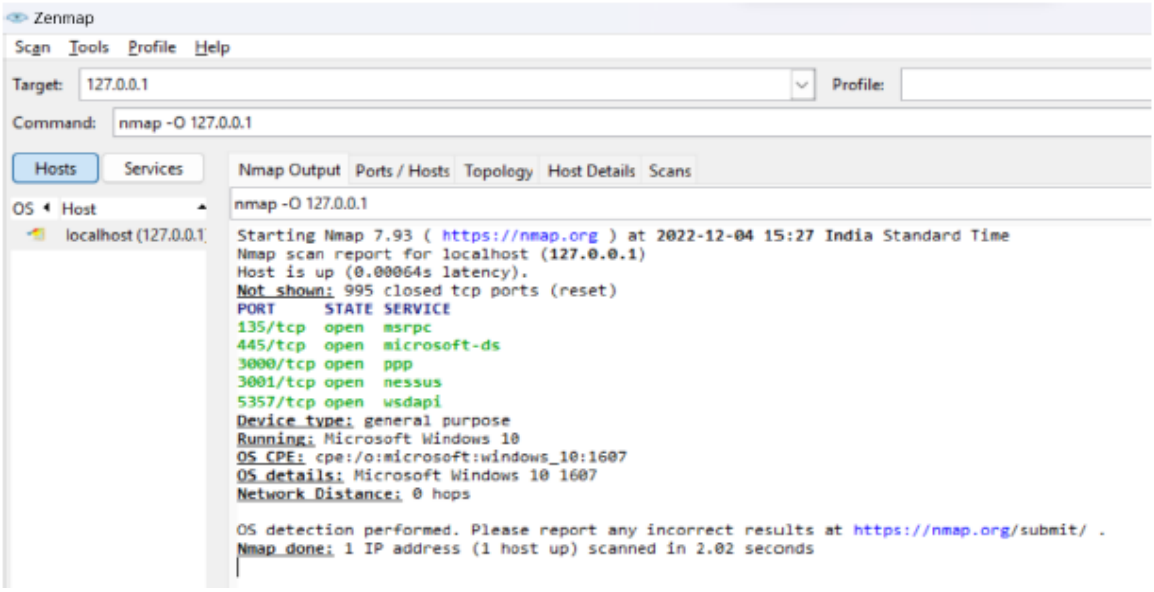

Figure 5.1.4 OS Detection using nmap tool

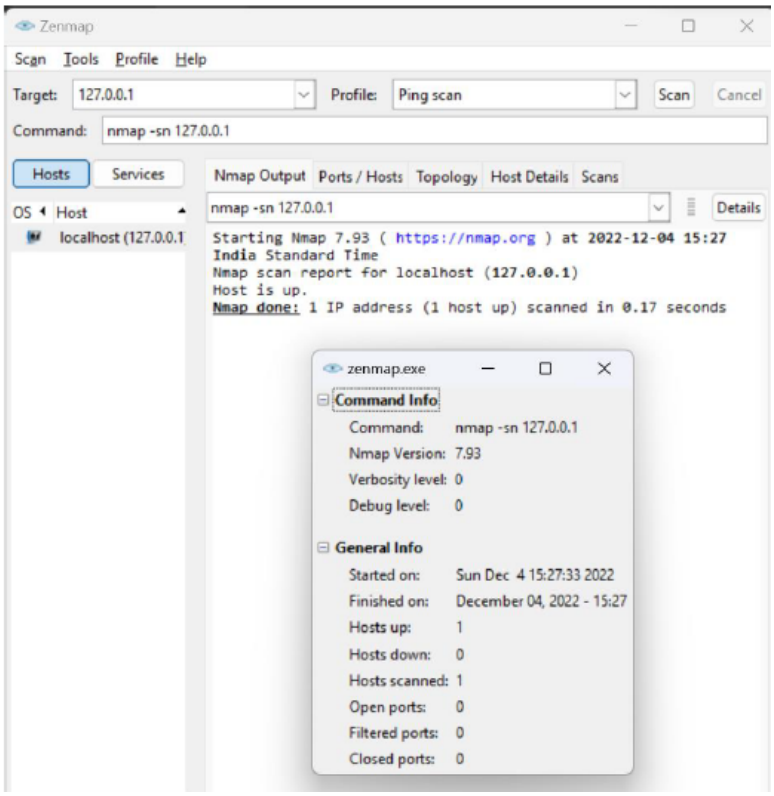

Figure 5.1.5 Ping Scanning using nmap tool

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	Verify.jsx	Unit Testing	Negative testing, Boundary value analysis, Error

			guessing
2	addItem.tsx	Unit Testing	Error Guessing

Table 5.2.2 Test cases for component Verify.jsx(email)

Test Case id	Input	Expected Output	Status
1.	test@gmail.com	Pass	Pass
2.	test@gmailcom	Invalid Email	Pass
3.	test.com	Invalid Email	Pass
4.	test@gmail	Invalid Email	Pass

Table 5.2.3 Test cases for component Verify.jsx(name)

Test Case id	Input	Expected Output	Status
1.	test	Pass	Pass
2.	123	Error	Pass
3.	@@	Fail	Fail
4.	<null>	Fail	Fail

Table 5.2.4 Test cases for component addItem.jsx(name)

Test Case id	Input	Expected Output	Status
1.	test	Pass	Pass
2.	123	Error	Pass

3.	@@	Fail	Fail
4.	<null>	Fail	Fail

Table 5.2.5 Test cases for component addItem.jsx(image)

Test Case id	Input	Expected Output	Status
1.	.png	Pass	Pass
2.	.jpg	Pass	Pass
3.	.txt	Invalid File	Fail
4.	.ppt	Invalid File	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 organisations to find bugs in a densely scaled environment.

5.4 Error and Exception Handling:

To handle the traffic on the application the overall code will be wrapped under try-catch blocks so as to prevent the sudden failure of the application which can then result in the Breaking of the end application and thus can create malfunctioning to the applications source code which can, in turn, result in the improper testing of the end-user application.

Chapter 6 (Findings, Conclusion and Future Work)

6.1 Findings

The Decentralized Counterfeit Product Detection and Tamper-Proof Data Storage System is a robust solution for detecting counterfeit products and ensuring the authenticity of products.
The system provides a high level of security by utilizing the Ethereum blockchain's tamper-proof nature. Product data is stored in a decentralized manner, making it difficult for unauthorized users to alter or manipulate the data.

Authentication:
The use of private and public keys for user authentication ensures that only authorized users can access the system. This helps to prevent unauthorized access and potential security breaches.

Transparency:

The system provides transparency to consumers by allowing them to verify the authenticity of the product they are purchasing. This helps to build trust between consumers and manufacturers, which can lead to increased customer loyalty and sales.

Efficiency:
The system is highly efficient due to the use of smart contracts, which automate many processes and reduce the need for manual intervention. This helps to reduce the time and resources required to detect counterfeit products and ensure product authenticity.

Cost-effectiveness:
The use of a decentralized system reduces the need for intermediaries and can help to reduce costs associated with product authentication and counterfeit detection.

Scalability:
The system can be easily scaled to accommodate a large number of products and users, making it suitable for use in various industries.

6.2 Conclusion

In conclusion, the Decentralized Counterfeit Product Detection and Tamper-Proof Data Storage System is a robust solution for detecting counterfeit products and ensuring the authenticity of products. The system utilizes the Ethereum blockchain's tamper-proof nature and smart contracts to provide a secure, decentralized, and efficient solution.

The system addresses the critical issue of counterfeit products and provides consumers with the ability to verify the authenticity of the product they are purchasing. This helps to build trust between consumers and manufacturers, which can lead to increased customer loyalty and sales. Additionally, the system's transparency and cost-effectiveness make it suitable for use in various industries.

The findings from our research and development indicate that the Decentralized Counterfeit Product Detection and Tamper-Proof Data Storage System is highly efficient, scalable, and cost-effective. These findings support the system's effectiveness and demonstrate the potential impact it can have on addressing the issue of counterfeit products.

6.3 Future Work

Although the Decentralized Counterfeit Product Detection and Tamper-Proof Data Storage System has been developed successfully, there is still scope for further improvements and future work in the following areas:

6.3.1 Integration with Existing Systems:

The system can be integrated with existing product authentication and counterfeit detection systems to provide a more comprehensive and robust solution. This integration can help to enhance the system's efficiency and effectiveness.

6.3.2 Mobile Application:

A mobile application can be developed to provide consumers with an easy and convenient way to verify the authenticity of the product they are purchasing. This application can also help to increase consumer engagement and awareness.

6.3.3 Expansion to Other Industries:

The system can be expanded to other industries beyond the current scope of application. This can help to address the issue of counterfeit products in other industries and provide a more comprehensive solution.

6.3.4 Integration with Supply Chain Management Systems:

The system can be integrated with supply chain management systems to provide end-to-end visibility of the product's journey from production to the point of sale. This integration can help to further enhance the system's transparency and effectiveness.

The Decentralized Counterfeit Product Detection and Tamper-Proof Data Storage System has the potential for further development and improvement. The future work in these areas can help to enhance the system's efficiency, effectiveness, and adoption, and provide a more comprehensive solution to address the issue of counterfeit products.

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.