A

Major Project Report

on

Fake Product Identification Using Blockchain Technology

Submitted in partial fulfillment of the requirements for the award of the degree of

Bachelor of Technology

By

Bagudam Sathvik

(20EG105403)

Gajula Sandeep

(20EG105413)

Vanguri Sravan Yadav

(20EG105449)

Under the guidance of

Mr. Jayendra Kumar

Assistant Professor

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

ANURAG UNIVERSITY

VENKATAPUR (V), GHATKESAR (M), MEDCHAL (D), T.S - 500088

TELANGANA

(2023-2024)

DECLARATION

We hereby declare that the major project report entitled **"Fake Product Identification using BlockChain Technology"** submitted to the **Anurag University** in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology (B. Tech)** in **Computer Science and Engineering** is a record of an original work done by us under the guidance of **Mr**. **Jayendra Kumar, Assistant Professor** and this report has not been submitted to any other University for the award of any other degree or diploma.

Place: Anurag University, Hyderabad

Bagudam Sathvik
(20EG105403)

Gajula Sandeep
(20EG105413)

Vanguri Sravan Yadav
(20EG105449)

CERTIFICATE

This is to certify that the project report entitled **"Fake Product Identification using BlockChain Technology"** being submitted by **B. Sathvik**, bearing the Hall Ticket number **20EG105403**, **G. Sandeep**, bearing the Hall Ticket number **20EG105413, V. Sravan Yadav,** bearing the Hall Ticket number **20EG105449,** in partial fulfillment of the requirements for the award of the degree of the **Bachelor of Technology** in **Computer Science and Engineering** to **Anurag University** is a record of bonafide work carried out by them under my guidance and supervision for the academic year 2023 to 2024.

The results presented in this report have been verified and found to be satisfactory. The results embodied in this report have not been submitted to any other University for the award of any other degree or diploma.

Signature of the Supervisor
Mr. Jayendra Kumar
Assistant Professor

Signature of Dean CSE
Dr. G. Vishnu Murthy

External Examiner

ACKNOWLEDGEMENTS

We would like to express our sincere thanks and deep sense of gratitude to project supervisor **Mr**. **JAYENDRA KUMAR,** Assistant Professor, Department of Computer Science and Engineering, Anurag University for his constant encouragement and inspiring guidance without which this project could not have been completed. His critical reviews and constructive comments improved our grasp of the subject and steered to the fruitful completion of the work. His patience, guidance and encouragement made this project possible.

We would like to acknowledge our sincere gratitude for the support extended by **Dr. G. VISHNU MURTHY**, Dean, CSE, Anurag University. We also express our deep sense of gratitude to **Dr. V. V. S. S. S. BALARAM**, Academic coordinator. **Dr. PALLAM RAVI**, Project Coordinator and project review committee members, whose research expertise and commitment to the highest standards continuously motivated us during the crucial stages of our project work.

We would like to express our special thanks to **Dr. V. VIJAYA KUMAR,** Dean School of Engineering, Anurag University, for his encouragement and timely support in my B. Tech program.

Bagudam Sathvik
(20EG105403)

Gajula Sandeep
(20EG105413)

Vanguri Sravan Yadav
(20EG105449)

ABSTRACT

An anti-counterfeiting decentralized Blockchain solution that manufacturers can use to deliver actual items. This will be accomplished by manner of authenticating the products at each level of the supply chain. For the cause that advent of Blockchain technology in 2008, it's been executed in excessive fields to guarantee high statistics reliability and safety, from the usage of Bitcoin to BaaS (Blockchain as a service), a cutting-edge blockchain fashion that competencies as a form of cloud-primarily based community for organizations who broaden blockchain-primarily based apps. Severe apps had been superior the use of the blockchain, that's gaining recognition. For the reason that Blockchain era serves as the foundation of all applications, the integrity of their statistics is assured. This have a look at applies a decentralized Blockchain technology and supply chain technique to illustrate that forestall customers in a supply chain do no longer definitely rely upon buyers or other one third parties to decide whether or not a product is counterfeit or not. This influences a commercial enterprise agency's income, brand, and backside line. Actual and fake products may be determined through allotted ledger. For each product introduced by manner of the admin which creates particular QR code using SHA256 QR Code era set of regulations and stores into the database .Customers or users scan the QR code and then they can detect the fake product. Digital information of products can be stored in the form of blocks in blockchain technology.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

Product counterfeiting happens when a product is sold pre- tending to be another product. It is consumer fraud and commonly defined as deceptive business practices that cause consumers to suffer financial or other losses. According to the Authentication Solution Providers' Association reports it costs the Indian economy INR 1 trillion every year. Counterfeit incidents are increasing by 20% average in between 2018-20. Counterfeit goods include counterfeit handbags, clothing, cosmetics, and electronics. It not only has negative effects on the economy, but on citizens too. For example, poor cosmetics can affect skin and cause skin diseases and rashes, counterfeit electronic components can cause malfunction in gadgets and can lead to unfavorable situations and mishaps. Poor quality clothes, shoes when worn can cause discomfort. Hence this issue necessitates finding some solution for the sale of counterfeit products.

Another consequence of counterfeiting is that a company's reputation suffers. Because many customers are clueless that the object, they are holding is a knock-off, they will accuse the genuine company if the knock-off product fails to perform properly, comes apart rapidly, or fails to satisfy their expectations. Customer demand recompense, either in the form of a refund or a new product, and they seek it out directly from the legitimate company. A lot of affected businesses may find themselves in a scenario where they are dealing with an unhappy customer who is complaining about the bad quality of the item, and the customer care representative is unaware that the item in question is a counterfeit. Companies are caught between a tough situation, attempting to avoid wasting time and effort dealing with poor imitations of their goods while yet trying to keep their customers pleased. The harm caused by counterfeiters extends beyond customer relationships. Because of the behaviors of counterfeiters, distributors, retailers, and other business partners frequently lose faith in legitimate enterprises.

The most successful mitigation measures for overcoming misleading counterfeit risk in global supply chains include network transparency, cost control and pre-supply evaluation approaches, and Retailer relationship management.

Hence the objective of this project is to present the system designed for anti-counterfeit using Blockchain technology and to give end user and Retailer power to track supply chain of product in a secured environment. In an overview of proposed system, it is aimed to solve the problem

of brand counterfeiting and provide the chance to the customer, vendors and Retailers to check the integrity of the product.

Blockchain is an arrangement of recording information that makes it troublesome or hard to change, hack, or cheat the framework. A blockchain is essentially a computerized record of transactions that is duplicated and distributed across the entire network of PC systems on the blockchain. Each block in the chain contains multiple transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's record. The decentralized database managed by the number of participants is known as Distributed Ledger Technology (DLT). Blockchain is a type of DLT in which transactions are recorded with an immutable cryptographic signature called a hash.

Blockchain technology helps to solve the problem of counterfeiting a product. Blockchain technology is more secure. Once the product is stored on the network hash code is generated of that product and it is possible to maintain all transaction records of the product and its current owner as a chain will be created for that product transactions. All the transaction records will be stored in the form of blocks in the blockchain. In the proposed system we are assigning a generated QR code to a particular product and the end customer can scan that QR code to get all information about that product. After scanning the QR code we can identify that the product is real or fake.

1.1 Project Scope

In recent years, the spread of counterfeit goods has become global. There are many fake products in the current supply chain. According to the report, fake product incidents have risen in the last few years. It is necessary to have a system for customers or users to check the all details of the product so that users can decide that the product is real or fake.

In India currently, there is no such system to detect counterfeit products. So, the solution involves a simple QR code-based identification that can help the end-user or customers to scan and identify the genuineness of the product by using a smartphone.

1.2 Project Objective

The idea of this project came into existence because of the increase in the counterfeit products. The objectives of this project are:

1. To Design Anti Counterfeit System using Blockchain.
2. To secure product details using a QR code.
3. Provide security to the clients by offering data to client.

1.3 Problem Statement

The worldwide improvement of an item or innovation consistently accompanies hazard factors, for example, forging and duplication. Forging items can influence the organization's name and the client's wellbeing. Presently days discovery of phony item is the greatest test. Fake items are causing a significant impact on the organization and the client's wellbeing. Hence, item creators are confronting enormous misfortune.

India and different nations are battling such fake and fake items. In the proposed framework, the framework produces QR codes utilizing Blockchain innovation. This innovation stores exchange records in blocks. These squares are secure and difficult to access and change the data from it. By utilizing a QR code we can recognize the fake item.

1.4 Existing System

The Existing system which can store the product details and they can be changed. Existing System is not feasible to detect fake products unlike the product details are correct. A delivery agent can change the details has he can or an intermediate person can able to change the details if he had the credentials. Existing System won't have any QR code system where there is a database in which the products are been searched using a unique code which can be manipulated.

1.4.1 Disadvantages of Existing System

Following are the disadvantages of existing system:

1. Brands used QR codes on products to prove the validity of the product. But the QR code can be copied and used to label counterfeit product.
2. It is not secure.

1.5 Proposed System

In proposed system, we will be using Quick Response (QR) code and image logo to provide robust technique to try and stop the practice of counterfeiting the products. Fake products can be detected using a Quick Response scanner, where a QR code attached to the product is linked

to the Blockchain network. Now, this concept might be used to store the data like product details and generated unique code for that product as blocks to the database of Blockchain. When the user uploads the unique code and the code is compared to the Blockchain database. If the code matches the code that was generated during the manufacturer, it will notify the customer saying the QR code is matched otherwise it will notify the customer that QR code is not matched and the product is fake.

1.5.1 Advantages of Proposed System

1. The recorded data is difficult to change without the consent of all parties concerned which makes the data extremely secure and protect from all vulnerabilities.
2. To secure product details using a QR code.

1.6 Requirement Specification

1.6.1 Hardware Requirements

Hardware interfaces specify the logical characteristics of each interface between the software product and the hardware components of the system. The following are some hardware requirements.

1. Processor: Intel Dual Core i5 or above
2. Hard disk: 8GB and above
3. RAM: 8GB and above
4. Input devices: Keyboard, mouse.

1.6.2 Software Requirements

Software Requirements specifies the logical characteristics of each interface and software components of the system. The following are some software requirements.

1. Operating system: Windows 8 and above
2. Front end: HTML, JavaScript, CSS, Bootstrap
3. Languages: Solidity
4. Extension: MetaMask
5. RPC: Matic – Mumbai

1.7 Algorithm used

1.7.1 SHA-256 Algorithm

The SHA-256 algorithm is one flavor of SHA-2 (Secure Hash Algorithm 2), which was created by the National Security Agency in 2001 as a successor to SHA-1. SHA-256 is a patented cryptographic hash function that outputs a value that is 256 bits long.

1. Sha-256 algorithm is used in blockchain to get a constant hash of 256 bits every time. This algorithm, is also part of encryption technology. So, now let's see how this algorithm works:
2. In this there is some data called IV which is of 256 bits. Now the input we get will be in the very large. So, be break it in size of 512 bits.
3. As the input will always be not a perfect multiple of 512 bits, So, some part of input will be left.
4. To this left input we do a padding concatenate the input with 10 bits before it. Now our input is perfect multiple, so we can proceed further.
5. Now 512-bit input is added with 256 bits IV to get total of 768 bit. These 768 bits is passed through compression function 'c' to get an output of 256 bit only.
6. This output 256 bit is again merged with 512 bits input from block B2.
7. Again, the total is passed through the compression function to yield a 256-bit output. This loop goes on fill the last block (block n).

2. LITERATURE SURVEY

[1]. Jinhua Ma, Xin Chen, hung-Min Sun, "A Blockchain-Based Application System for Product Anti-Counterfeiting", 2020.

The proposed system uses Ethereum as the back end Blockchain operating system and uses Ethereum's proprietary programming language Solidity as the high-level programming language for writing smart contracts. Solidity supports inheritance, library importing, etc. Solidity is designed for Ethereum Virtual Machine (EVM). Unlike Bitcoin's script, Solidity provides loops and it is Turing complete [1].

The total cost of running an application on the Ethereum public chain is directly related to the code simplicity of the distributed application. The future work of this system can be proof of code simplicity. The customer can trust that the distributed application because of the simplicity of code, and no redundancy code in it will have additional consumption.

[2]. Shovon Paul, Jubair Joy, Shaila Sarkar, "Fake News Detection In Social Media using Blockchain", 2019.

RFID-based anti-counterfeiting and anti-theft schemes are suitable for large scale implementation in retail environments. The proposed scheme is lightweight and suitable for implementation using low-cost passive RFID tags. Tran and Hong's anti-counterfeiting protocol are used. This system is immune to DOS attacks. Habib and Sardar et.al gives explanation on SCM trends[2]. They are examined in their work process that executives' difficulties and transaction issues are problems featured in the SCM. Hence proposed a solution, SCM by considering the blockchain as a technological feature for solving them. Primary method for structuring new models should find the transaction process at a plan level.

In the RFID based system that low-Cost RFID tags can be used for auto identification of products, but due to cloning of RFID tags, this method is not suitable. In AI and machine learning application, CNN takes more time and memory. It needs training and testing phase before its actual deployment. Artificial Intelligence fails to detect tag reapplication attacks, wherein a counterfeiter removes a legitimate tag from a genuine product and reapplies it to a counterfeit or expired product. There is no power for the customer, Retailers and retailers to check the integrity of product.

[3]. Ajay Funde, Pranjal Nahar, Ashwini Khilari, "Blockchain-Based Fake Product Identification in Supply Chain", 2019.

Proposed system to detect fake product with the help of QR code. End users can scan the QR code assigned to product to get the product details and transaction history, the steps involved Product enrolment, ship product to distributor, and ship product to retailer, end user gets details about the products [3].

In a Blockchain based system the data is stored on each node, then the nodes exchange information with each other over the network. Each node maintains all Blockchain data. The node verifies the received transactions and include them in the new block based on its own Blockchain data, and try to obtain the rights of the new block. Ethereum as the back-end Blockchain operating system. Store relevant information on product sales in Blockchain which is accessible to everyone. It is cost efficient. In this blockchain technology for information sharing is proposed. The information is in the control of the owner so third-party interference is difficult. Users are always aware of the data that is being collected about them and how it is used. The blockchain block contains sender, amount, receiver, transaction id, product id and metadata. Ethereum is an open-source Blockchain. Ethereum is a technology that's home to digital money, global payments and applications. The process is simple as to get into the portal, pick a wallet that lets you connect to Ethereum and manage your funds, Get the ETH, use applications powered by Ethereum, start building.

[4]. Si Chen, Rui Shi, Zhuangyu Ren, Jiaqi Yan, "A Blockchain-based Supply Chain Quality Management Framework", 14th IEEE International Conference on e-Business Engineering, 2017.

A Blockchain-based Supply Chain Quality Management Framework by Si Chen. In this paper, we propose a blockchain-based framework. This framework will provide a theoretical basis for intelligent quality management of the supply chain based on blockchain technology. Furthermore, it provides a foundation to develop theories about information resource management in distributed, virtual organizations[4].

Chen and Shi et.al explains SCQI. Framework for blockchain based SCQI provides a theoretical basis to intelligent quality management of supply chains based on blockchain

technology. RFID technology is used to record quality information, trans- action information. Smart contracts are used to execute quality control and improve the efficiency of the supply chain.

[5]. M. Nakasumi, "Information sharing for supply chain management based on block chain technology", IEEE 19th conference on business informatics (CBI), 2017.

To ensure the identification of real products throughout the supply chain, functional blockchain technology is used for preventing product counterfeiting. By using blockchain technology, consumers do not need to rely on trusted third parties to know the source of the purchased product safely. In this paper, counterfeit products are detected using a barcode reader, where a barcode of the product is linked to a Blockchain Based Management (BCBM) system. So, the proposed system may be used to store product details and the unique code of that product as blocks in the database. It collects the unique code from the customer and compares the code against entries in the blockchain database. If the code matches, it will give a notification to the customer, otherwise it gets information from the customer about where they bought the product to detect counterfeit product manufacturers [5]. This paper presents a modern and convenient phenomenon using the Blockchain and Supply Chain technologies which itself dispenses high security and transparency in the system, but to escalate these features some extra characteristics are added in this study which is using the One Time Password (OTP) authentication for verifying the legitimate supply chain members and products, and updating the product details in the blockchain after it is sent to the next stage in the supply chain, and further the product standards are monitored by the Quality Control Officer who is deployed by the factory in-charge for the same. Taking inspiration from the related works of the researchers who have developed various creative models which have been of great use to the community in preventing the counterfeit of products in different industries.

Table 2.1: Literature Survey of Fake Product Identification System.

S. No	Names of the Authors	Title	Year	Description	Merits/ Demerits
1	Jinhua Ma, Xin Chen, hung-Min Sun.	A Blockchain-Based Application System for Product Anti-Counterfeiting.	2020	The proposed system uses Ethereum as the back end Blockchain operating system and uses Ethereum's proprietary programming language Solidity [21] as the high-level programming language for writing smart contracts. Solidity supports inheritance, library importing, etc. Solidity is designed for Ethereum Virtual Machine (EVM). Unlike Bitcoin's script, Solidity provides loops and it is Turing complete.	The total cost of running an application on the Ethereum public chain is directly related to the code simplicity of the distributed application. Since the code is complex the cost of running will be more.
2	Shovon Paul, Jubair Joy, Shaila Sarkar	Fake News Detection In Social Media using Blockchain	2019	In the RFID based system that low-Cost RFID tags can be used for auto identification of products, but due to cloning of RFID tags, this method is not suitable. It needs training and testing phase before its actual deployment. Artificial Intelligence fails to detect tag reapplication attacks, wherein a counterfeiter removes a legitimate tag from a genuine product and reapplies it to a counterfeit or expired product. There is no power for the customer, Retailers and retailers to check the integrity of product.	In AI and machine learning application, CNN takes more time and memory.
3	Ajay Funde, Pranjal Nahar, Ashwini Khilari.	Blockchain-Based Fake Product Identification in Supply Chain.	2019	IPFS (Inter Planetary File System) is useful to maintain ownership of products. IPFS is a peer-to-peer distributed file system it stores a huge volume of data in either object or block or in the file form, it is similar to the Blockchain protocol. Also, it is better than HTTP, as HTTP downloads a file from a single device, and with help of an IPFS network, it is possible to distribute a	The proposed system focus on the disadvantages, promoting the blockchain in tracking, monitoring, and auditing the supply chain and helping manufacturers

				huge volume of data efficiently.	to record the transactions in authenticity.
4	Si Chen, Rui Shi, Zhuangyu Ren, Jiaqi Yan.	A Blockchain-based Supply Chain Quality Management Framework.	2017	we use a blockchain-based SCQI framework. Apart from enterprises on the supply chain, this framework consists of blockchain, smart contracts, and IoT sensors. blockchain provides safe distributed ledger with various quality information, assets information, logistics information and transaction information. Smart contracts bring privacy protection, automation and intelligence into this system, while IoT sensors gather various data from the real world.	These smart contracts are somewhat hard to maintain and take more time to update.
5	M. Nakasumi	Information sharing for supply chain management based on block chain technology	2017	This paper presents a modern and convenient phenomenon using the Blockchain and Supply Chain technologies which itself dispenses high security and transparency in the system, but to escalate these features some extra characteristics are added in this study which is using the One Time Password (OTP) authentication for verifying the legitimate supply chain members and products, and updating the product details in the blockchain after it is sent to the next stage in the supply chain, and further the product standards are monitored by the Quality Control Officer who is deployed by the factory in-charge for the same.	experience for OTP verification and tracing-and-tracking the product is not smoother.

3. DESIGN METHODOLOGY OF FAKE PRODUCT IDENTIFICATION

3.1 System Design

The proposed system uses Ethereum as the back end Blockchain operating system and uses Ethereum's proprietary programming language Solidity as the high-level programming language for writing smart contracts. Solidity supports inheritance, libraries importing, etc. Solidity is designed for Ethereum Virtual Machine (EVM). Unlike Bitcoin's scripts, Solidity provides loops and it is Turing complete. On the system, the public smart contract is based on Ethereum's Blockchain. In this project, for ease of testing, we use Geth to build a private chain and push the smart contract on this Private chain, so that the Private chain simulates the situation of the public chain. We use MetaMask for account balance and contract information management. The user interface seen by the user is a web page. The server side of the web page is made using the http-server suite, which was provided by node.js and web3.js is used as the link between the smart contract and the user interface. The Private Chain and Address information can be connected after setting the server. The overall system relationship is shown in the Figure 3.1.

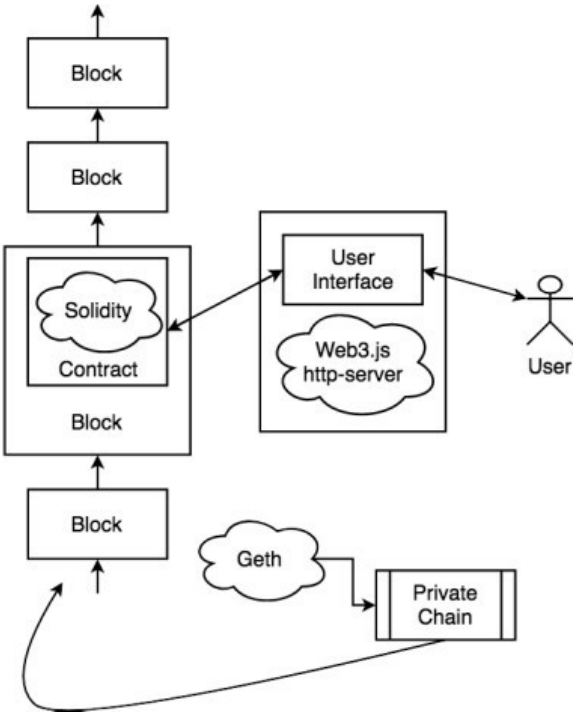

Figure 3.1 System Design of the system

3.2 System Architecture

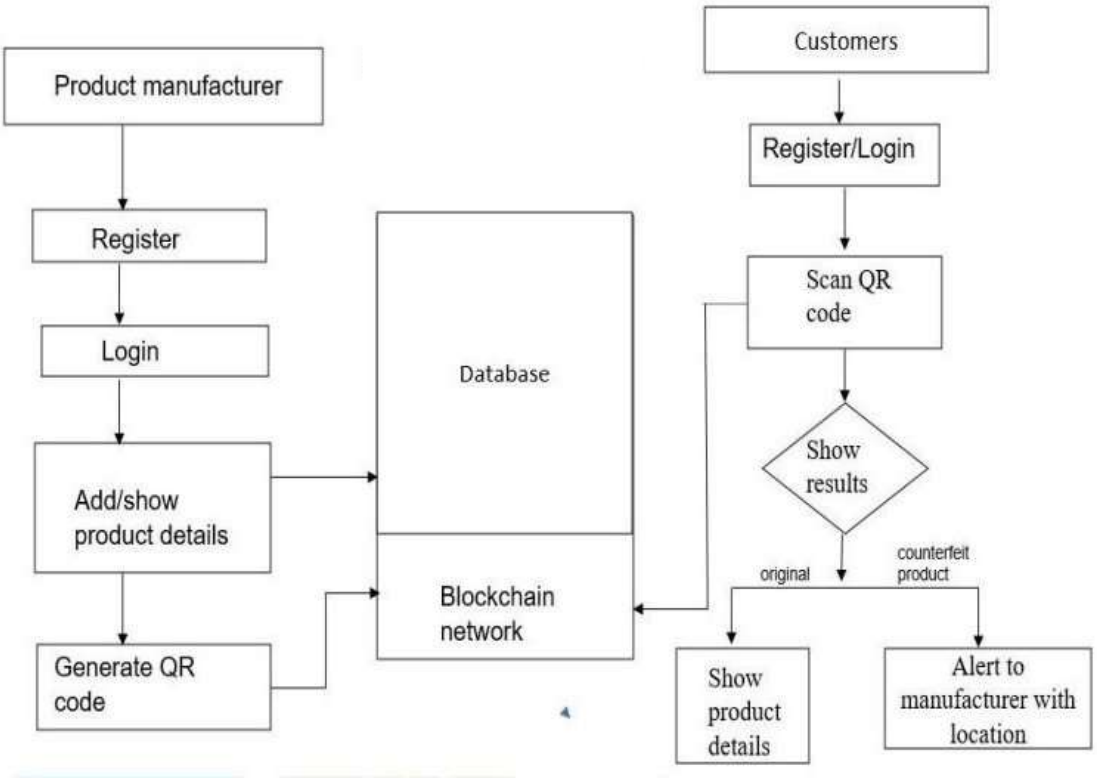

Figure 3.2 System Architecture of the system

Manufacturer:

Manufacturer logs into the manufacturer account and generates QR Code for Product and adds other required details of the product and by using his Ethereum wallet, the manufacturer adds a block to Ethereum blockchain as Shown in Figure 3.2. The user id of our local database and the wallet address of the entity will be mapped together, if both the things are there, that is a manufacturer logs in from his own account and uses his own wallet then only the block will be added to the digital ledger.

Retailer:

Retailer logs into Retailer account and scans the QR code on the product. The seller can access information about his products that the manufacturer has entered. It adds its own details of the product like shop destination and pushes it into the Blockchain. Those details can be viewed by the buyer.

Customer:

Customers can check the integrity of the product by scanning QR code which will list the history of transactions and thus verifying the genuinity of the product. At the time of customer purchasing the product after the QR scan in supply chain history, if the last location is not matched with the purchase location, the customer will know that the product is not genuine. It concludes that the QR code was copied and the customer becomes aware of counterfeiting.

3.3 UML Diagrams

3.3.1 Use Case Diagram

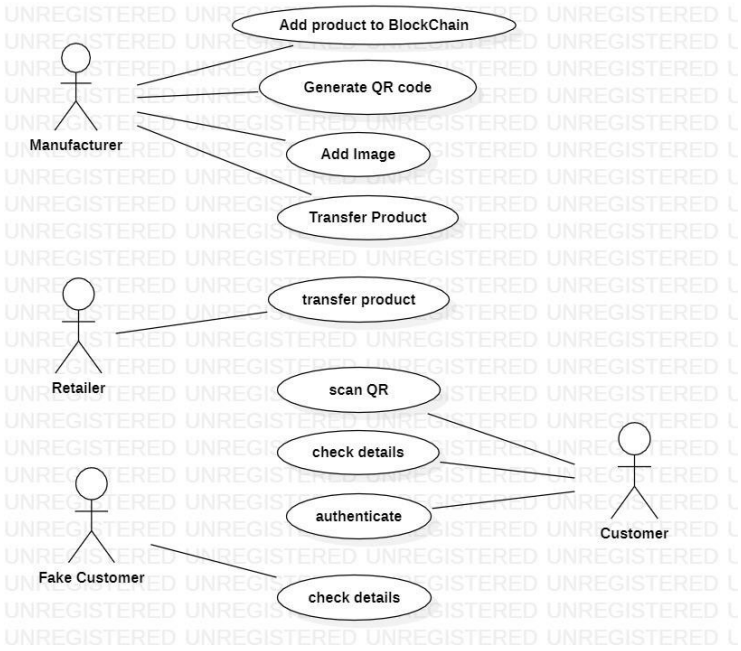

Figure 3.3 Use Case Diagram of Fake Product Identification System

The above Figure 3.3 is a Use Case Diagram which shows various use cases and different types of users the system has. The use cases are represented by either circles or ellipses. The actors are often shown as stick figures. Use Case diagram is helpful in exposing the requirements and planning the project during the initial stage.

3.3.2 Class Diagram

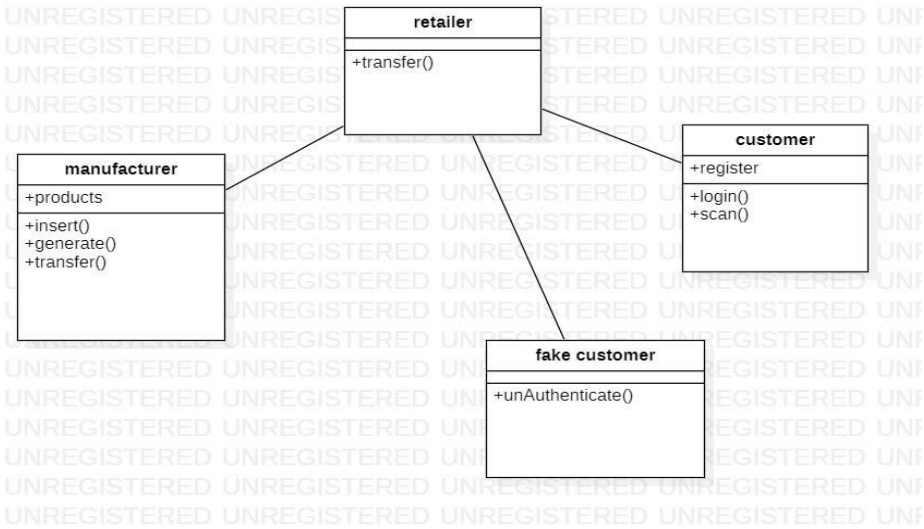

Figure 3.4 Class Diagram of Fake Product Identification System

The above Figure 3.4 is a Class diagram, a type of static diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among objects. A class diagram is used to visualize, describe, document various aspects of the system, and also construct executable software code.

3.3.3 Sequence Diagram

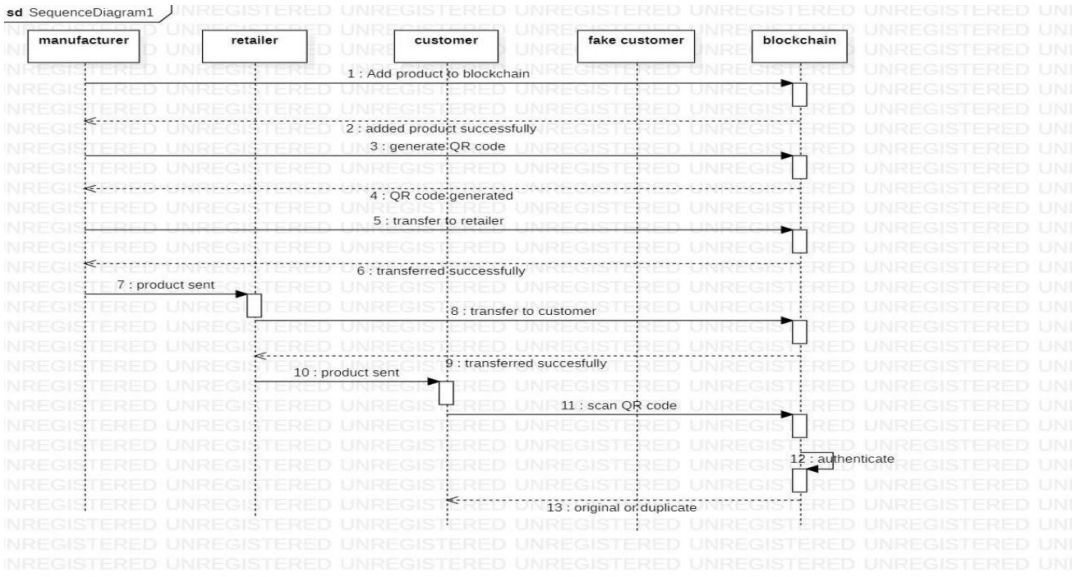

Figure 3.5 Sequence Diagram of Fake Product Identification System

The Figure 3.5 is a sequence diagram which shows object interactions arranged in time sequence. It depicts the objects involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams are typically associated with use case realizations in the logical view of the system under development.

3.3.4 Activity Diagram

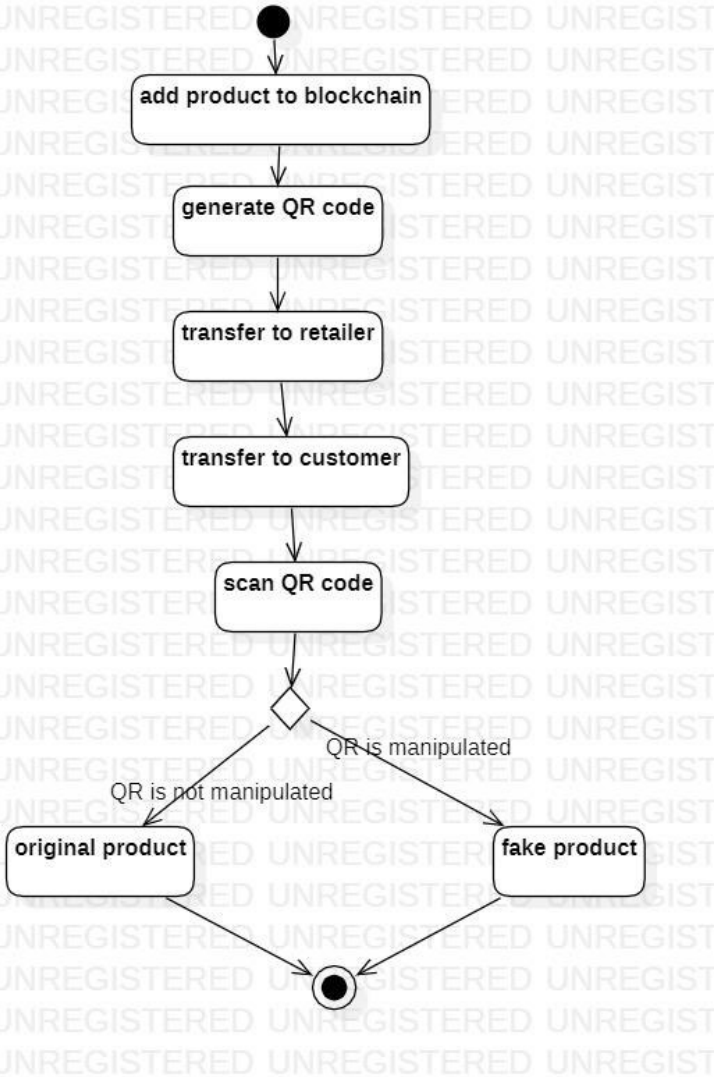

Figure 3.6 Activity Diagram of Fake Product Identification System

The above Figure 3.6 is an activity diagram which is a graphical representation of workflows of stepwise activities and actions with support for choice, iteration and concurrency. They can also include elements showing the flow of data between activities through one or more data stores.

4. TECHNOLOGIES INVOLVED

4.1 BLOCKCHAIN OVERVIEW

Blockchain is a decentralized system. It refers to the collective maintenance of a technical solution that maintains a continuous record file as a reliable database through decentralization. It was initially used extensively on Bitcoin. Figure 4.1 shows connections between blocks in Blockchain. The block generation method of Blockchain is to collect and verify the data and then generate a new block through. We first describe the Blockchain consensus mechanism using Bitcoin as an example, its Blockchain consensus mechanism is a proof of work algorithm (POW). Each node competes based on their respective computing power to solve a SHA256 math problem that is complicated to solve but easy to verify. The first node that solves this problem will get the new block accounting right.

Blockchain data is stored on each node, then the nodes exchange information with each other over the network. Each node maintains an entire Blockchain data. The node will verify the received transactions and include them in the new Blockchain data is stored on each node, then the nodes exchange information with each other over the network. Each node maintains an entire Blockchain data. The node will verify the received transactions and include them in the new

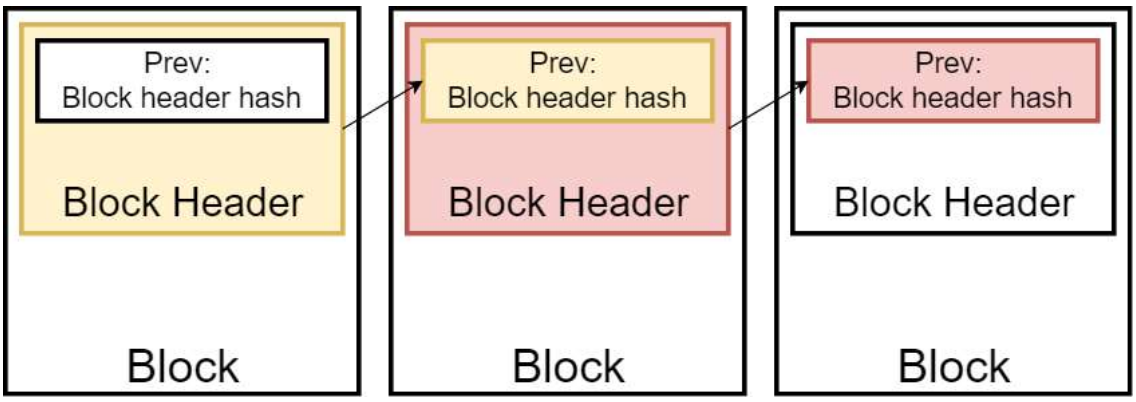

Figure 4.1 Connections between blocks in Blockchain

4.1.1 BLOCKCHAIN 1.0 – BITCOIN

Bitcoin is a decentralized virtual currency that does not rely on specific currency institutions to circulate. By using the Blockchain consensus mechanism to trade virtual currency transactions, the problem of virtual currency security can be perfectly solved, such as the

double-spending problem.

Only when the user's private key is leaked, or forgotten, the user's Bitcoin will be lost, this is shown in Figure 4.2.

Bitcoin is the first practical example of a Blockchain application. It has the following four characteristics:

1. Decentralized peer-to-peer network
2. Public transaction ledger
3. Fixed currency circulation
4. Decentralized transaction verification

Bitcoin is a representative of Blockchain 1.0. The information stored in the block is transaction data. It is used primarily as a decentralized electronic currency. Later, there were other research and development based on Bitcoin, such as color coin. Also, there are some other almost same protocols electronic currency such as Litecoin.

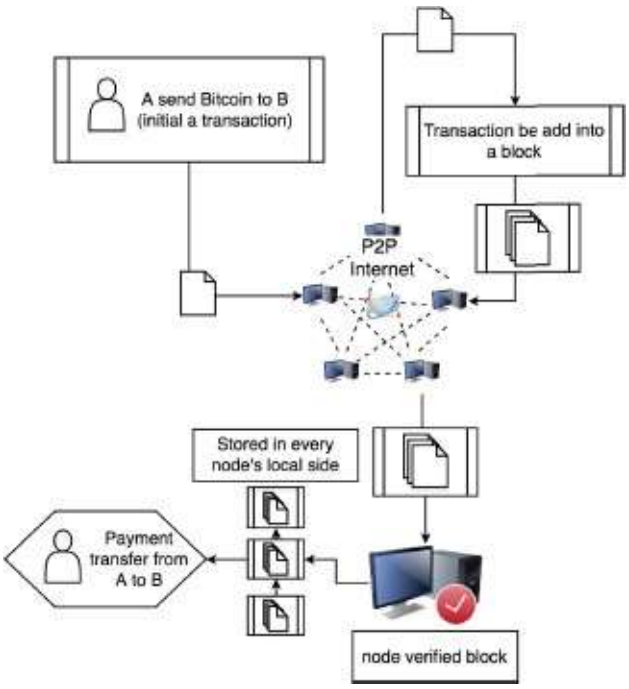

Figure 4.2 Flowchart of sending Bitcoin

4.1.2 BLOCKCHAIN 2.0 AND LATER VERSIONS – ETHEREUM

At the end of 2013, Vitalik Buterin published white paper of Ethereum, and yellow paper was published in 2014. In July 2015 launched Ethereum frontier system and continued to improve it to this day. Ethereum is a Blockchain platform. Unlike the Blockchain technology used by Bitcoin, Ethereum is no longer limited to transaction records and is more effective and robust than its counterpart Bitcoin.

Ethereum is a Blockchain platform that can build smart contracts using a Turing-completeness programming language. Anyone can write smart contracts or other decentralized applications on Ethereum. Users can set access permissions, transaction formats, state conversion equations, and so on, and build any desired rules.

Users of Ethereum will first write a smart contract using Solidity, then they will change their smart contract Solidity code into Ethereum bytecode, and add the bytecode into a transaction and deploy the transaction into the network. When miners of Ethereum receive the transaction, they will record the transaction in a block and run the bytecode in the Ethereum virtual machine each time a transaction of this smart contract is called, which is shown in Figure 4.3. To interact with a smart contract on Ethereum, the user has to send the information packaged in a transaction to communicate with the smart contract and interact with the smart contract by following the rule established within the smart contract. If successful, the smart contract will then have state changed on each miner's local storage. Figure 4.4 shows how transactions happen in Blockchain.

Ethereum is the representative of Blockchain 2.0. There also exist other Blockchain 2.0 and after applications such as Hyperledger. In Blockchain 2.0 and after, there is no longer just transaction data stored in a block. It can be any information, flexibility is much higher than that of Blockchain 1.0.

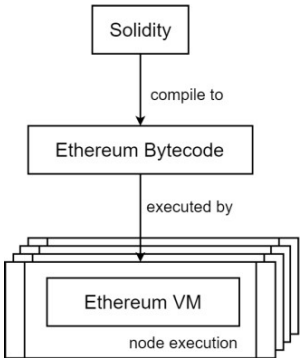

Figure 4.3 State change in Ethereum smart contract

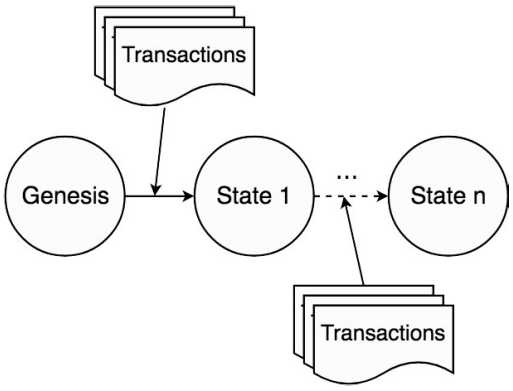

Figure 4.4 Transactions in Blockchain

Table 4.1: Comparison between blockchain 1.0 and blockchain 2.0 and later versions

Features	Blockchain 1.0	Blockchain 2.0 and after
Turing Completeness	No	Yes
State	Only two state	Multi-state
Block Time	Long	Short
Block Storage	Fixed script	Diversity of context height

5. IMPLEMENTATION AND RESULTS

Blockchain features to provide a more complete, convenient, and low-cost product anti-counterfeiting solution for manufacturing, retailer, and customers.

5.1 PROGRAMMING LANGUAGE AND SYSTEM STRUCTURE

The proposed system uses Ethereum as the back end Blockchain operating system and uses Ethereum's proprietary programming language Solidity as the high-level programming language for writing smart contracts. Solidity supports inheritance, libraries importing, etc. Solidity is designed for Ethereum Virtual Machine (EVM). Unlike Bitcoin's scripts, Solidity provides loops and it is Turing complete.

On the system, the public smart contract is based on Ethereum's Blockchain. In this paper, for ease of testing, we use Geth to build a private chain and push the smart contract on this Private chain, so that the Private chain simulates the situation of the public chain. Plus, use Mist for account balance and contract information management. The user interface seen by the user is a web page. The server side of the web page is made using the http-server suite, which was provided by node.js and web3.js is used as the link between the smart contract and the user interface. The Private Chain and Address information can be connected after setting the server. The overall system relationship is shown in the following diagram.

For adding a product in the blockchain, the function we use is

```
function add_product_details(uint32 unique_id, string memory prod_name) public{

      require(msg.sender == owner,"you are not authorized");
      product_details memory new_product ;
      new_product.unique_product_id = unique_id;
      new_product.product_name = prod_name;
      new_product.curr_owner_address = owner;
      new_product.curr_owner_state = owner_status(0);
      all_product_details[unique_id] = new_product;

   }
```

To transfer ownership in the blockchain, the function we use is

```
function transfer_owner_ship(uint32 product_id , address new_address) public{
      require(all_product_details[product_id].curr_owner_address == msg.sender,"you are not
the owner");
      all_product_details[product_id].curr_owner_address = new_address;
      if(all_product_details[product_id].curr_owner_state == owner_status(0)){
         all_product_details[product_id].curr_owner_state = owner_status(1);
      }else{
         all_product_details[product_id].curr_owner_state = owner_status(2);
      }
   }
```

1.1 GAS

Gas is the pricing value of the execution work in Ethereum. When the user wants to make some state change in the smart contract, the user has to pay the corresponding state change gas. Different program operation cost different amounts of gas to run the operation. The operation cost of gas is a fixed number. For instance, each SHA3 operation costs 30 gas, and the paid for each byte in a LOG operation's data cost is 6 gas. There is a function cost used in our system exhibited as follows

Table 5.1: Some of the fee in execution operations used in our system

Operation description	Fee cost
Memory expanding for each addition word	3 gas
The contract creation operation	32000 gas
For every transaction	21000 gas
Each SHA3 operation	30 gas
Get transaction caller address	2 gas
Every zero byte of data for a transaction	4 gas
Contract suicide operation	5000 gas

GAS PRICE

Gas price is the current price of gas. The gas price can be set by the user for any Wei. However, the higher the gas price is, the faster the transaction will be conducted in a block since the miner wants to earn higher rewards from the transaction and will give higher priority to the transaction with the higher price. EthGasStation is an open-source project that aims to increase the transparency of gas price. This site estimates over last 1,500 blocks and finds the recommended gas price for the user. The following are the estimate data of gas price in last 1500 blocks from block 5785125. The transaction is conducted in a block within five minutes. The statistics we choose are from EthGasStation. The recommended gas price it provides is based on the current network conditions and will have wave motion at different times. We choose the data with the latest update time in Block 5785125.

Table 5.2: The relation between transaction accepts speed and gas price in last 1500 blocks.

Transaction speed	Gas price
Lower than 30 minutes	3 gwei
Lower than 5 minutes	4 gwei
Lower than 2 minutes	14 gwei

Table 5.3: The relation between statistic set and exchange rate in last 1500 blocks

Statistic Set	Exchange rate
Earliest data in UTC time	498.02 US dollars
Highest data in the day	501.91 US dollars
Lowest data in the day	459.00 US dollars
Latest data in UTC time	477.49 US dollars

1.1.1 COST RESULT

Here we employ Remix to calculate the gas need in our system function execution. Remix is a web browser IDE for developers in developing solidity Decentralized Application (DApp). Our system function execution gas spend is in Table 5.1. The contract deploy function will only be called once for a new product. In our previous section prediction, the cost of contract deployment is 1.2893394289 US dollars. The other function cost will be 0.17415436749 US dollars, which means that each time a product sales process complete, it will cost 0.17415436749 US dollars. The overall cost of using our system for preventing counterfeited products is remarkably low cost to implement, and very straightforward to apply.

1.2 RESULTS

The below Figure 5.1 shows the home page of the application, the interface is created using basic HTML, CSS, JS and Bootstrap.

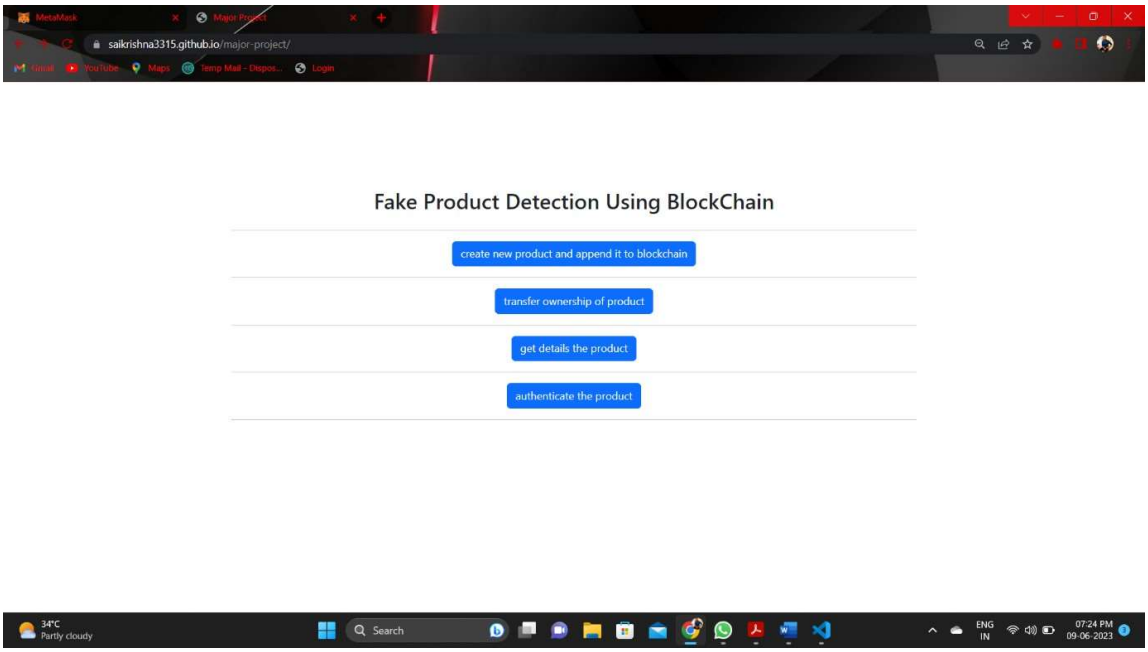

Figure 5.1 Home page of the application

The below Figure 5.2 shows, how we connect to the MetaMask wallet when we click on the connect wallet button from create new product page.

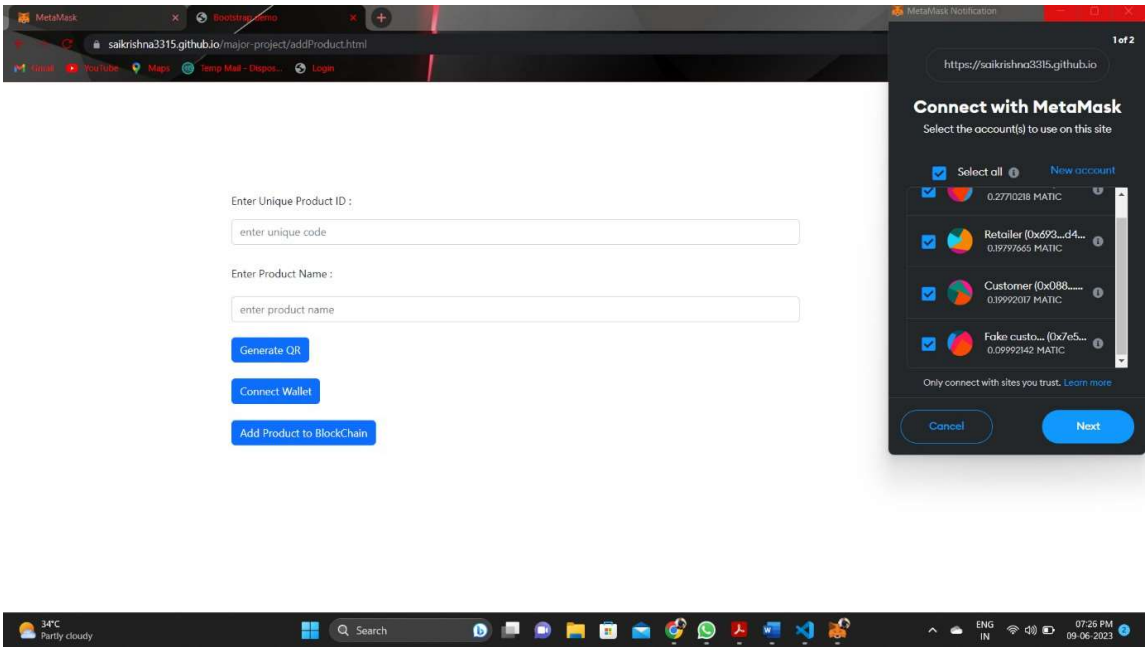

Figure 5.2 Connecting to the MetaMask wallet

After that, clicking next in the Metamask prompt, makes you connect to the Metamask wallet. It will generate a connected successfully prompt as shown in Figure 5.3

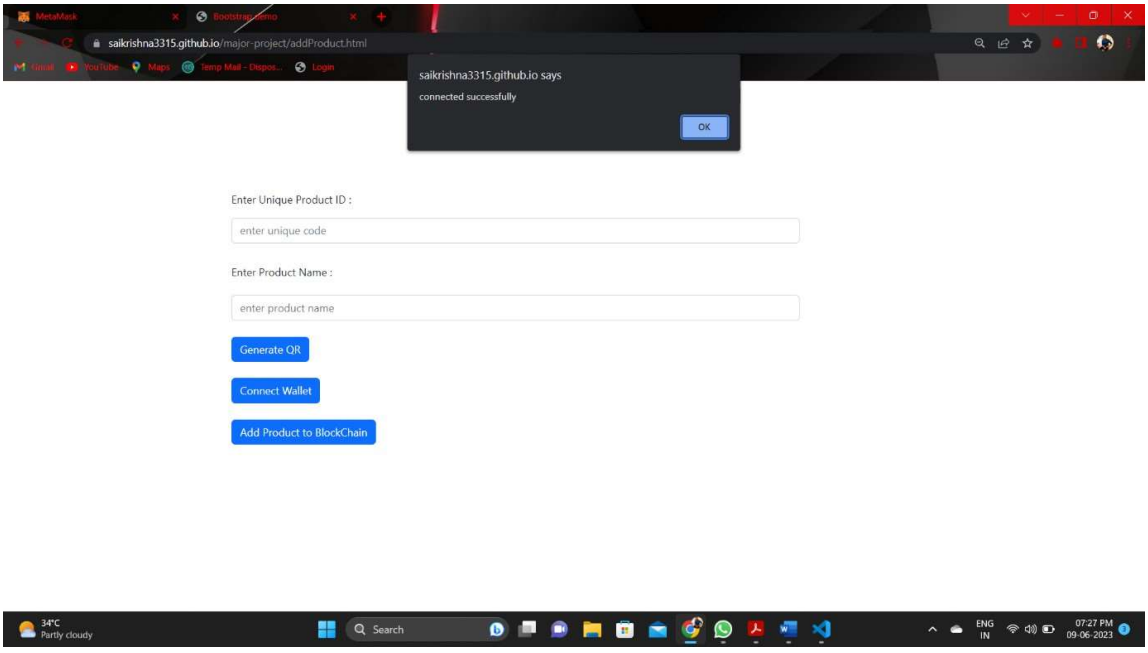

Figure 5.3 Successfully Connected to the MetaMask wallet

For the generating the QR Code of the product, we should enter product id and name then press Generate QR button. This will generate QR as shown in Figure 5.4

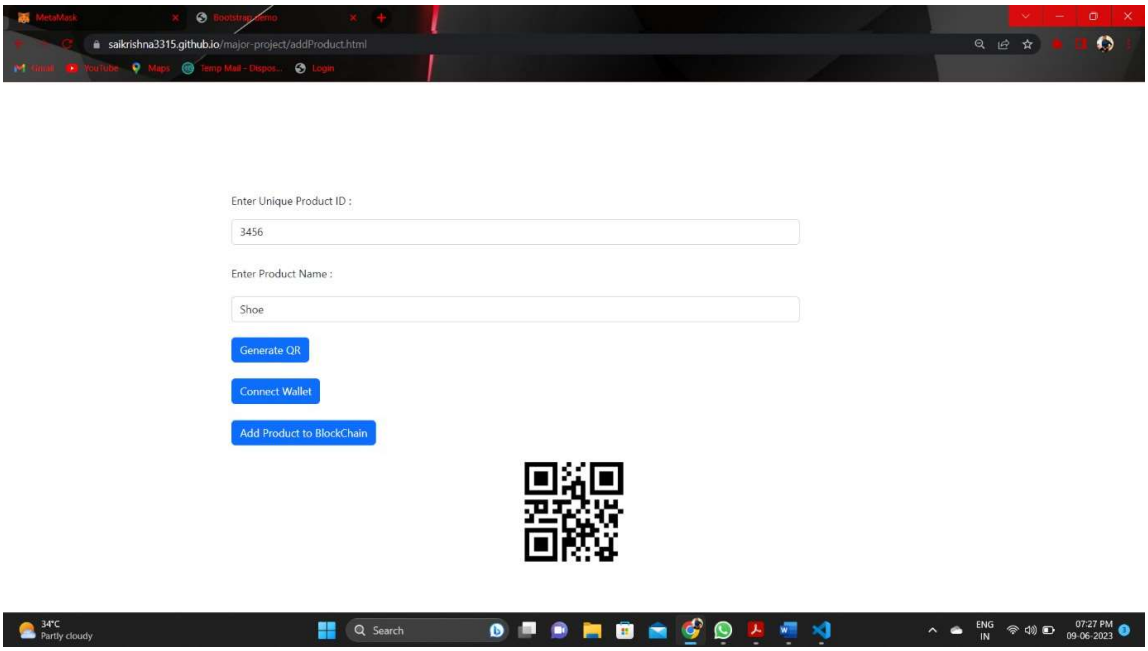

Figure 5.4 Generate QR code

After generating the QR, we should add it to the Blockchain, when we click on Add product to Blockchain button, again a metamask prompt appears to confirm as shown in Figure 5.5

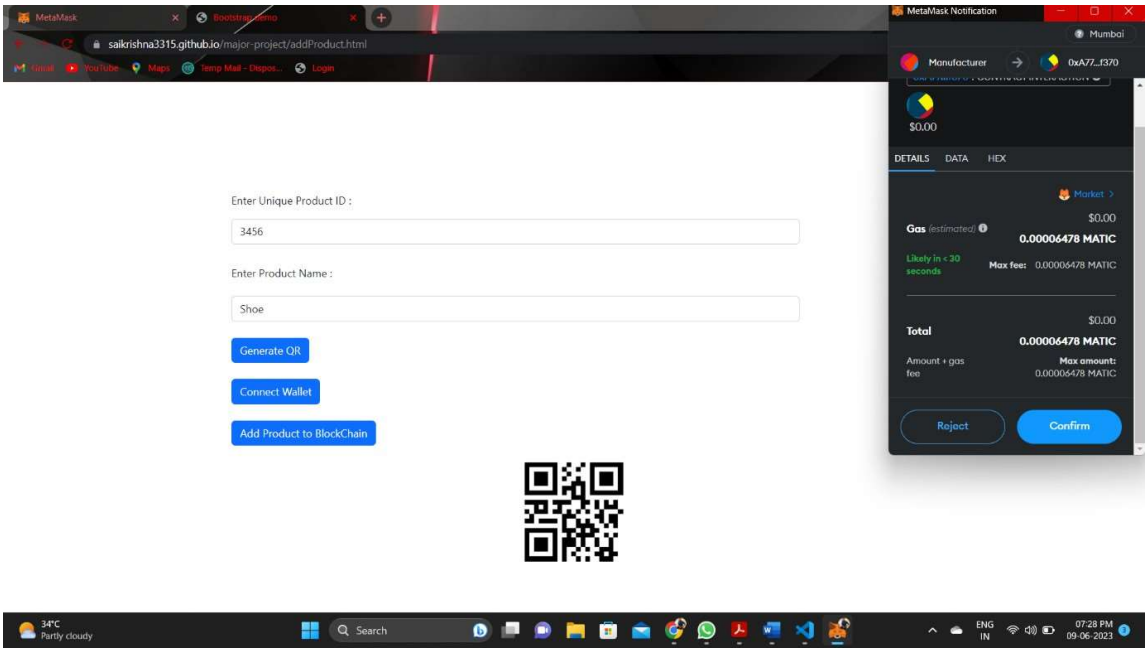

Figure 5.5 Adding the product to the Blockchain

The below Figure 5.6 shows the data inserted into blockchain alert when we confirm the transaction, which consumes some amount of gas to make it successful.

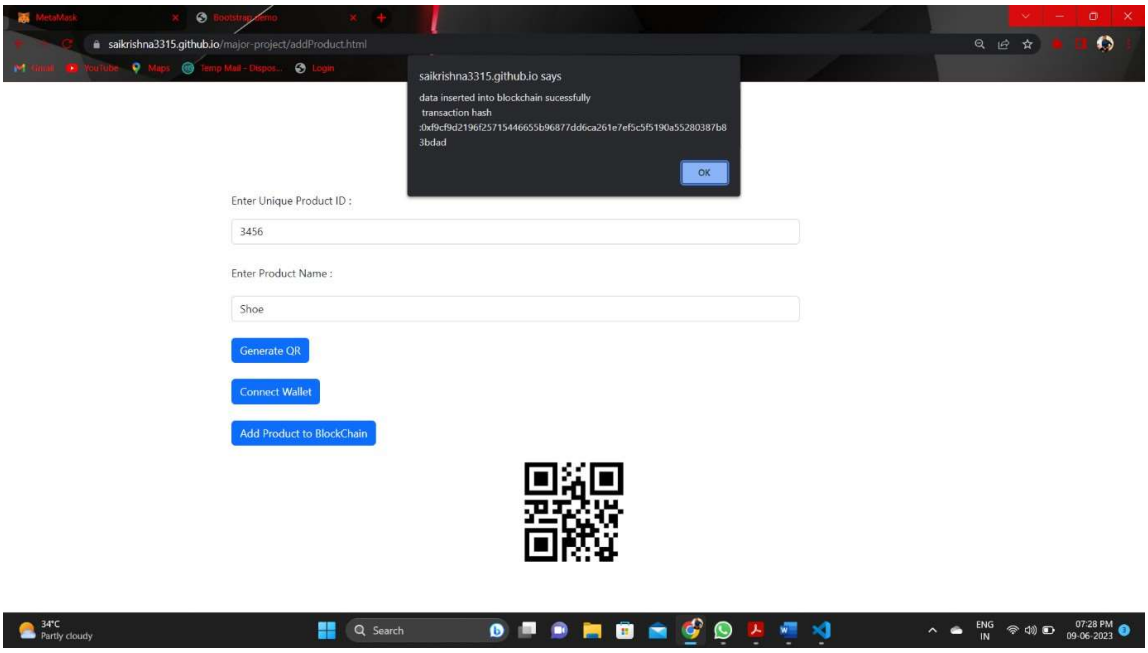

Figure 5.6 Successfully added the product to the Blockchain

We can get details of the product from get details screen, which ask you scan the QR. After that it fetch the complete details of the product like id, name, current owner address and product holder as shown in Figure 5.7

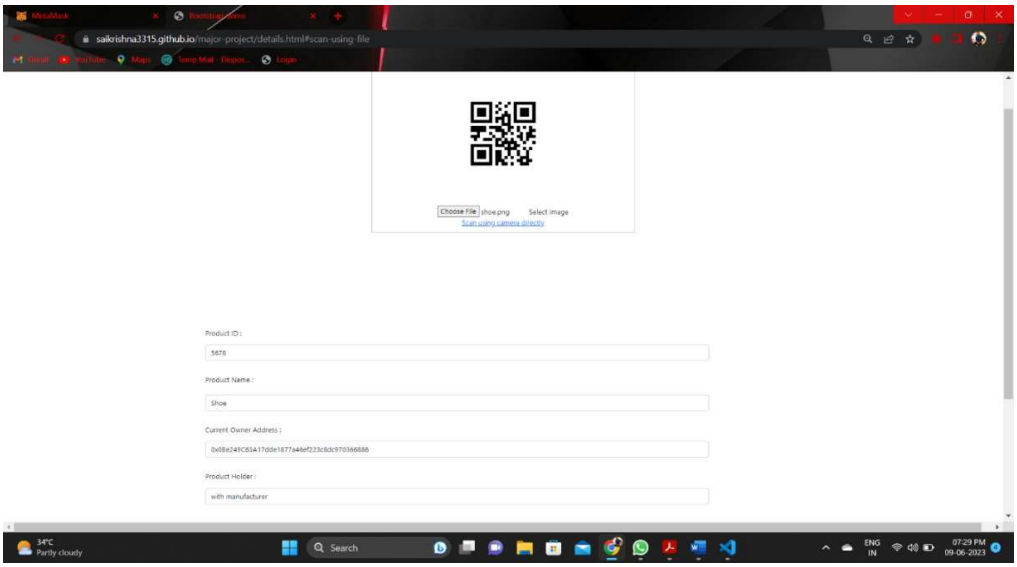

Figure 5.7 Get details page

We can transfer the product from transfer product screen, by clicking transfer ownership button, which again prompts you to confirm in MetaMask as shown in Figure 5.8 and it generates a alert of successfully transferred as shown in Figure 5.9

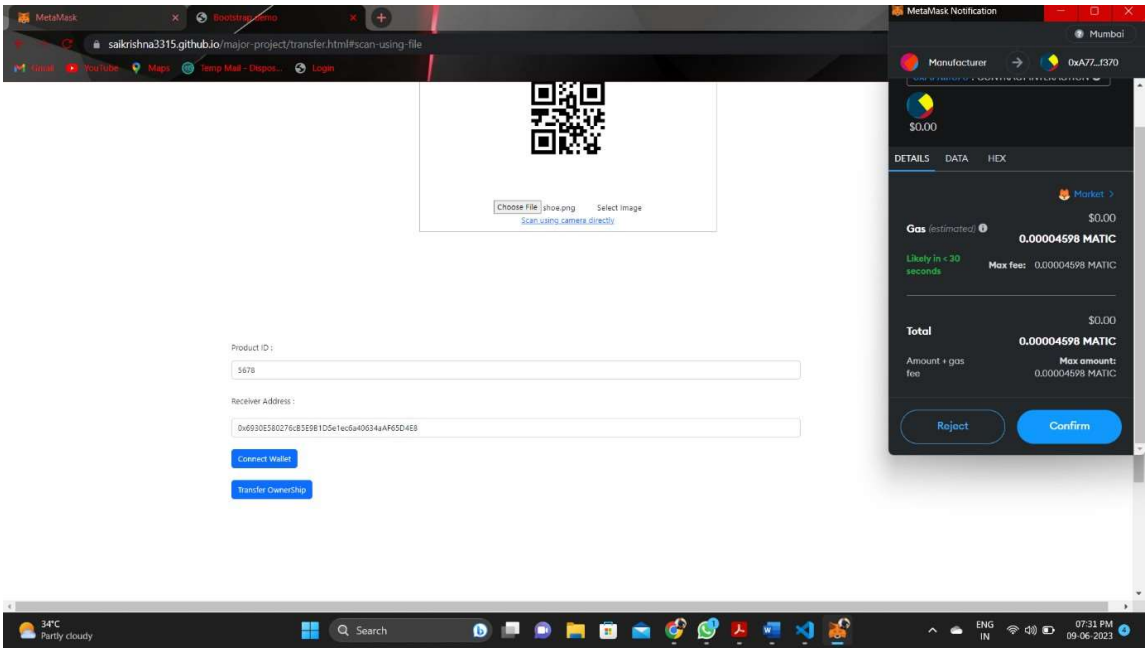

Figure 5.8 Transfer ownership

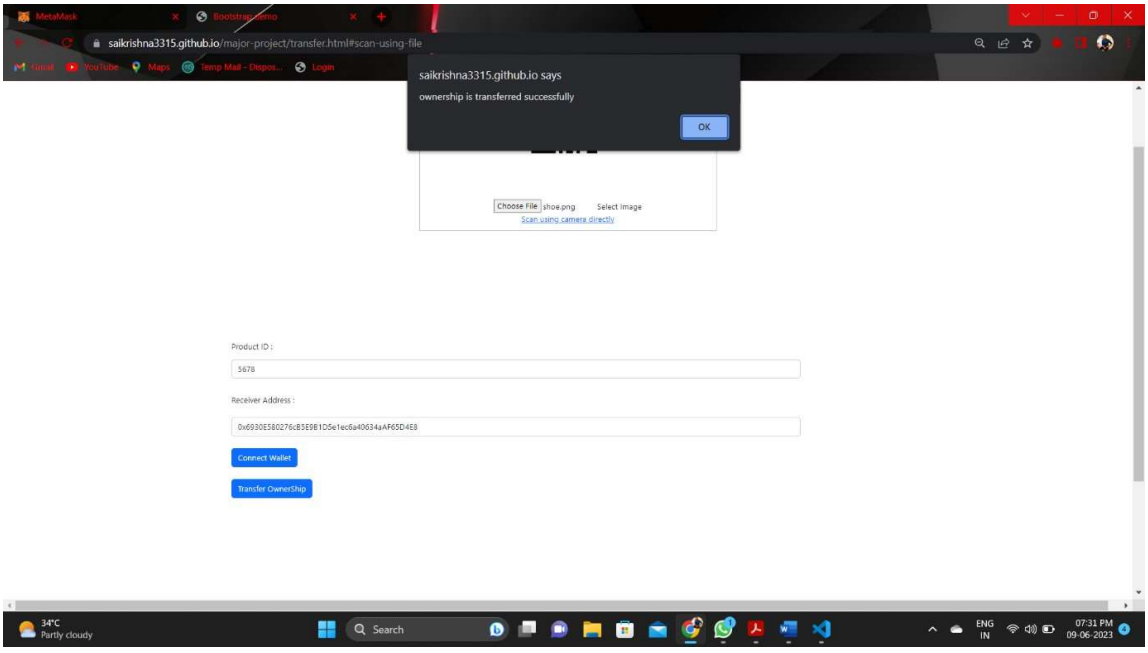

Figure 5.9 Ownership transferred successfully

After transferring the product, we can validate the product whether it is fake or original in authenticate product screen. If it is fake, it will generate a alert as shown in Figure 5.10 and if it is original, it will generate alert as shown in Figure 5.11.

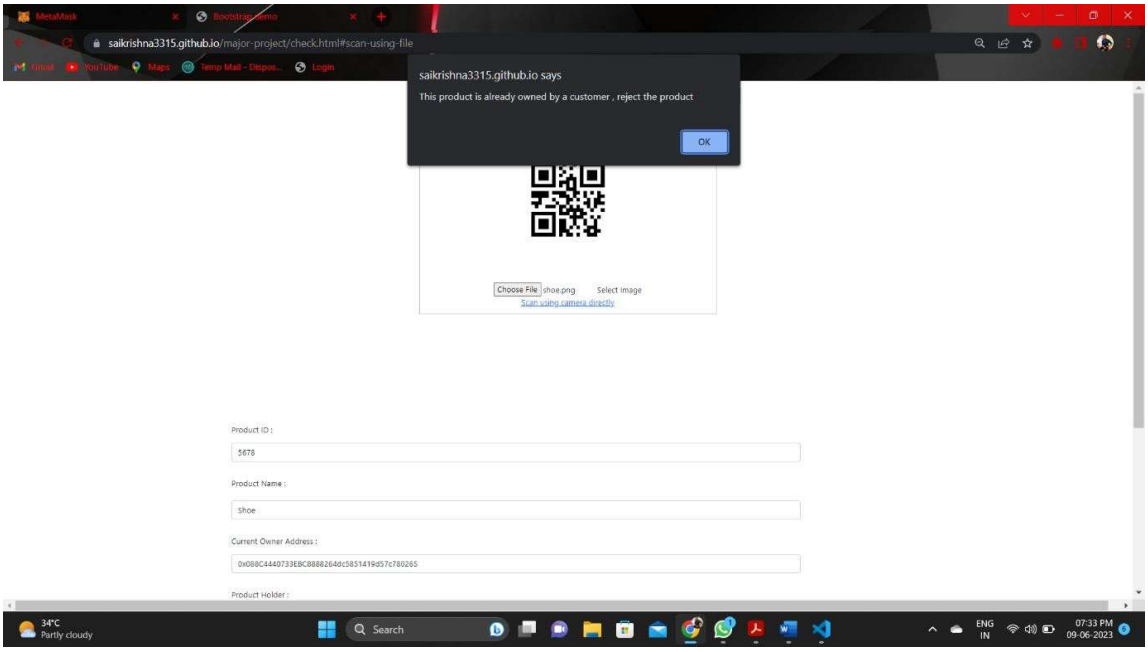

Figure 5.10 Fake product alert

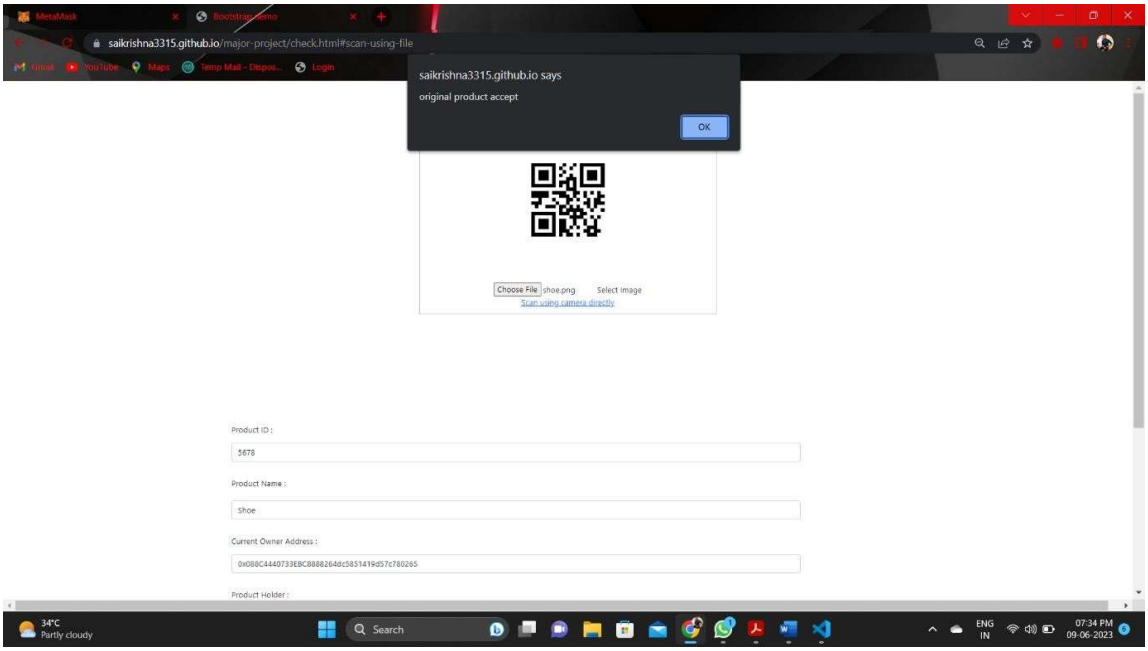

Figure 5.11 Original product alert

CONCLUSION

Blockchain system that proposes a fully functional anti-product forgery system. By paying a very low transaction fee, users of our system no longer need to be concerned about the possibility of acquiring a counterfeited product.Manufacturers can use the system to store relevant information on product sales in Blockchain which is accessible to everyone. The total amount of sales that can be sold by the seller and the number of products currently left by the seller are transparent. The user can use the functions provided by our system to immediately perform vendor-side verification. The system provides identity verification by using digital signatures. There are no other means to decrypt the private key of the key owner unless the key owner accidentally leaks his key.

FUTURE SCOPE

Anti-fraud Solutions: The combination of blockchain and image processing can be used to detect fraudulent activities, such as insurance fraud, credit card fraud, and identity theft.

Consumer Protection: Blockchain can provide consumers with a secure and transparent way to verify the authenticity of a product. This can help build trust between brands and consumers, and ensure that consumers are not unknowingly purchasing counterfeit products.

Smart Contracts: Smart contracts can be used to automate the process of detecting counterfeit products. For example, a smart contract can be created to trigger a notification if the product is not registered on the blockchain or if there is any tampering with the product's packaging or label.

REFERENCES

[1]. Jinhua Ma, Xin Chen, hung-Min Sun, “A Blockchain-Based Application System for Product Anti-Counterfeiting”, 2020.

[2]. Shovon Paul, Jubair Joy, Shaila Sarkar, “Fake News Detection In Social Media using Blockchain”, 2019.

[3]. Ajay Funde, Pranjal Nahar, Ashwini Khilari, “Blockchain-Based Fake Product Identification in Supply Chain”, 2019.

[4]. Si Chen, Rui Shi, Zhuangyu Ren, Jiaqi Yan, “A Blockchain-based Supply Chain Quality Management Framework”, 14th IEEE International Conference on e-Business Engineering, 2017.

[5]. M. Nakasumi, “Information sharing for supply chain management based on block chain technology”, IEEE 19th conference on business informatics (CBI), 2017.

[6]. J. Leng, P. Jiang, K. Xu, Q. Liu, J. L. Zhao, Y. Bian, and R. Shi, Makerchain: A blockchain with chemical signature for self-organizing process in social manufacturing," J. Cleaner Prod., vol. 234, pp. 767-778, Oct. 2019.

[7]. N. Alzahrani and N. Bulusu, ``Block-supply chain: A new anti-counterfeiting supply chain using NFC and blockchain," in Proc. 1st Workshop Cryptocurrencies Blockchains Distrib. Syst. (CryBlock), 2018, pp. 30-35.

[8]. M. Rosenfeld. (2012). [Online]. Available: https://bitcoil.co.il/BitcoinX.pdf

[9]. S. Matthew English and E. Nezhadian, ``Application of bitcoin data-structures & design principles to supply chain management," 2017, arXiv:1703.04206. [Online]. Available: http://arxiv.org/abs/1703. 04206

[10]. F. Tian, ``An agri-food supply chain traceability system for China based on RFID & blockchain technology," in Proc. 13th Int. Conf. Service Syst. Service Manage. (ICSSSM), Jun. 2016, pp. 1-6.

[11]. S. Shepard, RFID: Radio Frequency Identification. New York, NY, USA: McGraw-Hill, 2005.

[12]. Q. Lu and X. Xu, ``Adaptable blockchain-based systems: A case study for product traceability," IEEE Softw., vol. 34, no. 6, pp. 21-27, Nov./Dec. 2017.

[13]. K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, ``A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain," IEEE Access, vol. 5, pp. 17465-17477, 2017.

[14]. Zignuts Technolab, how blockchain architecture works? basic understanding of blockchain and its architecture., https: / / www.zignuts.com / blogs/ how - blockchain - architecture - works - basic - understanding- of- blockchain- and-its- architecture/ (2022)

[15]. Fake News Detection in social media using Blockchain: - Shovon Paul, Jubair Joy, Shaila Sarkar.

[16]. M.A. Benatia, D. Baudry, A. Louis, Journal of Ambient Intelligence and Humanized Computing PP. 1-10 (2020)

[17]. E. Daoud, D. Vu, H. Nguyen, M. Gaedke, Improving Fake Product Detection Using Ai-Based Technology, in 18th International Conference e-Society (2020).

[18]. S. Panikkar, S. Nair, P. Brody, and V. Pureswaran, ``ADEPT: An IoT practitioner perspective," IBM Inst. Bus. Value, New York, NY, USA, White Paper, 2015, pp. 1-18