**KATHFORD INTERNATIONAL COLLEGE OF**

**ENGINEERING AND MANAGEMENT**

Balkumari, Lalitpur

A

Major Project Report

On

**“FAKE PRODUCT IDENTIFICATION USING QR CODE BASED ON BLOCKCHAIN SYSTEM”**

[Subject Code: EX707]

**Project Members**

Bharat Karki (003/BEX/2074)

Niranjan Tamang (007/BEX/2074)

Sagar Shrestha (011/BEX/2074)

**DEPARTMENT OF COMPUTER AND ELECTRONICS**

**COMMUNICATION AND INFORMATION ENGINEERING**

**LALITPUR, NEPAL**

**APRIL, 2022**

**KATHFORD INTERNATIONAL COLLEGE OF ENGINEERING AND MANAGEMENT**

Balkumari, Lalitpur

(Affiliated to Tribhuvan University)

**“FAKE PRODUCT IDENTIFICATION USING QR CODE BASED ON BLOCKCHAIN SYSTEM”**

A

PROJECT REPORT

SUBMITTED TO THE DEPARTMENT OF COMPUTER AND ELECTRONICS, COMMUNICATION AND INFORMATION ENGINEERING IN PARTIAL FULFILLMENT OF THE

REQUIREMENTS FOR THE DEGREE OF BACHELOR IN ELECTRONICS & COMMUNICATION ENGINEERING

**Submitted by:**

Bharat Karki (25053)

Niranjan Tamang (25055)

Sagar Shrestha (25059)

**Submitted to:**

DEPARTMENT OF COMPUTER AND ELECTRONICS COMMUNICATION AND INFORMATION ENGINEERING

APRIL, 2022

**COPYRIGHT**

No part of this report can be copied without the permission of the authors. However, the authors have agreed that the Library, Department of Computer and Electronics & Communication, Kathford International College of Engineering and Management may take this project freely available for inspection. Moreover, authors have agreed that the permission for extensive copying of this project for scholarly purpose may be granted by the Professor(s), who supervised the project. It is understood that recognition will be given to the authors and to the department in any use of the parts of this project. Copying of publication or other use of this project for financial gain without approval of the department and author’s written permission is prohibited.

Request for permission to copy or to make any use of the material in this project in whole or part should be addressed to:

Head of the Department

Department of Computer and Electronics & Communication Engineering Kathford International College of Engineering and Management

Balkumari, Lalitpur,

Nepal

**TRIBHUVAN UNIVERSITY**

**KATHFORD INTERNATIONAL COLLEGE OF ENGINEERING AND MANAGEMENT**

**DEPARTMENT OF COMPUTER AND ELECTRONICS & COMMUNICATION ENGINEERING**

**Letter of Approval**

The undersigned certify that they have read and recommended to the Department of Computer and Electronics & Communication Engineering for acceptance, a project entitled **“FAKE PRODUCT IDENTIFACTION USING QR CODE BASED BLOCKCHAIN SYSTEM”**, submitted by **Bharat Karki, Niranjan Tamang** and **Sagar Shrestha** in partial fulfillment of the requirement for the major project of **“Bachelor in Electronics and Communication Engineering”**.

External Examiner: Project Coordinator and Supervisor:

…………………… …………………………

Er. Saban Kumar K.C.

Lecturer

Department of Computer and Electronics Engineering

Kathford International College of Engineering and Management

APRIL, 2022

Balkumari, Lalitpur-8, Nepal

**Tel.:** +977-1-5201241/5201911

**Fax:** +977-1-5201899

G.P.O.Box: 23483, Kathmandu

**E-mail:** info@kathford.edu.np

**Web:** www.kathford.edu.np

**DEPARTMENTAL ACCEPTANCE**

The project entitled “**FAKE PRODUCT IDENTIFICATION USING QR CODE BASED ON BLOCKCHAIN SYSTEM**”, submitted by ***Bharat Karki, Niranjan Tamang*** *and* ***Sagar Shrestha*** in partial fulfillment of the requirement for the major project in **“*Bachelor in Electronics and Communication Engineering*”** has been accepted as a bonfire record of work carried out by them in the department.

………………………….

**Er. Prabin Kumar Jha**

Deputy Head of the Department

Department of Computer and Electronics & Communication Engineering Kathford International College of Engineering and Management

Balkumari, Lalitpur

Nepal

APRIL, 2022

**ACKNOWLEDGEMENT**

We would like to acknowledge the guidance and constructive suggestions provided by the teachers and individuals in course of the preparation of this report. We would like to express our sincere thanks to **Er. Saban Kumar K.C**, Project Coordinator for his assistance and help during the process.

We are also obliged to all the individuals and groups who have directly or indirectly assisted in the preparation of this report, especially **Er. Bikal Adhikari** and **Er. Kiran Bagale** for providing the comments and assistance in preparing the report. We extend our gratitude towards DHOD of Department of Electronics and Communication of Kathford International College of Engineering and Management **Er. Prabin Kumar Jha** for providing us the opportunity and the required environment, support and help to do this project.

We would like to convey our thanks to all teaching and non-teaching staff members of Department of Computer and Electronics & Communication Department of Kathford Engineering College of Engineering and Management for their invaluable support and help throughout the project period.

Also, we would like to express our deep sense of gratitude to our seniors **Er. Bibek Koirala** and **Er. Mahesh Sharma**, our friend **Mr. Abiral Bhandari,** all our beloved friends and family members who tried to encourage us while doing this project with their valuable suggestions to approach our goals. The entire team is thankful to all the peoples who have either directly or indirectly helped for the successful completion of the project.

Lastly, we would humbly welcome any suggestions and guidance for the improvement of this report.

Thank You.

# ABSTRACT

A counterfeit product results in huge loss to company. In Nepal, a lot of counterfeits are found in market. As a result of counterfeit product, it not only makes customer dissatisfied but also a loss to retailer. A lot of solution to these problems have been addressed using various techniques. And most of the solutions are based on centralized system where information about product is stored in central server. In such centralized system, there are lots of problems such as single point of failure, prone to attacks. Using the Blockchain, data is distributed over the peer-to-peer network instead of central server handling all the data. In Blockchain, data is shared among the nodes in network. In this prototype, information about the product is stored in distributed ledger so that any one on the network can view the data. By scanning QR codes attached to the product, a customer can query about the product that he/she is buying and check whether the product is genuine or not. The main aim of this project is to make decentralized application (Dapps) using framework such as hardhat and implement business logic in the smart contract using solidity programming language. QR code is attached to the product containing hash value of product information and is stored in blockchain. A customer scans QR code to get product information. If someone has attached QR code to product which is fake, then it will be easily identified.

**Keywords:** Blockchain, Ethereum, Smart contracts, anti-counterfeiting, decentralization

# TABLE OF CONTENTS

[ABSTRACT i](#_Toc100688949)

[TABLE OF CONTENTS ii](#_Toc100688950)

[LIST OF FIGURES iv](#_Toc100688951)

[LIST OF ABBREVIATIONS v](#_Toc100688952)

[1. INTRODUCTION 1](#_Toc100688953)

[1.1 Background 1](#_Toc100688954)

[1.2 Problem Statement 1](#_Toc100688955)

[1.3 Objectives 2](#_Toc100688956)

[1.3.1 Main Objective 2](#_Toc100688957)

[1.3.2 Specific Objectives 2](#_Toc100688958)

[1.4 Scopes and Application 2](#_Toc100688959)

[2. Literature Review 3](#_Toc100688960)

[3. Project Methodology 8](#_Toc100688961)

[3.1 Block Diagram 8](#_Toc100688962)

[3.2 Flow chart 14](#_Toc100688963)

[3.3 UML diagram 16](#_Toc100688965)

[3.3.1 Use Case diagram 16](#_Toc100688966)

[3.3.2 Sequence Diagram 17](#_Toc100688967)

[4. Hardware and Software requirements 19](#_Toc100688968)

[4.1 Hardware Requirements 19](#_Toc100688969)

[4.2 Software Requirement 19](#_Toc100688970)

[5. Results and Discussion 23](#_Toc100688971)

[5.1 Results 23](#_Toc100688972)

[5.2 Discussion 27](#_Toc100688973)

[6. Conclusion 29](#_Toc100688974)

[7. Limitation and Future Enhancement 30](#_Toc100688975)

[7.1 Limitations: 30](#_Toc100688976)

[7.2 Future Enhancement: 30](#_Toc100688977)

[8. References 31](#_Toc100688978)

[Appendices 33](#_Toc100688979)

# LIST OF FIGURES

[**Figure 3‑1: Block Diagram of the System** 8](file:///C:\Users\niran\Downloads\final.docx#_Toc100612885)

[**Figure 3‑2: Public Key Cryptography** [16] 12](#_Toc100612886)

[**Figure 3‑3: Flow chart of system** 14](file:///C:\Users\niran\Downloads\final.docx#_Toc100612887)

[**Figure 3‑4: Use Case Diagram** 16](file:///C:\Users\niran\Downloads\final.docx#_Toc100612888)

[**Figure 3‑5: Sequence Diagram for Manufacturer** 17](file:///C:\Users\niran\Downloads\final.docx#_Toc100612889)

[**Figure 3‑6: Sequence Diagram for User** 18](file:///C:\Users\niran\Downloads\final.docx#_Toc100612890)

[**Figure 5‑1: Register Product** 23](#_Toc100612891)

[**Figure 5‑2: Scanning QR code of Product** 24](#_Toc100612892)

[**Figure 5‑3: Original and sold product status** 25](#_Toc100612893)

[**Figure 5‑4: Local Blockchain** 26](#_Toc100612894)

[**Figure 5‑5: Deployment of Smart Contract** 26](#_Toc100612895)

[**Figure 5‑6: Register product** 27](#_Toc100612896)

[**Figure 5‑7: Calling Smart Contract Function** 27](#_Toc100612897)

LIST OF ABBREVIATIONS

Dapps Decentralized Application

IPFS Inter Planetary File System

DSA Digital Signature Algorithm

ECC Elliptic Curve Cryptography

QR code Quick Response Code

# 1. INTRODUCTION

## 1.1 Background

Lots of fake product of renowned company is found in market. Because of this it causes a lot of renowned company a huge loss and also breaks trust about the product for a customer. Individual customer also gets in loss because they get the fake product not the genuine one. Also, retailer who is selling a genuine product may have to compete with the retailer who is selling a Counterfeiting product. As a result, retailer who is selling a genuine product may result to his/her business loss. In order to resolve these problems, one popular technology that can be used is Blockchain. One of the renowned Blockchain applications is Bitcoin cryptocurrency. Blockchain is simply a chain of blocks connected together with hash value. If any of data gets changed in one block, whole of the block following that block gets wrong. Any application built using Blockchain technology ensures that contents in data are tamper-proof, secured, immutable, decentralized and distributed.

The main goal of our project is to make a decentralized Blockchain system to keep the record of information of manufactured product. At the customer side, we tend to use the QR code scanner to get the information about product and check whether or not the product is genuine or not which indeed help the customer decide to buy the given product or not.

## 1.2 Problem Statement

Many fake products have been generated in existing supply chain in the market. In order to resolve these problems, there must be a system for end user to check details about the product and determine whether to buy the product or not by checking whether the product is genuine or not. In past, the information about the products is stored in centralized manner. So, hacker can attack on just a single system and cause the whole system to fail i.e., cause single point of failure. Due to this single point of failure, we fail to track the information about the products. In some of case, QR code is being used but the information about the product is stored in centralized database which is not so good because bad people can attack such system easily than the decentralized system. So, our main aim is to build the decentralized blockchain system for sharing the information about the product for product anti-counterfeiting. In such a system, it is much difficult for attacker to change information about the products and get their fake products in the market.

## 1.3 Objectives

The objectives of this project are divided into two main and specific objectives and shown below:

### 1.3.1 Main Objective

To design and develop a decentralized Blockchain system for fake product identification using QR code.

### 1.3.2 Specific Objectives

1. To design and develop a web based decentralized application ( Dapps)
2. To publish smart contract instance in the blockchain
3. To generate QR code for a product.

## 1.4 Scopes and Application

These are the fields where this project can be used as listed below:

1. To determine the genuineness of the product in the manufacturing company.
2. To track the product status so that it can be used in data science to increase the sell rate.

# 2. Literature Review

Satoshi Nakamoto [1] explained that a purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. He proposes a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work.

A. Funde [2] described about how IPFS (Inter Planetary File System) which is Distributed Web can be used to manage the ownership of products. IPFS is more useful than http as it can distribute huge volume of data efficiently and IPFS doesn’t allow duplication. IPFS and the Blockchain are similar. You can address large amounts of data with IPFS, and place the immutable, permanent IPFS links into a blockchain transaction. This timestamps and secures your content, without having to put the data itself on the chain.

Product anti-counterfeiting solutions are developed and implemented with centralized system architecture relying on centralized authorities or any form of intermediaries. Vulnerabilities of centralized product anti-counterfeiting solutions could possibly lead to system failure or susceptibility of malicious modifications performed on product records or various potential attacks to the system components by dishonest participant nodes traversing along the supply chain [3].

J. Leng introduces about new decentralized blockchain-driven model, named Makerchain, is presented to handle the cyber-credit of social manufacturing among various makers. An anti-counterfeiting method composed of chemical signature is proposed to represent unique features of personalized products. Twinning unique signature data to blockchain and other functional databases is realized and anticipated to make manufacturing service transactions among makers more trustworthy. Based on an automated execution mechanism of smart contracts among makers, a decentralized manufacturing network can be enabled for automating transactions among makers, as well as third-party verification of product lifecycle through a trail of historic events [4].

Blockchain paradigm when coupled with cryptographically-secured transaction has demonstrated its utility through a number of projects with Bit coin being one of the most notable ones. Ethereum implements this paradigm in generalized manner. Furthermore, it provides a plurality of such resources each with distinct state and operating code but able to interact through a message-passing framework with others [5]. The algorithm that makes Blockchain system secure is hash algorithm.

Current anti-counterfeiting supply chains rely on a centralized authority to combat counterfeit products. This architecture results in issues such as single point processing, storage, and fail-ure. Blockchain technology has emerged to provide a promising solution for such issues. N. Alzahrani [6]proposed the block-supply chain, a new decentralized supply chain that detects counterfeiting attacks using blockchain and Near Field Communication (NFC) technologies. Block-supply chain replaces the centralized supply chain design and utilizes a new proposed consensus protocol that is, unlike existing protocols, fully decentralized and balances between efficiency and security.

Although there has been many related studies focusing on supply chain quality management, the technologies used still have difficulties in resolving problems arising from the lack of trust in supply chains. The root reason lies in three challenges brought to the traditional centralized trust mechanism: self-interests of supply chain members, information asymmetry in production processes, costs and limitations of quality inspections. Si Chen and his team [7] discussed how to improve the supply chain quality management by adopting the blockchain technology, and propose a framework for blockchain-based supply chain quality management.

QR i.e. “Quick Response” code is a 2D matrix code that is designed by keeping two points under consideration, i.e. it must store large amount of data as compared to 1D barcodes and it must be decoded at high speed using any handheld device like phones. QR code provides high data storage capacity, fast scanning, omnidirectional readability, and many other advantages including, error-correction (so that damaged code can also be read successfully) and different type of versions. Different varieties of QR code symbols like logo QR code, encrypted QR code, iQR Code are also available so that user can choose among them according to their need. QR code is applied in different application streams related to marketing, security, academics etc. [8].

Smart contract are self-executing contracts with the terms of agreement between interested parties. The contracts are written in form of program codes that exist across a distributed, decentralized blockchain network. Smart contract allow transaction to be carried out between untrusted parties without the need of central authority. Early work on the smart contract has been done by Szabo and Miller. Blockchain technology represented by bit coin and other crypto currencies is called a blockchain 1.0 which is temper-resistant, decentralization [9]. However, writing a complex logic is not possible due to the limitations of the Bit coin scripting language which has only 256 instructions set. So, bit coin is considered as prototype of smart contracts. Recent blockchain platforms such as Ethereum introduce the idea of running user-defined programs on the blockchain. The codes of Ethereum smart contract are written in stack-based byte code language and executed in Ethereum Virtual Machine. Ethereum is currently the most popular platform for developing smart contracts, so called as Blockchain 2.0. Smart contract is more like an autonomous agents that live inside the EVM, always executing a specific piece of code when called by message or transaction, and having a direct control over their own ether balance. The term transaction is used in Ethereum to refer to signed data package that stores a message to be sent from an externally owned account

The main intent of Ethereum is to create an alternative protocol for building decentralized application. While building such decentralized system, it has two types of account: externally owned accounts, controlled by private keys and contract accounts, controlled their contract code. An externally owned account has no code, and can send messages from an externally owned account by creating and signing a transaction; in contract account, every time the contract account receives a message its code activates, allowing it to read and write to internal storage and send other messages or create contract in turn. Externally owned account address is calculated as:

Externally owned account address = SHA3 (public key)

Also, note that contract address is calculated as:

Contract address = SHA3 (EOA + nonce)

The number of bits outputted by the SHA3 hashing algorithm is of fixed sized 256 bit number. Hash algorithm is one of most important algorithm that plays a significant role in the blockchain network because it helps to maintain the integrity. For example, if you change the only 1 bit of information to input to hash algorithm, then whole hash value becomes totally different than the previous one. Due to this important feature, Blockchain system cannot be tampered with. Since, blockchain is nothing but the decentralized database in the peer to peer to network consisting of chain of blocks. A single block is made of multiple transactions. If any changes is made in past block, the whole forward blocks needs to compute the hash value so as to make the chain valid. Here, way to generate the public and private key in Ethereum blockchain is by using ECC (elliptical curve cryptography) algorithm other than RSA algorithm because key generated using ECC algorithm is much more secure than the key generated by the RSA algorithm. The main intent of public private key cryptography is to make the communication system between two parties much more secure. One of key properties of the public private key cryptography is that one cannot generate the private key given the public key. In other words only public key can be generated from private key but the vice versa is almost impossible for today’s computing system. It is much more like a trap door function that is, given private key you can generate the public key. But once you get the public key, you cannot generate private key. How the encryption and decryption is done is given as:

Encrypted message = Encryption (private\_key, message)

message= Decryption (public\_key, Encrypted message)

Once the message is encrypted using the private key it can only be decrypted using the public key or vice versa. In the most of Blockchain system, this concept of public private key cryptography is used for validation of transaction in the blockchain. In simple way, the concept of digital signature plays a huge role in making blockchain system in storing and transferring of information in system [10].

We have reviewed many journals, research papers, projects books related to fake product identification. From that we have analyzed and draw some new design for solving fake product problem. Most of the Fake product identification system, uses centralized system to store the information of product and which has disadvantages such as single point of failure and one can capture their server and attacker can generate their own product. But blockchain technology has overcome this problem because of the decentralization features and immutability. Our system works on proof of existence algorithm which is implemented using smart contract code. Unlike other system design, we have combined the concept of the blockchain and QR code to be able to register the new manufactured product and store into blockchain and get the QR code according to product information. Attach the QR code into the product. Then at user side, user scans QR code and gets information about product whether the product is original or fake. User can also get information whether product is sold or unsold.

H. Wu explained that Supply Chain Management is fundamental for gaining financial, environmental and social benefits in the supply chain industry. However, traditional SCM mechanisms usually suffer from a wide scope of issues such as lack of information sharing, long delays for data retrieval, and unreliability in product tracing. Recent advances in blockchain technology show great potential to tackle these issues due to its salient features including immutability, transparency, and decentralization [10].

J. Ma explained that any application using Blockchain technology as the base architecture ensures that the contents of its data are tamper-proof. Decentralized Blockchain technology approach to ensure that consumers do not fully rely on the merchants to determine if products are genuine. He described a decentralized Blockchain system with products anti-counterfeiting, in that way manufacturers can use this system to provide genuine products without having to manage direct-operated stores, which can significantly reduce the cost of product quality assurance [11].

# 3. Project Methodology

## 3.1 Block Diagram

Blockchain

Smart contract Instance

Get Information

Scanning the QR code

Product Data

Manufacturer App

**Figure 3‑1: Block Diagram of the System**

From the Block diagram we can see that, at first the manufacturer registers the product using front end of our system by entering the product information. Then our system takes the product information entered by the manufacturer and hashes the information and stores into the blockchain. The business logic is implemented using smart contracts. The QR code is generated according to the information provided by the manufacturer. The user uses the client app to scan the QR code of the product then our system takes the information from the QR code and hashes the information and gets the information about the product from the blockchain according to the information scanned. Before registering or buying the product, he/she needs to select the accounts from the Metamask to perform operation in blockchain.

Technical details related to block diagram are explained below:

* **Blockchain:**

A blockchain is a decentralized, distributed digital ledger that is used to record transactions across peer-to-peer networks so that the record cannot be altered and achieve transparency. Blockchain is formed by a series of blocks. The new block formed is linked to the previous block by cryptographic hashes. One Blocks contains the number of transactions. Each transaction of its hashes. Transaction is created if any node on the network tries to modify the data or perform the operation on the data. After the transaction is completed transaction hash is computed based on the transaction details such as the account sending the transaction, destination, value, data and nonce. Transactions are combined to create a block. Number of transactions that can be stored in a block is computed using the total gas used by all the transaction which must be less than gas limit.

Mnemonics is 12 or 24 length words which helps to derive the sequence of public key, private key and account address. There is two types of address in blockchain, one is contract address and another is Externally owned address. When contract is deployed to the network, deployed address is given to it so that we can send the transaction to that smart contract instance. Each smart contract maintains it’s state. If any operation tries to change state then to complete that transaction one need pay gas fee. Contract address contains smart contract code but EOA doesn’t contain the smart contract code and is able to send transaction and call function of smart contract**.**

There are mainly two types of nodes in the blockchain network. They are

main node and light node.

1. **Main node:**

The main node is the node which has a full copy of the blockchain and performs the mining operations.

1. **Light node:**

Light nodes are those nodes that have a partial copy of blockchain history.

1. **Merkle tree:**

A Merkle tree is a type of binary tree, composed of a set of nodes with a large number of leaf nodes at the bottom of the tree containing the underlying data, a set of intermediate nodes where each node is the hash of its two children, and finally a single root node, also formed from the hash of its two children, representing the "top" of the tree.

1. **Block hash:**

Block Hash is hash value by hashing the block header through SHA256 hashing algorithm. A block header is roughly 200-byte piece of data that contains the timestamp, nonce, previous block hash and the root hash of a data structure called the Merkle tree storing all transactions in the block.

* **Types of Blockchain**

There are mainly two types of block chain they are:

1. Public Blockchain
2. Private (or Managed) Blockchain
3. Consortium Blockchain
4. Hybrid blockchain
5. **Public Blockchain**

In this type of Blockchain there is no central authority, allow anyone to join, and are completely decentralized. For example: Ethereum, Bitcoin, Litecoin.

1. **Private Blockchain**

A private blockchain is managed by a network administrator and participants need consent to join the network. For example: Ripple (XRP) and Hyperledger.

* **Consensus Algorithm**

Consensus is an algorithm that helps to make state of data synchronized shared among peers in network.It's an automated process to ensure that there exists only one single valid copy of record shared by all the nodes. For example, Proof of Work consensus algorithm in bitcoin blockchain, proof of stake in Ethereum blockchain and so on.

* **Smart Contracts**

Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. In our case, Smart contracts are written in solidity programming language. The major function of smart contracts is to implement the business logic.

* **Hashing with SHA-256**

Hash functions transform arbitrary large bit strings called messages, into small, fixed-length bit strings called message digests, such that digests identify the messagesthat produced them with a very high probability. Digests are in that sense fingerprints: a function of the message, simple, yet complex enough that they allow identification of their message, with a very low probability that different messages will share the same digests.

In SHA-256, messages up to 2⁶⁴ bit (2.3 exabytes, or 2.3 billion gigabytes) are transformed into digests of size 256 bits (32 bytes). For perspective, this means that an object 7 times the size of Facebook’s data warehouse in 2014 passed to SHA-256 would produce a chunk of data the size of a 32-letter string of ASCII characters, and that string would the object’s very special fingerprint.

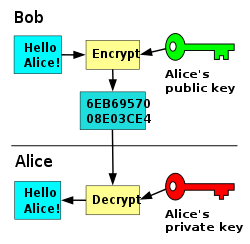
### 

* **IPFS**

A peer-to-peer hypermedia protocol designed to preserve and grow humanity’s knowledge by making the web upgradeable, resilient, and more open. The Interplanetary File System (IPFS) is a protocol and peer-to-peer network for storing and sharing data in a distributed file system. IPFS uses content-addressing to uniquely identify each file in a global namespace connecting all computing devices.

* **Public key cryptography**

Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys. Each pair consists of a public key (which may be known to others) and a private key (which may not be known by anyone except the owner). The generation of such key pairs depends on cryptographic algorithms which are based on mathematical problems termed one-way functions. Effective security requires keeping the private key private; the public key can be openly distributed without compromising security.



**Figure 3‑2: Public Key Cryptography** [16]

In such a system, any person can encrypt a message using the intended receiver's public key, but that encrypted message can only be decrypted with the receiver's private key. This allows, for instance, a server program to generate a cryptographic key intended for a suitable symmetric-key cryptography, then to use a client's openly-shared public key to encrypt that newly generated symmetric key. The server can then send this encrypted symmetric key over an insecure channel to the client; only the client can decrypt it using the client's private key (which pairs with the public key used by the server to encrypt the message). With the client and server both having the same symmetric key, they can safely use symmetric key encryption (likely much faster) to communicate over otherwise-insecure channels. This scheme has the advantage of not having to manually pre-share symmetric keys (a fundamentally difficult problem) while gaining the higher data throughput advantage of symmetric-key cryptography.

With public-key cryptography, robust authentication is also possible. A sender can combine a message with a private key to create a short digital signature on the message. Anyone with the sender's corresponding public key can combine that message with a claimed digital signature; if the signature matches the message, the origin of the message is verified (i.e., it must have been made by the owner of the corresponding private key).

* **JSON-RPC**

JSON-RPC is a remote procedure call protocol encoded in JSON. It is similar to the XML-RPC protocol, defining only a few data types and commands. JSON-RPC allows for notifications (data sent to the server that does not require a response) and for multiple calls to be sent to the server which may be answered asynchronously. JSON-RPC is simply a remote procedure call protocol that is used on Ethereum to define different data structures. It also defines the rules on how data structures are processed in the network. Because it is transport-agnostic, you can use it to interact with an ETH node over sockets or HTTP. If you are already well-versed on this topic and are already using your JSON and JSON-RPC knowledge to hook up to APIs or create your specifications to interact with Ethereum nodes and build on the Ethereum blockchain, you should look up Moralis for the exciting possibility of speeding up the process, skipping the clunky initiation phases and building serverless dApps seamlessly.

## 3.2 Flow chart

## 

Changes

Changes

Store to Block chain

Product Status?

Product Status?

Fake

Fake

Real

Real

Yes

Yes

No

No

Buy?

Buy?

Get Manufactured Product Data

Get Manufactured Product Data

Scan QR code

**Figure 3‑3: Flow chart of system**

Manufacturer stores the data to blockchain system. Then user can get the information about the product by scanning the QR code attached to product. User can observe the status of the product on web app. Status of product show information whether the product is original or fake. After scanning the QR code, frontend call function inside smart contract which don’t change the state of blockchain so it doesn’t require the gas fee and shows the result to frontend. When user buy the product, then frontend sends transaction to the smart contract instance and changes the state of the blockchain according to the information sent by scanning QR Code. So, status of product is show whether it is fake or Original.

## 3.3 UML diagram

### 3.3.1 Use Case diagram

Scan QR

Blockchain

Product Information

Buy

<<include>>

<<extend>>

<<include>>

User

Manufacturer

**Figure 3‑4: Use Case Diagram**

Our fake product identification system involves buyer(user) and manufacturer. Manufacturer register the product information in blockchain system. Blockchain contains our smart contract instance which have persistence data storage. Any User or Buyer can scan QR code and can decide whether to buy the information or not. Our system sends the scanned data to blockchain system to get information about the product. Our blockchain system don’t store product information directly instead it stores the hash of that information so that outsider don’t know the original information.

### 3.3.2 Sequence Diagram

Metamask

Frontend

Smart contract

Select Account

Enter Data

Request to Blockchain

Successfully saved to Blockchain

Select valid account

[If Valid account]

[Else]

**Alternative**

**Figure 3‑5: Sequence Diagram for Manufacturer**

Manufacturer first select account to register product. He/she add data about the product in the blockchainsystem. The blockchain system checks whether product information is sent from a valid account or not. If the product information is sent from a valid account, then product information is saved to the blockchain. If that’s not the case, the blockchain will just reject the transaction and don’t store it in the blockchain.

Manufacturer first select account to register product. He/she add data about the product in the blockchainsystem. The blockchain system checks whether product information is sent from a valid account or not. If the product information is sent from a valid account, then product information is saved to the blockchain. If that’s not the case, the blockchain will just reject the transaction and don’t store it in the blockchain.

Metamask

Frontend

Smart contract

Select Account

Scan QR code

Call Function

Product Information

Send Transaction

Buy

Status

**Figure 3‑6: Sequence Diagram for User**

Customer scans QR code and scanned data is sent to the blockchain to get details about the product. By observing the details, users can send buy requests to buy products. Then front end sends a transaction to the blockchain to update the status of a product.

# 4. Hardware and Software requirements

## Hardware Requirements

Following are the hardware components required for this project:

* + A computer with internet connection
  + Mobile Device with Camera with internet connection

## Software Requirement

1. **Ethereum**

Ethereum is a decentralized, open source blockchain with smart contract functionality. Ethereum is the community-run technology powering the cryptocurrency ether (ETH) and thousands of decentralized applications. Ethereum is open access to digital money and data-friendly services for everyone no matter your background or location. It’s a community-built technology behind the cryptocurrency ether (ETH) and thousands of applications you can use today.

1. **Solidity**

Solidity is an object-oriented, high-level language for implementing smart contracts. Smart contracts are programs which govern the behavior of accounts within the Ethereum state. Solidity is a curly-bracket language. It is influenced by C++, Python and JavaScript, and is designed to target the Ethereum Virtual Machine (EVM). Solidity is statically typed, supports inheritance, libraries and complex user-defined types among other features. With Solidity you can create contracts for uses such as voting, crowdfunding, blind auctions, and multi-signature wallets.

1. **HTML**

HTML (Hyper Text Markup Language) is the most basic building block of the Web. It defines the meaning and structure of web content. Other technologies besides HTML are generally used to describe a web page’s appearance/presentation (CSS) or functionality/behavior (JavaScript). “Hypertext” refers to links that connect web pages to one another, either within a single website or between websites. Links are a fundamental aspect of the Web. By uploading content to the Internet and linking it to pages created by other people, you become an active participant in the World Wide Web. HTML uses “markup” to annotate text, images, and other content for display in a Web browser. HTML markup includes special “elements such as <head>, <title>, <body>, <header>, <footer>, <article>, <section>, <p>, <div>, <span>, <img>, <aside>, <audio>, <canvas>, <datalist>, <details>, <embed>, <nav>, <output>, <progress>, <video>, <ul>, <ol>, <li> and many others.

1. **CSS**

CSS is the language we use to style an HTML document. CSS describes how HTML elements should be displayed. CSS stands for Cascading Style Sheets. CSS describes how HTML elements are to be displayed on screen, paper, or in other media. CSS saves a lot of work. It can control the layout of multiple web pages all at once. External stylesheets are stored in CSS files.

1. **GIT**

Git is a free and open-source distributed version control system designed to handle everything from small to very large projects with speed and efficiency. Git is easy to learn and has a tiny footprint with lightning-fast performance. It outclasses SCM tools like Subversion, CVS, Perforce, and ClearCase with features like cheap local branching, convenient staging areas, and multiple workflows.

1. **JavaScript**

JavaScript is a high-level, often just-in-time compiled language that conforms to the ECMAScript standard. It has dynamic typing, prototype-based object-orientation, and first-class functions. It is multi-paradigm supporting event-driven, functional, and imperative programming styles. JavaScript is the world’s most popular programming language. JavaScript is the programming language of the Web.

1. **Reactjs**

React (also known as React.js or ReactJS) is a free and open-source front-end JavaScript libraryfor building user interfaces based on UI components. It is maintained by Meta (formerly Facebook) and a community of individual developers and companies. React can be used as a base in the development of single-page, mobile, or server-rendered applications with frameworks like Next.js. However, React is only concerned with state management and rendering that state to the DOM, so creating React applications usually requires the use of additional libraries for routing, as well as certain client-side functionality. React makes it painless to create interactive UIs. Design simple views for each state in your application, and React will efficiently update and render just the right components when your data changes.

1. **Web3.js**

Web3.js is a collection of libraries that allow you to interact with a local or remote Ethereum node using HTTP, IPC or WebSocket. The following documentation will guide you through [installing and running web3.js](https://web3js.readthedocs.io/en/v1.7.1/getting-started.html#adding-web3) as well as providing an API reference documentation with examples.

1. **Metamask**

Metamask is a crypto wallet and gateway to blockchain apps. It is available as a browser extension and as a mobile app, Metamask equips you with a key vault, secure login, token wallet, and token exchange everything you need to manage your digital assets. Metamask provides the simplest yet most secure way to connect to blockchain-based applications. You are always in control when interacting on the new decentralized web. Metamask generates passwords and keys on your device, so only you have access to your accounts and data. You always choose what to share and what to keep private.

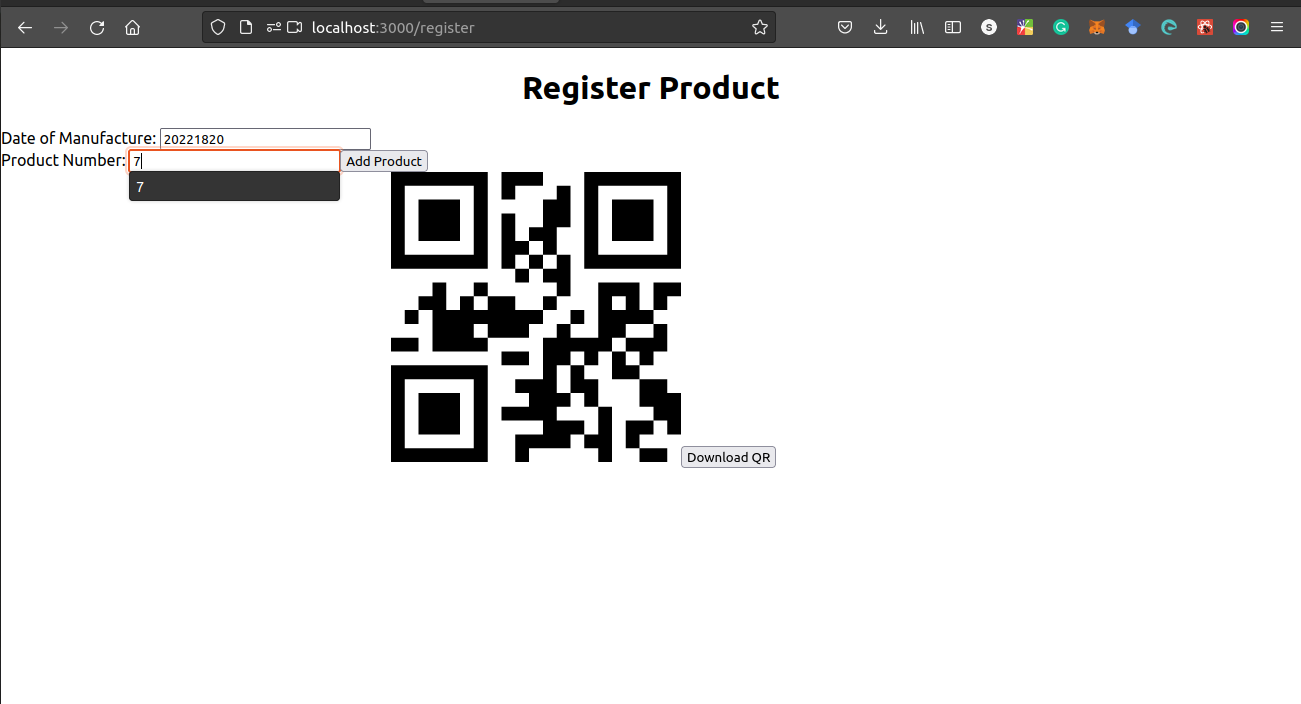
1. **Hardhat**

Hardhat is a development environment to compile, deploy, test, and debug your Ethereum software. It helps developers manage and automate the recurring tasks that are inherent to the process of building smart contracts and dApps, as well as easily introducing more functionality around this workflow. This means compiling, running and testing smart contracts at the very core. Hardhat comes built-in with Hardhat Network, a local Ethereum network designed for development. Its functionality focuses around Solidity debugging, featuring stack traces, console.log () and explicit error messages when transactions fail.

# Results and Discussion

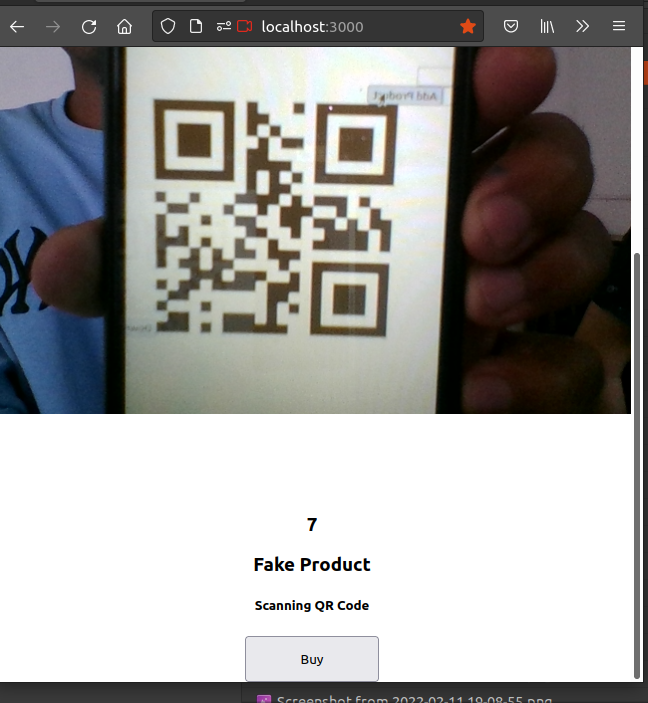
## 5.1 Results

* **Generation of QR code for a product using Web based decentralized application (Dapps)**

****

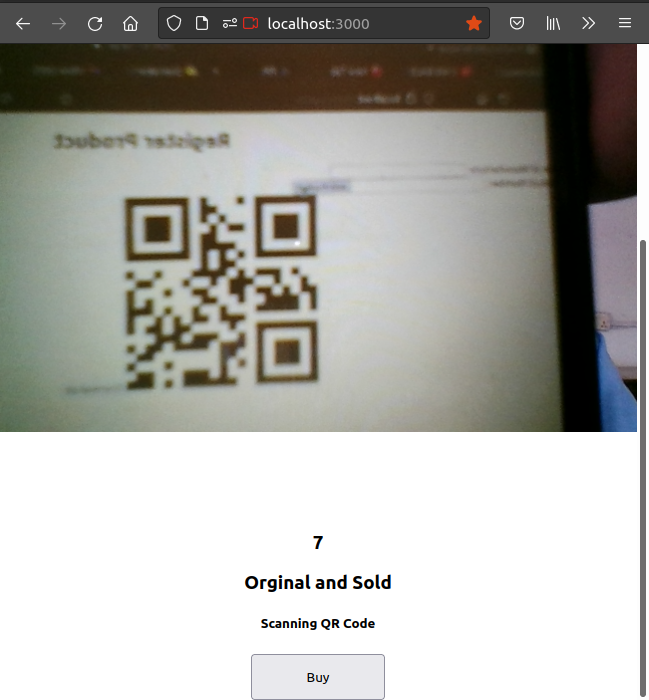
**Figure 5‑1: Register Product**

With the help of frontend part of manufacturer, manufacturer was able register the product with the product information. After product was added to blockchain, manufacturer was able generate and download the QR code given the product information. Manufacture can now able to attach the QR code.



**Figure 5‑2: Scanning QR code of Product**

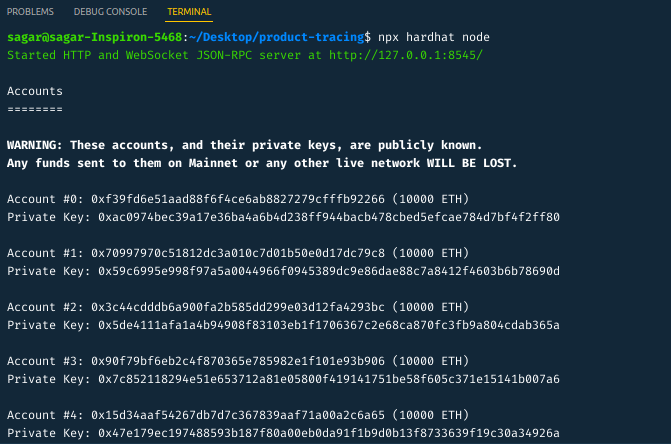
Consumer got information whether the product is real or fake by scanning QR code. After the product was added to blockchain, consumer could get information about the product whether the product is fake or not.

****

**Figure 5‑3: Original and sold product status**

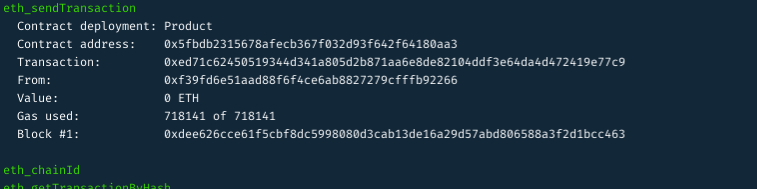
From consumer side, we have the separate frontend for consumer. There is scan button, consumer can scan QR code and get the information.

* **Publishment of smart contract instance in the blockchain that identify fake product**

****

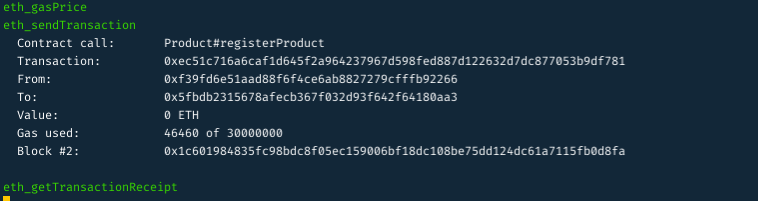
**Figure 5‑4: Local Blockchain**

Deployment of local blockchain has been done successfully using hardhat.

****

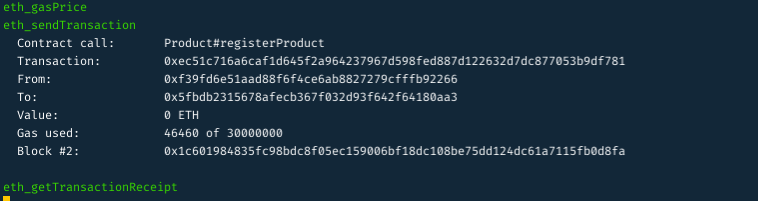
**Figure 5‑5: Deployment of Smart Contract**

Smart contract instance to the local blockchain containing 20 nodes have been deployed successful.

****

**Figure 5‑6: Register product**

Storing of information about product in blockchain have been done successfully.



**Figure 5‑7: Calling Smart Contract Function**

Call to smart contract function through web3 API and displayed the result to user has been done.

## **5.2 Discussion**

Using the blockchain system, business logic for storing the information about the product has been done successfully with the feature to determine the fakeness of the product. The whole business logic is implemented using smart contracts written in the solidity programming language. While implementing business logic using smart contracts, openzeppelin libraries help to write secure smart contracts so that it helps to reduce the loophole in the smart contracts. Fake product identification without blockchain has a few problems such as a single point of failure that means if the server gets hacked or fails to work then the whole system used to identify the fakeness becomes collapsed.

There are different ways to detect the copying of QR codes. One way to achieve this is to insert a copy-sensitive digital image at the center of the QR Code (called copy detection pattern or secure graphic). The secure graphic will naturally degrade and lose information if a counterfeiter tries to copy it, due to uncontrollable effects of dot gain and ink smearing. A good example of how this is done can be seen with the Scantrust secure QR Code. But these systems have one demerit, one can attack their system and get their data to their server and add their product to the market. A blockchain system with QR codes will help to achieve this because of the feature of decentralization no one can change the data that has already been added to the blockchain which is also called immutability. As blockchain has feature called transparency i.e., anyone can see what’s in blockchain. That means anyone can see data that has been stored to blockchain. Since our product information needs be secured on the blockchain so that counterfeiter cannot get data and generate the QR code accordingly. To resolve this problem, hashing algorithm helps to secure the product information. In our blockchain system, we use proof of existence concept to determine fakeness of the product.

This project is much more similar to findings of N. C. Yiu who studied the supply chain management and store information about the product according state of product wheather it is in production state or shiping state or retailer state or any other state depending upon type of bussiness model. But this project doesn’t implement concept o of supply chain. It only takes the information about product such as product number and stores hash of product number to the blockchain.

This project is a bit similar to finding of Jiewn Leng who implemented the chemical signature to represent unique features of product. But this project implemented the QRcode to contains the hash of information of the product data and stored in the blockchain.

# Conclusion

After the completion of this project, Dapp for identifying fakeness of the product has been developed which works on understanding blockchain infrastructure. Deployment of smart contract instance has done successfully on local blockchain called hardhat network. Recording of product information only by the valid manufacturer has been done. Scanning of the QR code by user to get information has been completed. Also, consensus algorithm called proof of existence algorithm has been using solidity programming has been implemented successfully.

# Limitation and Future Enhancement

## Limitations:

* The user needs to have a QR code scanner in order to check the product information.
* Active Internet connection is required.
* One smart contract instance needs to be deployed for every different company.

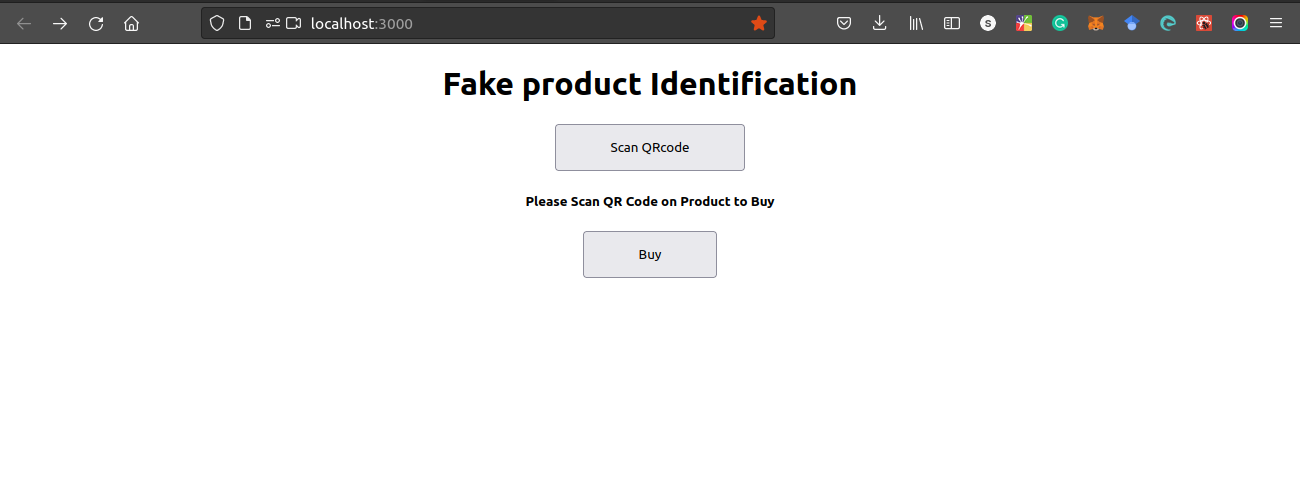
## Future Enhancement:

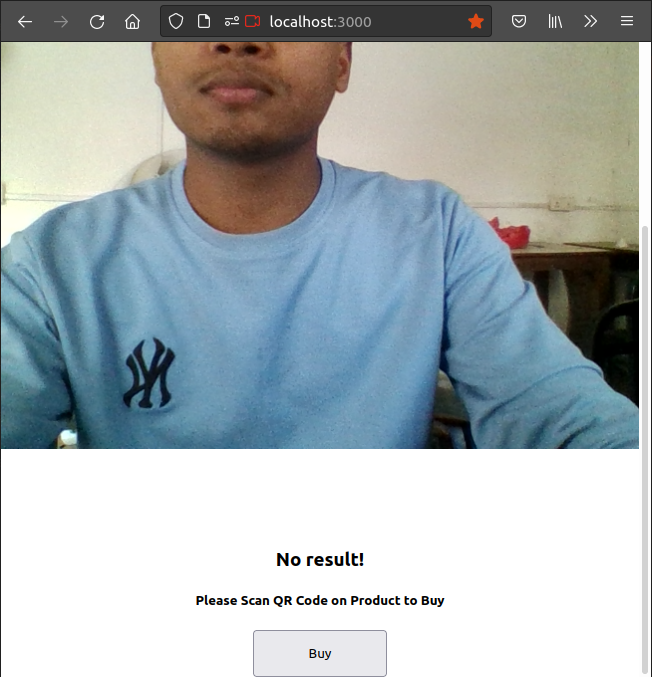
* Virtual Transactions.
* To implement the ownership concept.
* Implement our own tokens which can be sold to users so that they can purchase ownership of a product using tokens.

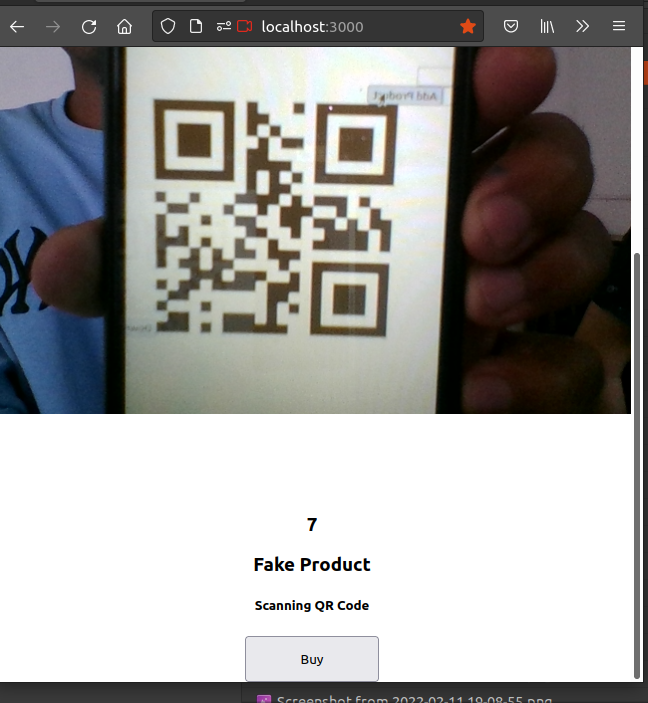
# References

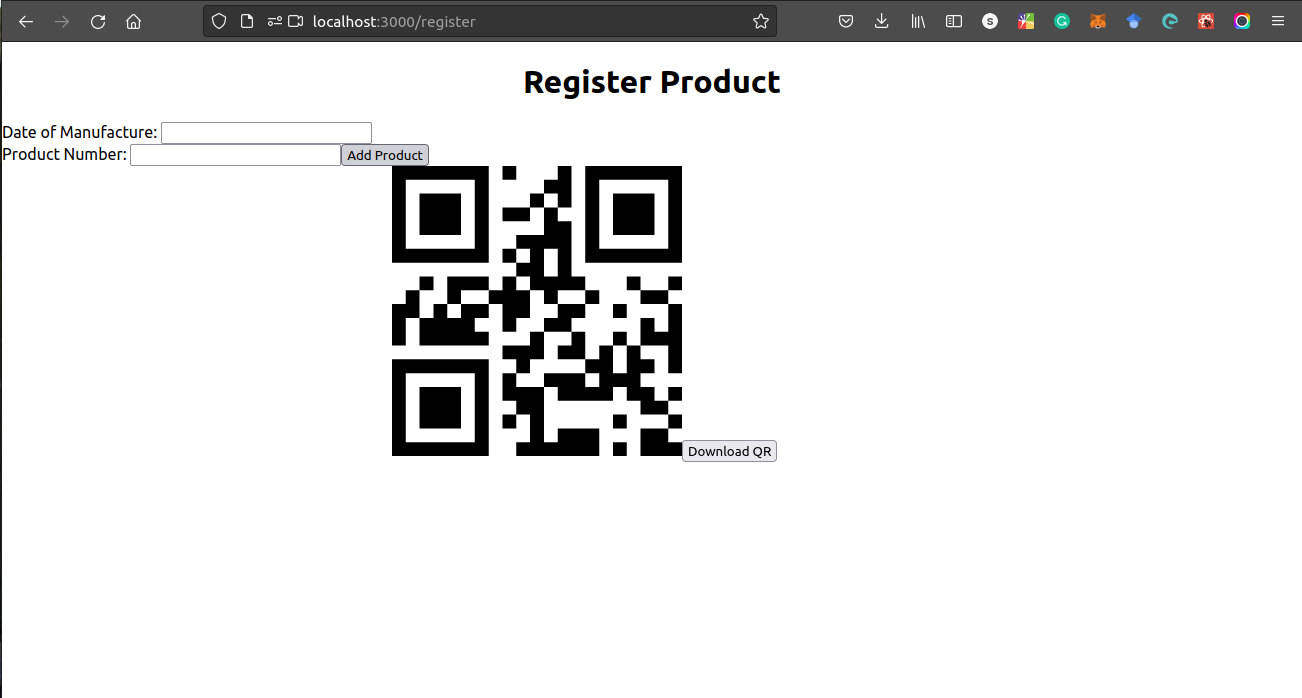
|  |  |
| --- | --- |
| [1] | S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. |
| [2] | P. N. A. K. N. M. M. N. N. A. Funde, "Blockchain Based Fake Product Identification in Supply Chain," in *International Research Journal of Engineering and Technology*, Maharashtra, India, 2019. |
| [3] | N. C. Yiu, "Toward Blockchain-Enabled Supply Chain Anti-Counterfeiting and Traceability," in *IEEE*, 2021. |
| [4] | P. J. Q. L. R. S. J. Leng, " |
| [5] | D. G. WOOD, "ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER," 2021. |
| [6] | A. A. Kamat, "Using QR codes to track and identify counterfeit products". |
| [7] | R. S. Z. R. J. Y. Y. S. J. Z. Si Chen, "A Blockchain-based Supply Chain Quality Management Framework," 2017. |
| [8] | S. Tiwari, "An Introduction To QR Code Technology," in *International Conference on Information Technology*, 2016. |
| [9] | Y. Y. X. W. S. Wang, "An Overview of Smart Contract: Architecture, Applications, and Future Trends," Suzhou, China, 2018. |
| [10] | J. C. Y. Y. C. L. T. S. J. H. Wu, "Data Management in Supply Chain Using Blockchain: Challenges and a Case Study". |
| [11] | S. L. X. C. H. S. J. Ma, "A Blockchain-Based Application System for A -Blockchain-Based Application System for," *IEEE.* |
| [12] | B. Ramamurthy, "Blockchain Specialization," [Online]. Available: https://www.coursera.org/specializations/blockchain. |
| [13] | "web3.js," [Online]. Available: https://web3js.readthedocs.io/en/v1.7.1/. |
| [14] | "Solidity," [Online]. Available: https://docs.soliditylang.org/en/v0.8.13/. |
| [15] | "hardhat," [Online]. Available: https://hardhat.org/. |
| [16] | "Public-key cryptography," [Online]. Available: https://en.wikipedia.org/wiki/Public-key\_cryptography. |

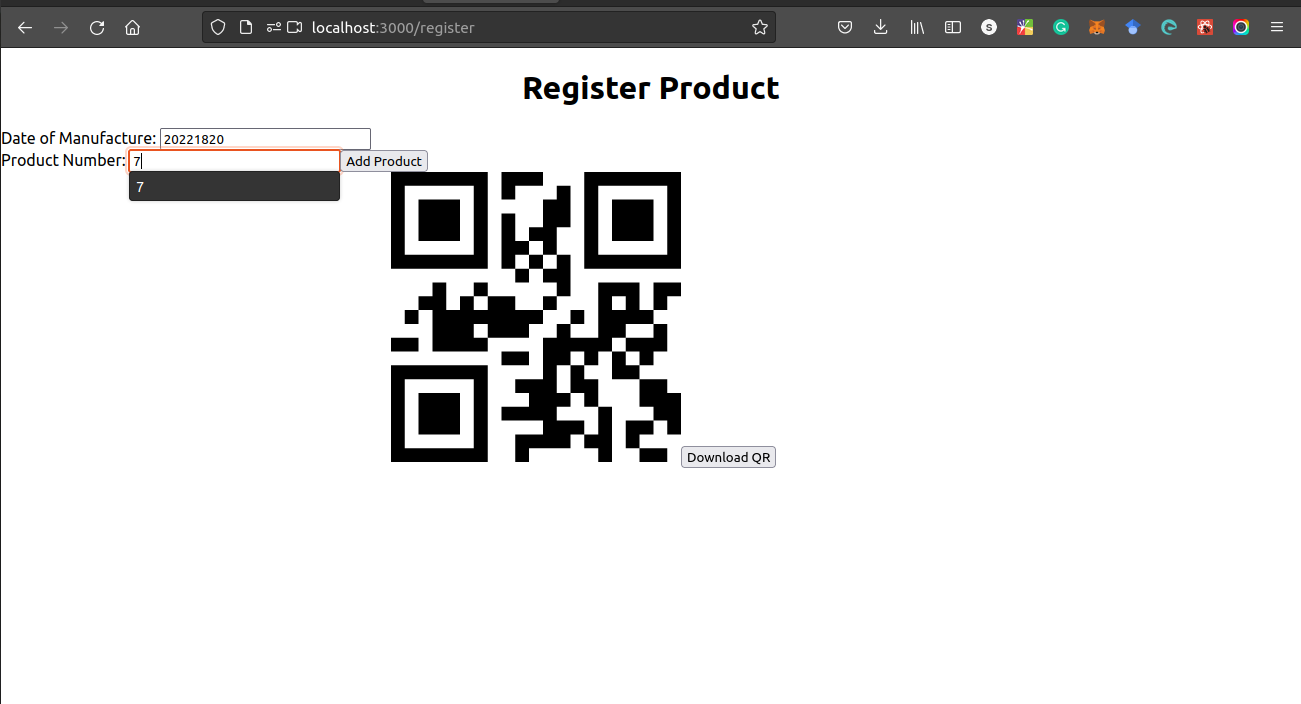
# Appendices

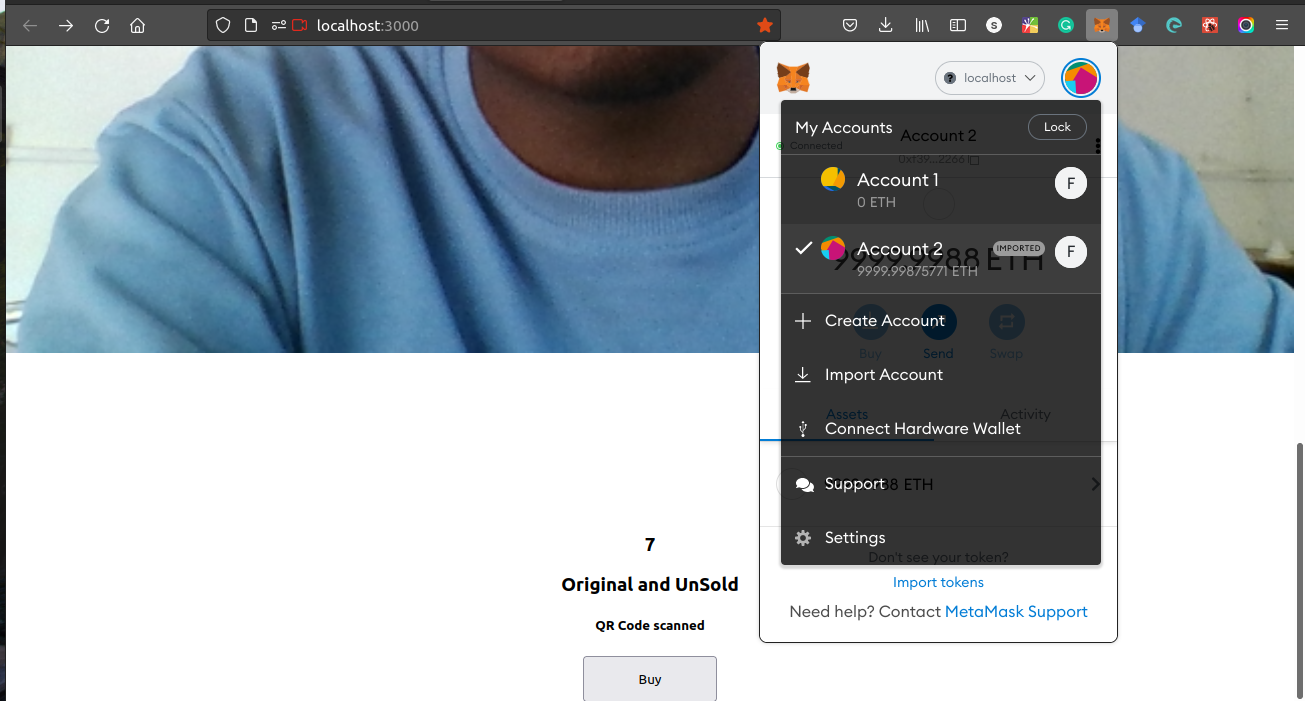
****

****

****

****

****

****



e