FMDB *Transactions on Sustainable Technoprise Letters*

Developing Blockchain Technology to Identify Counterfeit Items Enhances the Supply Chain's Effectiveness

Maruf Farhan[1,*], Rejwan Bin Sulaiman[2]

[1,2]Department of Computer Science and Engineering, Northumbria University, London, United Kingdom.
marufrigan9@gmail.com[1], rejwan.sulaiman@northumbria.ac.uk[2]

Abstract: Fake products have become a common term in business, especially in the consumer market. Due to the fake products, companies are going through a lot of financial losses, hampering the brand name, and at the end of the day, every day, they are losing customers. Product counterfeiting is rampant in the modern economy, and it is difficult to detect whether the product is genuine or fake by simply looking at it. In Bangladesh, the market is full of fake products, making it difficult for local customers to detect them. Because of those counterfeit products, legitimate companies are facing issues. Several historical solutions have been developed to overcome the issue of product counterfeiting. Among the most widely used approaches are RFID tags, AI, QR code-based systems, etc. However, the mentioned system has some drawbacks. For example, a QR code can be copied from a genuine product and put into a fake product. The objective of the project is to enhance the identification of counterfeit items. Utilizing blockchain technology facilitates this capability, enabling the distinct identification of products and subsequent monitoring across the whole supply chain. The use of distributed ledger technology, commonly known as Blockchain, enables multiple people to access and see the data concurrently. One of the primary advantages of the system is its robustness against unauthorized modifications to the recorded data, necessitating the consensus of all relevant parties. This attribute enhances the security of the data, shielding it from potential weaknesses. This study presents a novel approach to detecting counterfeit products using blockchain technology.

Keywords: Developing Blockchain Technology; Identify Counterfeit Items; Supply Chain's Effectiveness; Potential Weaknesses; Counterfeit Products; Fake Products; Losing Customers; National Consumers' Rights; Decentralized Application System.

Received on: 05/01/2023, **Revised on:** 15/04/2023, **Accepted on:** 07/07/2023, **Published on:** 17/12/2023

Cite as: M. Farhan and R. Bin Sulaiman, "Developing Blockchain Technology to Identify Counterfeit Items Enhances the Supply Chain's Effectiveness," *FMDB Transactions on Sustainable Technoprise Letters*, vol. 1, no. 3, pp. 123–134, 2023.

1. Introduction

Each day brings more technological progress. Today's company market is competitive, and everyone strives to give customers the best options. Some people sell unlicensed things to get rich quickly. The Organisation for Economic Co-operation and Development (OECD) and the European Union Intellectual Property Office (2019) define counterfeit goods as products that copy the appearance of genuine goods without permission [1]. Recent years have seen a boom in counterfeit goods, and the spectrum of products in danger has grown. With almost half of US Customs and Border Protection's counterfeit items being clothes and accessories, copyright violations have increased. While international trade has remained flat, counterfeit goods have grown to 3.3% [1]. Over the past decade, counterfeit products have flooded Bangladesh's market. The National Consumers' Rights Protection Directorate identified counterfeit powdered milk and cosmetics in large stores in Banani, Gulshan, and other affluent areas during enforcement operations [2]. During the raid, officers found that several facilities were making counterfeit consumer products without MRP, importer names, or addresses. Even during the COVID-19 pandemic, dishonest businessmen

[*] Corresponding author.

created fake masks, gloves, and sanitisers. A group of dishonest merchants has started selling phoney and low-quality goods during the coronavirus crisis. Famous national and international brands are being forged alarmingly. This includes food, medicine, and life-saving items.

Blockchain technology is a popular topic among intellectuals. Blockchain has emerged in the supply chain, pharmaceutical, and health sectors. No third-party participation is a benefit of decentralized blockchain design. Blockchain has several advantages and can be used in industries where manufacturers can create blockchain-based QR codes, and customers can obtain real products. Manufacturers can transfer product ownership to sellers using blockchain technology, and buyers can verify product legitimacy before buying. Blockchain technology secures digital asset ownership certificates and preserves their physical properties. Blockchain makes it difficult for an attacker to edit, change, or replicate this data. Considering these prospects, a system architecture is developed that uses blockchain technology to protect product ownership and lets customers pick between counterfeit and authentic Ethereum smart contract products. This technology lets users scan products using blockchain-based QR codes to verify authenticity, and it reduces manufacturing costs.

2. Problem statement

This problem is getting worse because the value of the offering is being questioned. The product's value is determined by its physical characteristics and marketability and effectiveness in the world of technology. Our objective is to help preserve product authenticity by storing the serial number of the product and generating a blockchain-based QR code that will act as a single point of product authentication among the customer. The customer will have the ability to verify the product information, such as supplier code, manufacturer ID, and product ID.

Objective:

- Critical literature review on the use of Blockchain technology to detect fake products in the context of Bangladesh.
- Proposed framework based on the analysis of the critical literature review.
- This paper aims to assess the efficacy of the framework in ensuring product authentication in the market and help to develop and establish customer trust in the Bangladesh market.

3. Literature Review

Numerous organizations and businesses have invested considerably in technologies and resources to prevent consumers from purchasing counterfeit items [11]. For the last forty years, the world has experienced numerous technological developments, creating innumerable solutions that help track and detect counterfeit products [5]. RFID is one of the earliest developed tools for monitoring supply chain systems [4]; [19].

Recently, the development of blockchain technology has led to the creation of methods for identifying counterfeit products. The adoption of such technology is being used by many renowned brands such as Prada, Cartier, and Louis Vuitton [8]. Apart from that, many pharmaceutical industries are also adopting this technology to fight counterfeit drugs. For example, to ensure that pharmaceutical products are genuine, Zuellig Pharma created eZTracker [14].

A large number of blockchain-based applications have been developed. Few applications focused on payment systems [2] and the securities market (TzeRO). On the other hand, some researchers are focusing on integrating blockchain technology with IoT for purposes including documenting IoT device data for example, gaming [7], Gambling (Augur) online voting (Agora), Recently few researchers are implementing blockchain technology to detect fake news [20] fake profile and fake reviews [6].

Kalpana Devi et al., [9] Introduces a distributed Blockchain-based system to combat product forgeries by empowering consumers to confirm the legitimacy of products without relying on vendors. By eliminating the intermediary, this suggested strategy would save manufacturers money on quality control for their products in the retail sector. Using a distributed ledger technology (Blockchain) to record and share information about products allows for clear accounting of seller earnings and available stock. The solution employs digital signatures for identity verification and provides vendor-side verification. The article stresses the value of keeping code as simple as possible to optimize an Ethereum-based app's use of resources and keep costs down. The research does present a workable anti-product forgery technique, although it does have some restrictions. It doesn't go into sufficient depth concerning the inner workings of the Blockchain system or its technical implementation. The paper does not address concerns about security and scalability, which may emerge when the proposed technique is implemented on a larger scale. More work must be done to overcome these obstacles to improve the system's security and scalability.

The study by Mallegowda et al. [12] presents convincing arguments in favour of employing blockchain technology and QR codes to prevent the production of counterfeit goods. However, it seems to gloss over certain limitations and potential difficulties. For instance, the authors barely touch upon the potential vulnerabilities of blockchain technology and QR codes. While Blockchain is extremely secure, it is still vulnerable to attacks, and QR codes can be easily duplicated or altered. The study also ignores the potential resistance to Blockchain among producers and consumers. The learning process and the necessary technological infrastructure may make widespread adoption challenging. There is also no discussion of scalability in the text. The verification procedure may take longer if the Blockchain grows too large and cumbersome due to an increase in the volume of products and transactions. Finally, the report does not address the issue of confidentiality. While transparency is crucial to the success of Blockchain, it has the potential to raise security concerns among users and business owners alike. In this study, researchers focused on

Musale. et al. [13] proposed an approach where proposed QR codes and blockchain technology to fight against counterfeit products. The study's main objective is to promote transparency, decrease piracy and track products at every stage of production and shipment. Nonetheless, there are several drawbacks to the study. It does not address potential data security problems related to using a MySQL database for storing user login information and assumes that users have a high degree of technological literacy. MySQL databases may be vulnerable to SQL injection attacks, which can compromise user data and system integrity, as reported in a scholarly study by Halfond and Orso (2005). However, the author's aspiration to apply the system to other industries, such as banking and healthcare, ignores the sector's distinct difficulties and regulatory needs. Finally, evaluating the feasibility of the suggested system is complicated by a lack of evidence to support the study's claims. These concerns should be addressed in further studies so that more evidence of the system's potential impact may be provided.

Kumar and Tripathy [10] proposed an approach based on a private blockchain technique where the certificate authority will issue digital signatures to the regulatory body, and with the help of QR technology, they will be able to identify the traceability of medicine from manufacturer to end user and detect counterfeit drugs. Here, the authors tried to focus on the supply chain of medicine, where tracking each supply chain step at the individual drug level can be monitored and identified. They used PKI and digital signatures in their proposed framework, which offers protection against replay and MiTM attacks. Their proposed framework needed to provide concrete, practical workflow or suggest whether they can implement this in the consumer goods sector.

In another study, Mallegowda et al., [21] used blockchain technology with the help of QR technology to detect counterfeit products. When the product's QR code is connected to the Blockchain, fake goods can be found using that QR scan. Thus, this system may need to store database blocks for the unique code and product information. After asking for it, it compares the user's unique code to blockchain database entries. If the code matches, the consumer will see complete product information. Otherwise, no evidence of the product's authenticity would be shown. The author showed the product's history in this study, but verification needs to be done directly. In the study, the author should have suggested what categories should be included in the project to check the authentication. In the proposed research, product categories and markets were not identified.

Anjum and Dutta [3] introduced the DApp (Decentralized application system), which is built on the Ethereum blockchain. Here, the authors tried to focus on the ownership of the products and proposed a system where every good on the Blockchain will have its own unique QR code, which consumers can use to authenticate the product's provenance and ownership by simply scanning the code. The study also indicated that it may be extended to retail and e-commerce websites, thereby expanding access for all customers. While RFID has been utilized in the past, it suffers from security and privacy flaws that may be efficiently addressed by implementing blockchain technology. In this case, the retailer is responsible for paying a registration fee to the producer. Then, the vendor may proceed with the purchase and inventory tracking. The option to "transfer ownership" had also been implemented. In their study, they did not mention any product category, and the researcher did not mention the market.

Another research conducted by Singh and Shandilya [16] proposed a combined approach where it’s easy to maintain the cost of product quality and track the authenticity of the product from origin to end user. The author used the combined approach of DBT (Decentralized blockchain technology) and supply chain and using a One-time password on the recipient's phone and deploying quality assurance specialists are two methods for ensuring the authenticity of products along the supply chain. In the proposed approach, researchers focused on Liquor, drugs and agricultural items but not on consumer goods. In the paper, the researchers focused on the European market. However, researchers focused on using OTP to verify the authentication system is not sufficient. That's why. In our study, we opted to employ QR codes instead of OTP. According to a recent study (MBCS,2023), OTP can be bypassed easily by the attacker, and as a result, they might use it to create fake products.

Ma et al. [11] suggested that customers should not trust the stores to check the authenticity of their products. If manufacturers use decentralized blockchain systems to provide genuine products without running their physical stores, it will help them reduce production costs and maintain product quality. In this study, the authors did not focus on any product category. The authors in this paper included basic facts regarding Ethereum and Bitcoin, such as the gas cost and limit. Technology has the potential to efficiently reduce the minimum requirement of authentic items and enable firms with constrained financial resources. One of the key benefits of this method is that it offers a reliable way to verify the legitimacy of purchased items, which can significantly boost buyer trust and confidence. By using this method, buyers can rest assured that they are getting exactly what they paid for and not falling victim to counterfeit products. However, the code used in this method may benefit from simplification and redundancy reduction, making the process even more efficient and streamlined.

Toyoda. et al. [18] proposed a system known as POMS (Product Ownership Management System), where counterfeiters cannot verify the existence of products, so they attempt to replicate them. Buyers can refuse counterfeit products without ownership, even if the seller provides a valid product code. This method can identify several counterfeit products, but this approach needs to be more robust against duplicate tags. After an attacker has made a copy of the RFID tags connected to the genuine product, they will inject the counterfeit version of the label into the distribution chain. This is why we advocated using QR codes in our study, which will be linked to blockchain technology to identify counterfeit goods. The suggested system also cannot verify that a buyer receives genuine goods from a legitimate vendor. Hence, the issue of product counterfeiting remains unresolved.

Sivaganesan et al. [17] proposed a secure mechanism to help distribute medicine in the supply chain. It employs a request-response event model to verify and monitor medicine distribution. In their proposed mechanism, smart contracts store all the transactions on the Blockchain and let things be tracked back to their original manufacturers. In this study, researchers used DApp, which is connected to Blockchain. The study aimed to enhance security and create openness for the pharmaceutical industry to avoid counterfeit products. In this study, the author did not specify whether this method should be implemented in any other sector.

Saxena. et al. [15] proposed an application tool based on the Ethereum blockchain, created with AWS, that can record and time stamp the transfer of goods at every point in the pharmaceutical supply chain. All these processes will be noted and time-stamped by scanning the bar code. To propose the solution, researchers interviewed 30 people involved in the pharmaceutical industry, and most of them agreed with the counterfeit drugs. However, there are many issues and restrictions with the present approaches. The researcher also mentioned that implementing this technology is going to be costly and needs to work on the scalability issues. This study completely focused on the pharmaceutical industry, and the author did not inform whether it can be used in another sector.

4. Proposed Framework

This framework uses Blockchain to detect counterfeit products. Blockchain requires manufacturers to register before selling authentic products. Manufacturers will then contribute product details to the Blockchain. A new smart contract will manage product data in the Blockchain and maintain the authority to add every detail. When added to the network, the product creates the cryptographic hashing technique needed to generate the QR code. The QR code will be checked for validity later. The manufacturer might check seller queries. After manufacturing the product QR, they will add seller information where they wish to sell it. The seller will add product information for sale. The vendor puts customer codes in the selling list so they may verify who bought the merchandise. This area offers two consumer alternatives. Customer purchase history and product verification. Customers can enter their code and check their purchase history in one section and their code in another (Figure 1).

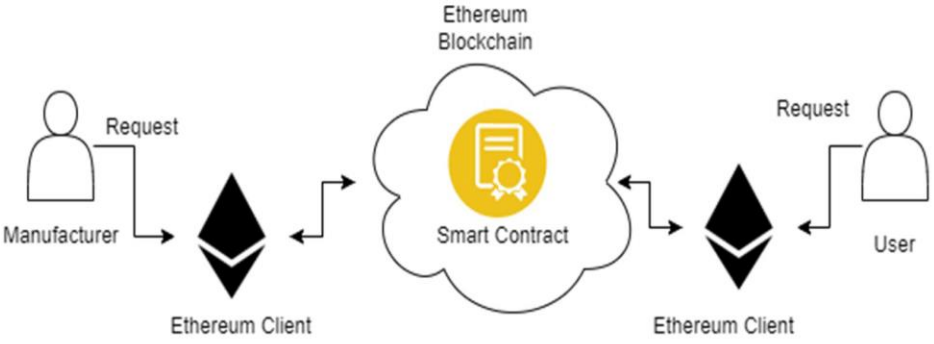


Figure 1: Proposed Framework

5. System Design

Ethereum is recommended for the system's back end. Ethereum smart contracts are written in solidity, a high-level programming language designed for Ethereum. Solidity supports inheritance, library imports, and more. For Ethereum Virtual Machine deployment, solidity is suggested. Ethereum Blockchain powers the platform's public smart contract while the web page interfaces with users. Web3.js links smart contracts to user interfaces. The website's server side uses node.js' HTTP-server package. After server configuration, supply private chain and address information. The figure shows the connections of all system components (Figure 2).

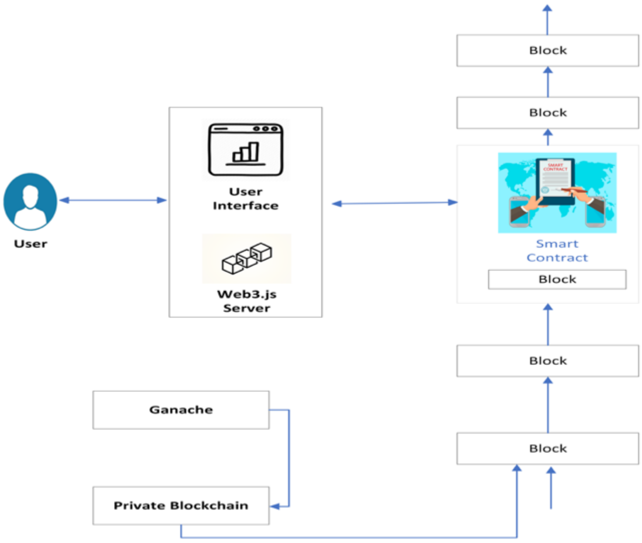
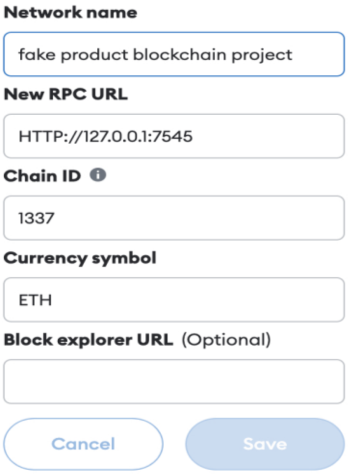


Figure 2: System Design

So, at first, we need to configure the truffle-config.js; now it's time to open metamask and create a network with the RPC server details mentioned in the ganache, which is http://127.0.0.1:7545. By doing this, it will allow the metamask to communicate with the local Blockchain (Figure 3).

- Install the metamask extension and create a new wallet by providing the new passwords.
- Click on the network menu (by default, Ethereum network)
- Click on Add network manually and enter the Ganache RPC server URL with port details, chain ID and currency symbol and save. Once it is added, click on switch to account.



Network name

fake product blockchain project

New RPC URL

HTTP://127.0.0.1:7545

Chain ID

1337

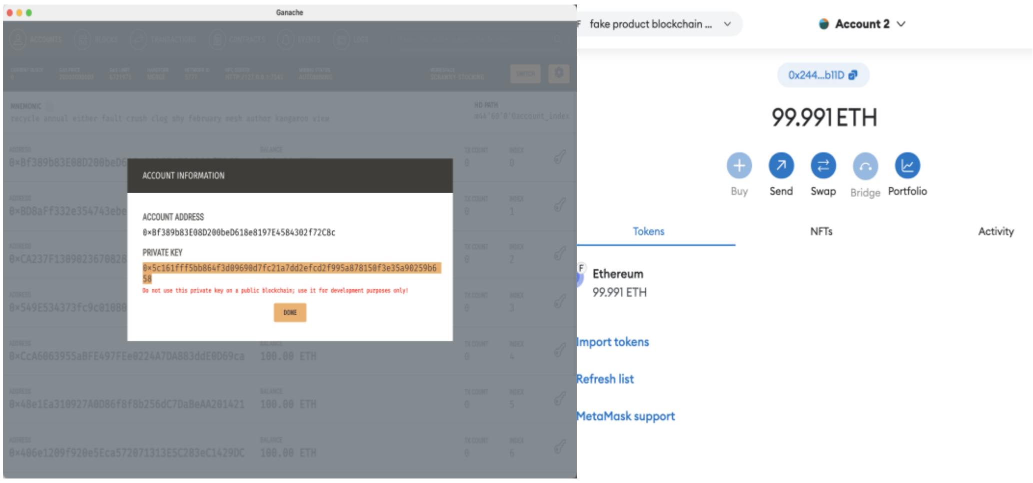
Currency symbol

ETH

Block explorer URL (Optional)

Figure 3: Add RPC server details from the Ganache to Metamark

Once the account is created, the private key from the ganache needs to be copied and pasted into the import account (metamask) and import (Figure 4).



ACCOUNT INFORMATION

ACCOUNT ADDRESS

0×8f389b83E08D200beD618e8197E4584302f72C8c

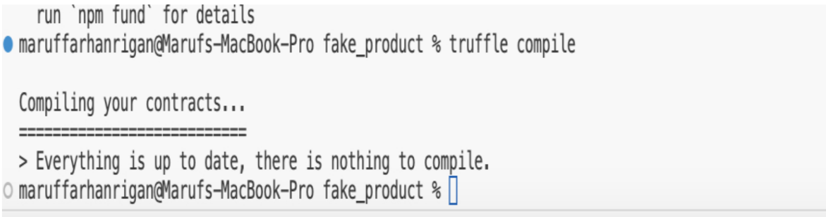
PRIVATE KEY

0×5c161fff5bb864f3d09698d7fc21a7dd2efcd2f995a878158f3e35a90259b658

Do not use this private key on a public blockchain; use it for development purposes only!

Figure 4: Copy the private key from the 1st Address of the Ganache window and Add it to the metamask account.

Once the metamask wallet is connected with the ganache, you need to run the “truffle compile” command in the VSC terminal (Figure 5).

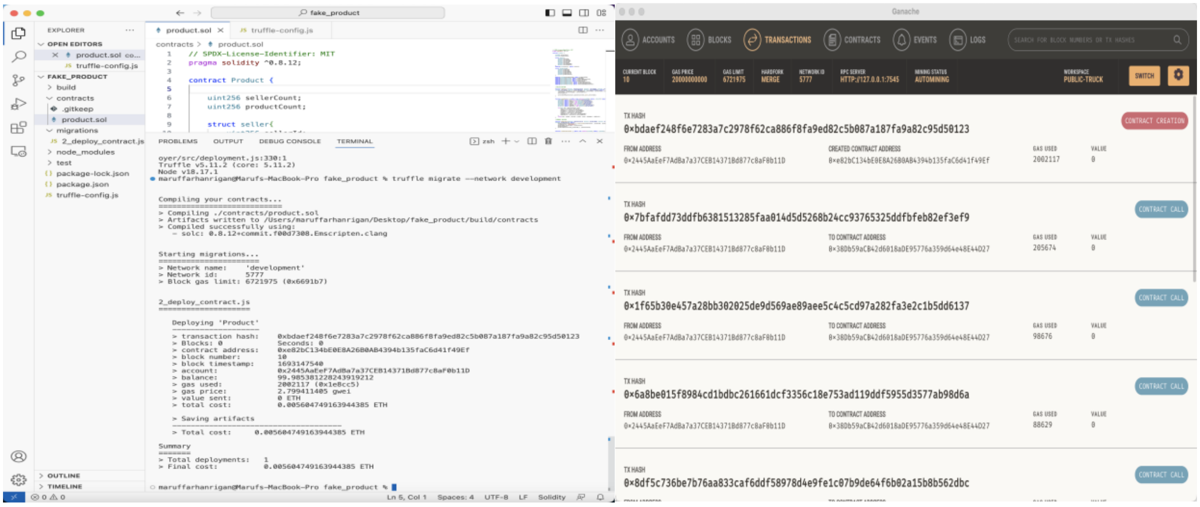


```
  run `npm fund` for details
● maruffarhanrigan@Marufs-MacBook-Pro fake_product % truffle compile

 Compiling your contracts...
 ===========================
 > Everything is up to date, there is nothing to compile.
○ maruffarhanrigan@Marufs-MacBook-Pro fake_product % 
```

Figure 5: Truffle compile command to run in VSC

After completing the compile, execute the command “truffle migrate –network development”. After a few seconds, it will complete the deployment of the contract to the local development network (Ganache). The contract address and other transaction details can be viewed in the deployment summary, which indicates that the deployment transaction was completed successfully (Figure 6).



```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.12;

contract Product {

    uint256 sellerCount;
    uint256 productCount;

    struct seller{
```

```
oyer/src/deployment.js:330:1
Truffle v5.11.2 (core: 5.11.2)
Node v18.17.1
● maruffarhanrigan@Marufs-MacBook-Pro fake_product % truffle migrate --network development


Compiling your contracts...
===========================
> Compiling ./contracts/product.sol
> Artifacts written to /Users/maruffarhanrigan/Desktop/fake_product/build/contracts
> Compiled successfully using:
   - solc: 0.8.12+commit.f00d7308.Emscripten.clang


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


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

   Deploying 'Product'
   -------------------
   > transaction hash:    0xbdaef248f6e7283a7c2978f62ca886f8fa9ed82c5b087a187fa9a82c95d50123
   > Blocks: 0            Seconds: 0
   > contract address:    0xe82bC134bE0E8A26B0AB4394b135faC6d41f49Ef
   > block number:        10
   > block timestamp:     1693147540
   > account:             0x2445AaEeF7AdBa7a37CEB14371Bd877c8aF0b11D
   > balance:             99.985381228243919212
   > gas used:            2002117 (0x1e8cc5)
   > gas price:           2.799411405 gwei
   > value sent:          0 ETH
   > total cost:          0.005604749163944385 ETH

   > Saving artifacts
   -------------------------------------
   > Total cost:     0.005604749163944385 ETH

Summary
=======
> Total deployments:   1
> Final cost:          0.005604749163944385 ETH

○ maruffarhanrigan@Marufs-MacBook-Pro fake_product % 
```

CURRENT BLOCK 10 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MERGE | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE PUBLIC-TRUCK

TX HASH 0×bdaef248f6e7283a7c2978f62ca886f8fa9ed82c5b087a187fa9a82c95d50123 — CONTRACT CREATION
FROM ADDRESS 0×2445AaEeF7AdBa7a37CEB14371Bd877c8aF0b11D
CREATED CONTRACT ADDRESS 0×e82bC134bE0E8A26B0AB4394b135faC6d41f49Ef
GAS USED 2002117
VALUE 0

TX HASH 0×7bfafdd73ddfb6381513285faa014d5d5268b24cc93765325ddfbfeb82ef3ef9 — CONTRACT CALL
FROM ADDRESS 0×2445AaEeF7AdBa7a37CEB14371Bd877c8aF0b11D
TO CONTRACT ADDRESS 0×38Db59aCB42d6018aDE95776a359d64e48E44D27
GAS USED 205674
VALUE 0

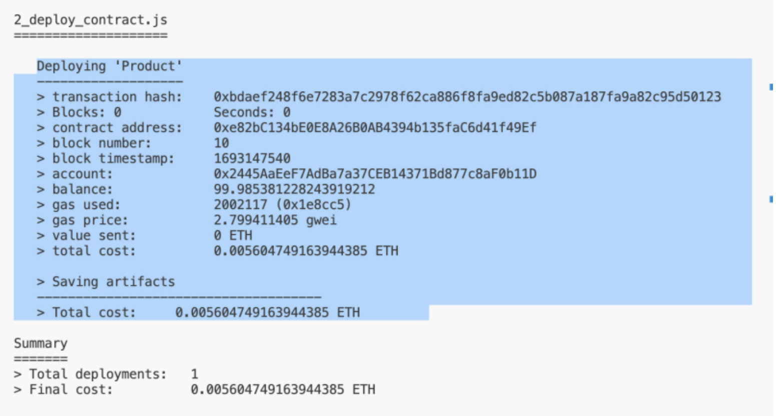
TX HASH 0×1f65b30e457a28bb302025de9d569ae89aee5c4c5cd97a282fa3e2c1b5dd6137 — CONTRACT CALL
FROM ADDRESS 0×2445AaEeF7AdBa7a37CEB14371Bd877c8aF0b11D
TO CONTRACT ADDRESS 0×38Db59aCB42d6018aDE95776a359d64e48E44D27
GAS USED 98676
VALUE 0

TX HASH 0×6a8be015f8984cd1bdbc261661dcf3356c18e753ad119ddf5955d3577ab98d6a — CONTRACT CALL
FROM ADDRESS 0×2445AaEeF7AdBa7a37CEB14371Bd877c8aF0b11D
TO CONTRACT ADDRESS 0×38Db59aCB42d6018aDE95776a359d64e48E44D27
GAS USED 88629
VALUE 0

TX HASH 0×8df5c736be7b76aa833caf6ddf58978d4e9fe1c07b9de64f6b02a15b8b562dbc — CONTRACT CALL

Figure 6: Deploying the product contract.sol

While performing the task, its written in the deploying “product” and showed transaction details occurred (Figure 7):



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

   Deploying 'Product'
   -------------------
   > transaction hash:    0xbdaef248f6e7283a7c2978f62ca886f8fa9ed82c5b087a187fa9a82c95d50123
   > Blocks: 0            Seconds: 0
   > contract address:    0xe82bC134bE0E8A26B0AB4394b135faC6d41f49Ef
   > block number:        10
   > block timestamp:     1693147540
   > account:             0x2445AaEeF7AdBa7a37CEB14371Bd877c8aF0b11D
   > balance:             99.985381228243919212
   > gas used:            2002117 (0x1e8cc5)
   > gas price:           2.799411405 gwei
   > value sent:          0 ETH
   > total cost:          0.005604749163944385 ETH

   > Saving artifacts
   -------------------------------------
   > Total cost:     0.005604749163944385 ETH

Summary
=======
> Total deployments:   1
> Final cost:          0.005604749163944385 ETH
```

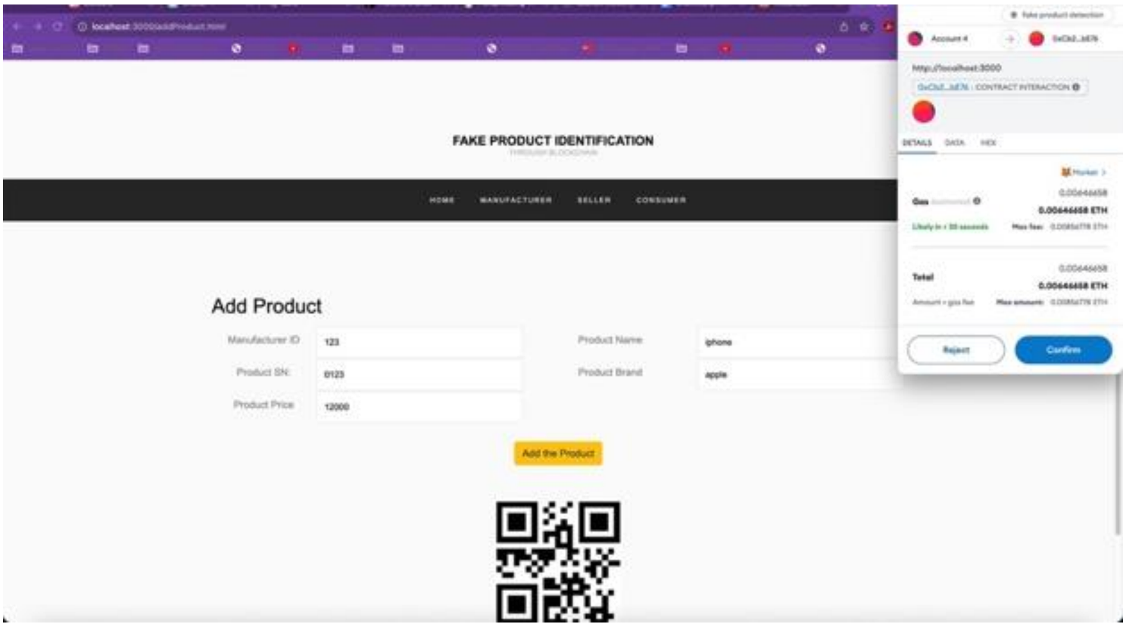
Figure 7: Deploy history

6. Result and Discussion

This chapter demonstrates our framework, showing readers and organizations how Blockchain may revolutionize authenticity verification by establishing a QR code. In this chapter, readers will learn about the simple user interface designed to improve user experience and adoption. This study shows how blockchain technology can provide an unalterable and verifiable transaction record. This boosts supply chain confidence and responsibility. A complete blockchain system interface demonstration is shown in this chapter. Manufacturers initially add products and information on the Blockchain. Manufacturers then add sellers and sell to them. After sales, clients can use QR codes to verify product legitimacy. An in-depth explanation of each phase is meant to demonstrate the innovation and explain the process. This section will describe the solution, identify issues, and offer solutions. Considering practical hurdles and the broader consequences for organizations coping with counterfeit goods issues, we will debate the efficacy of our strategy. This section applies theoretical concepts to practice, closing the gap. Watch the demonstration and imagine what happens when cutting-edge technology meets consumer trust and credibility.

Stage 1: add product to Blockchain

The first step is for the manufacturer to visit the website and add product details, which will help the manufacturer add the product to the Blockchain. After entering the details, it will generate a blockchain-based QR code, which will be saved for further investigation. During this process, metamask will notify the confirmation and need to click on continue (Figure 8).



Add Product

Manufacturer ID: 123

Product Name: iphone

Product SN: 0123

Product Brand: apple

Product Price: 12000

http://localhost:3000

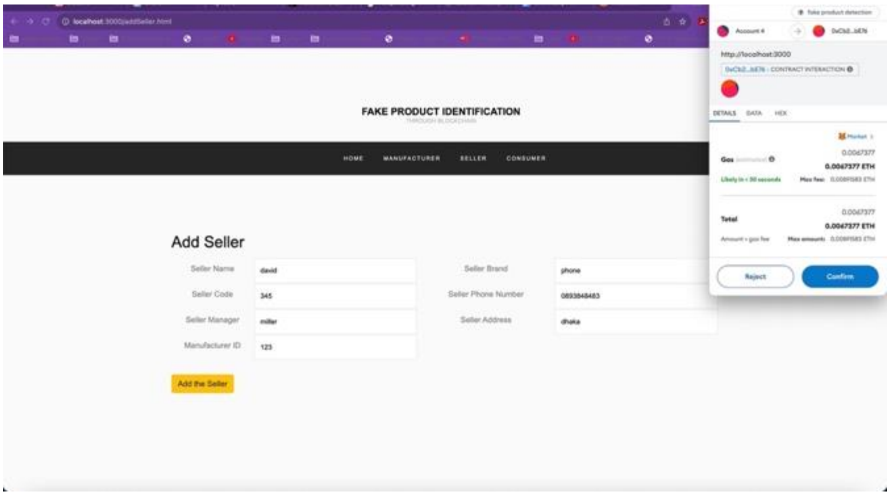
Gas: 0.00646658 ETH

Total: 0.00646658 ETH

Figure 8: Add product details

Stage 2: Add seller

In the next task, the manufacturer will go to the add seller tab and insert a few details such as Seller name, Seller Brand, Seller code, Seller phone number, Seller Manager, Address, and manufacturer ID and add the seller (Figure 9).



Add Seller

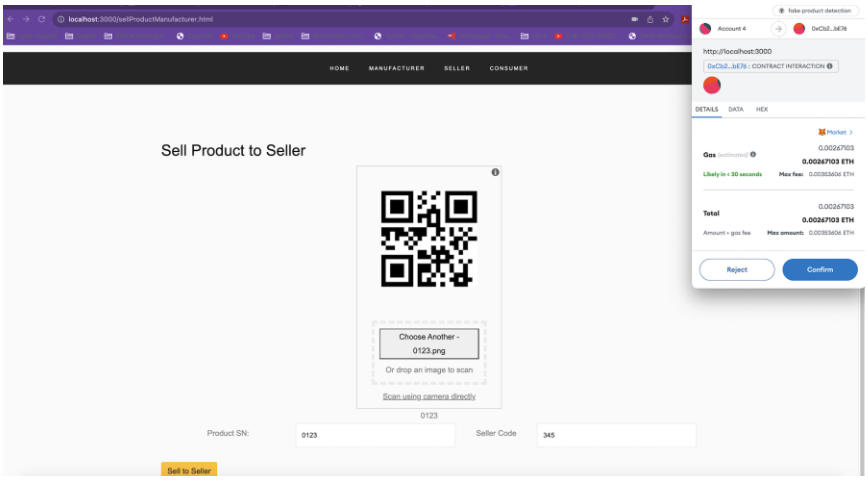
Seller Name: david
Seller Brand: phone
Seller Code: 345
Seller Phone Number: 0893848483
Seller Manager: miller
Seller Address: dhaka
Manufacturer ID: 123

Gas: 0.0067377 ETH, Likely in < 30 seconds, Max fee: 0.0089583 ETH
Total: 0.0067377 ETH, Max amount: 0.0089583 ETH

Figure 9: Add seller details to the block

Stage 3 Sell Product to Seller:

Once the manufacturer adds the seller, they will sell their product to the seller. In that tab, the manufacturer will add or scan the QR code. After that, all the necessary information, such as product SN and seller code, will be automatically uploaded to the website (Figure 10).



Sell Product to Seller

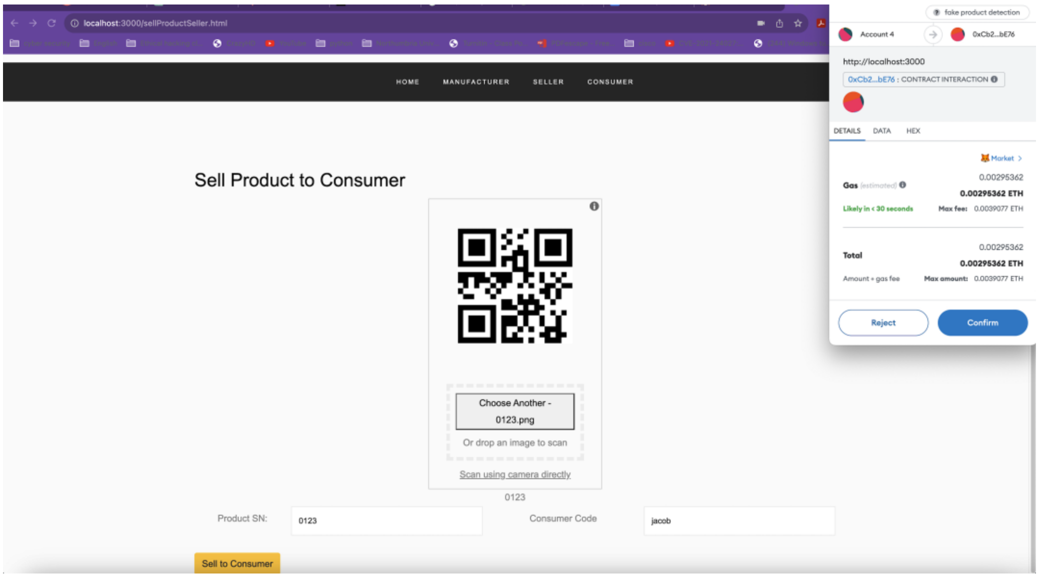
Product SN: 0123
Seller Code: 345

Gas: 0.00267103 ETH, Likely in < 30 seconds, Max fee: 0.00353606 ETH
Total: 0.00267103 ETH, Max amount: 0.00353606 ETH

Figure 10: Sell product to seller

Stage 4:

At this stage, when a customer visits the seller shop or seller who wants to deliver the product to a customer, then they will add the QR code and add some information such as product SN and customer code (Name) and sell to the consumer (Figure 11).



Sell Product to Consumer

0123

Product SN: 0123

Consumer Code: jacob

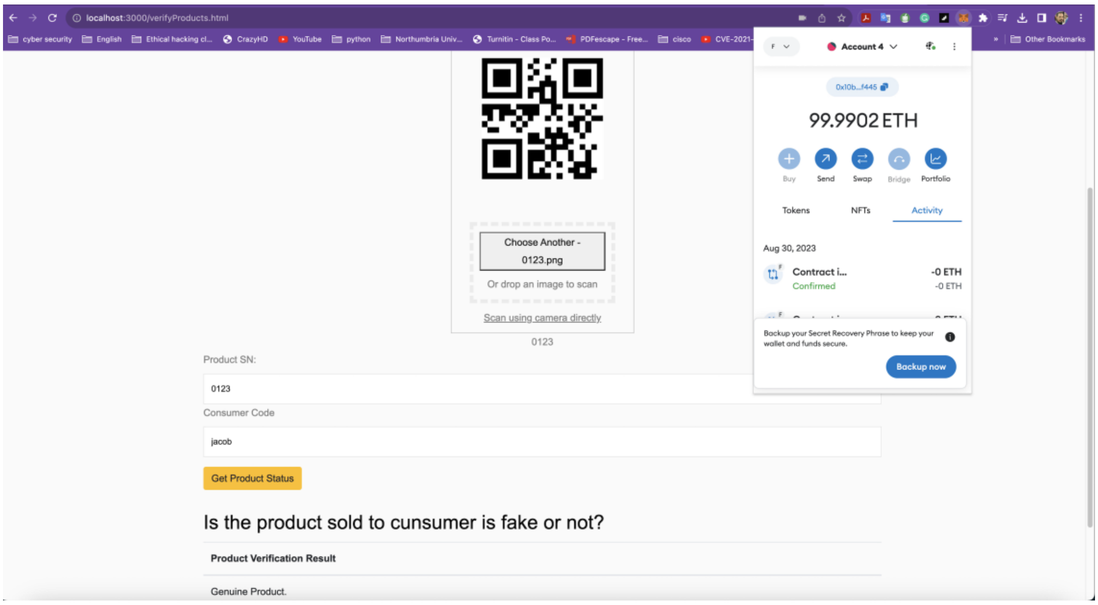
Gas (estimated) 0.00295362
0.00295362 ETH
Likely in < 30 seconds Max fee: 0.0039077 ETH

Total 0.00295362
0.00295362 ETH
Amount + gas fee Max amount: 0.0039077 ETH

Figure 11: Seller sells the product to the seller

Stage 5:

When the product is sold, the customer will visit the website and go to the customer section. In the customer section, there are two options: product history and product verification. Once the customer scans the QR code, the product serial number will be uploaded, and the customer needs to enter the customer code. After that, when he or she clicks on the product status, it will show details about whether the product is genuine or fake. In the below picture, when there was no tampering with the data, especially the QR code, the customer received the genuine product. Apart from that, in the customer section, there is an option for a customer to check the purchase history, where he can get information about seller ID and manufacturing ID as well (Figure 12).



0123

Product SN:

0123

Consumer Code

jacob

Is the product sold to cunsumer is fake or not?

Product Verification Result
Genuine Product.

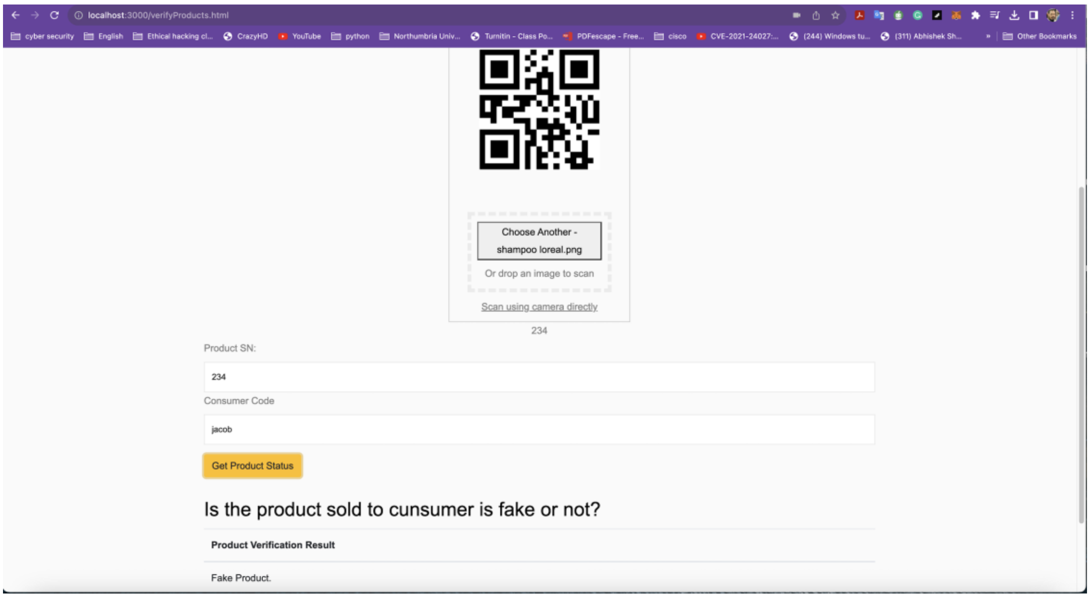
99.9902 ETH

Aug 30, 2023
Contract i... -0 ETH
Confirmed -0 ETH

Backup your Secret Recovery Phrase to keep your wallet and funds secure.

Figure 12: Customer verifying the product.

Suppose the manufacturer added the product and all information in the first stage and generated the blockchain-based QR. Suppose the seller tampered with the QR code and sold it to the customer. When the customer goes through stage 5 again and verifies the QR code, it will prompt a fake product notification and provide information to the manufacturer from where he got the fake products so that the manufacturer can trace it (Figure 13).



234

Product SN:

234

Consumer Code

jacob

Get Product Status

Is the product sold to cunsumer is fake or not?

Product Verification Result
Fake Product.

Figure 13: Fake product detection

So, by following the procedure with the help of blockchain technology, customers can detect whether they purchased genuine products or fake products.

7. Result Analysis

Transaction cost is associated with blockchain data transmission. In Ethereum, transaction cost is the amount of cryptocurrency (in this case, Ether ETH) needed to complete a transaction or smart contract. This cost is related to the computing resources needed to validate the network transaction. This procedure uses gas prices and limits to determine transaction codes. Here is how it works:

Gas price: The sender's ether investment per unit of gas is the gas price. Each transaction uses a certain amount of gas, a computer unit. The sender sets the gas price, which is the amount they will pay miners per cubic metre.

Gas limit: Gas limit refers to the maximum amount of gas required for a transaction or contract execution.

Total transaction cost calculated as a: Total transaction cost: gas price * gas limit.

If the gas price is higher, it becomes more appealing to the miners, who include transactions with higher gas fees in the blocks they mine. Miner earns gas fees as a reward for processing transactions and executing smart contracts. Here, the etherscan.io was used to convert Ether to USD. Visual studio code was used to develop the smart contract to determine the gas needs. A metamask was used to interact with the contract and find out the costs. The cost for deploying the product contract was 0.005604749 ETH, equivalent to 9.14 USD (based on today's exchange rate). The overall cost for the system is less than 15 USD, proving the proposed model's cost-effectiveness (Table 1).

Table 1: Gas Calculation

Step	Gas used	Gas prices (Gwei)	Transaction cost	Gas Fee
Deployment transaction	2002117	2.79	0.005604749	9.14 USD
Manufacturer adds the product and generates a QR code	205,854	20	0.000411708	0.6720 USD
Manufacturer adds a Seller	228,644	20	0.000457288	0.7460 USD
Selling the product to the Seller	88,665	20	0. 0.00017733	0.2893 USD
Selling the product to the Customer	101,189	20	0.000202378	0.3304 USD
Customer doing the verification	31,586	20	0.000063172	0.1031 USD
Total transaction cost			0.007916628 ETH	12.2905 USD

There are many benefits to using blockchain technology to identify counterfeit products, but there are also drawbacks. The downsides include:

Technological experts: Blockchain-based counterfeit detection may need technical skills. For small firms or organizations with few resources, creating such a system may be tough.

Limited Adoption: Blockchain-based counterfeit detection technologies are rarely used, leaving items and manufacturers uncovered. This may limit its ability to identify counterfeit products throughout the process.

False positive: Blockchain-based counterfeit detection systems focus on counterfeit products. However, these algorithms may produce false positives, misclassifying legitimate products as counterfeit. This could lead to the elimination of real products or excessive financial obligations on businesses.

In Bangladesh, Blockchain is still new, and most people are unaware of it. To popularize Blockchain and its applications, authorities should provide more training and awareness. Another barrier was blockchain technology ignorance. The suggested solution helps producers and buyers prevent counterfeit items from being sold. Still, it may fail if a dishonest person removes a legal QR code from a product and transfers it to a counterfeit one. The first product sold is real, whether it is phoney or real, and another product is fake. The system will cost more because each product's supply chain information requires a lot of memory. The next step is to utilize this concept and develop ways to overcome its restrictions, such as embedding material in the product so that when someone takes a QR code, the chip or anything else sends the signal. Future work will focus on this.

8. Conclusion and further work:

Counterfeit goods are everywhere, so a secure method to detect and eliminate them is needed. Blockchain detects and stops counterfeit products automatically. Considering everything mentioned thus far, a fully operating application that verifies product authenticity is quite valuable to the retail industry. This protects the manufacturer's reputation and guarantees buyers that their purchases are authentic and labelled. Only Blockchain enhances data security and functionality. Blockchain-based applications help commodity producers and customers. We provide a fully functional app that compares a product to a known authentic sample to help consumers identify counterfeits. Manufacturers pioneered blockchain product data storage. Their QR code provides third-party information. When the item arrives, additional parties' ownership details will be included. Finally, the consumer scans the QR code, reads the product's history, and verifies authenticity. The current method requires manual inputs and restricts size. This opens growth and improvement. Automation increases data entry speed and reduces errors. Ethereum's pricing inhibits system growth. Any large Ethereum value changes will raise our system's costs. Devs can divide open-source blockchains and establish a blockchain framework for specific use cases, minimizing Ethereum utilization. Immutability, security, and smart contract automation protect customers. Scalability and usefulness need further study. To overcome limitations, materials can be embedded in products to convey signals when a QR code is scanned. Work will focus on this.

Acknowledgement: I would like to express my sincere gratitude to my research project supervisor, Rejwan Bin Sulaiman for their invaluable guidance and support throughout this project. His expertise and mentorship were instrumental in shaping my research and ensuring its success. I am also grateful to Northumbria University for providing access to the resources and facilities that made this research possible. My deepest thanks also go to my family for their unwavering encouragement and support. I am especially grateful to my family members for their support. Finally, I acknowledge the blessings of Allah, which have guided and sustained me throughout this journey.

Data Availability Statement: In the spirit of open science and transparency, the datasets were not used in this study. Should you have any questions regarding the access, please contact Maruf Farhan at marufrigan9@gmail.com

Funding Statement: This research was conducted independently and self-funded as part of my personal exploration during the research project proposal course at Northumbria University.

Conflicts of Interest Statement: The author declares no conflicts of interest in relation to the publication of this paper. The research was conducted with integrity and objectivity, free from any external influence that could compromise its findings. All data sources are duly cited and referenced within the project.

Ethics and Consent Statement: This research adhered to the ethical standards and guidelines established by Northumbria University, London. All research procedures involving human subjects were reviewed and approved by the university's ethics committee and my supervisor. Informed consent was obtained from all participants, and they were assured of the confidentiality and anonymity of their information. The ethical conduct of this research aligns with the principles outlined in the research outline.

References

1. OECD, “Trends in trade in counterfeit and pirated goods, illicit trade”, Oecd.org, 2019. [Online]. Available: https://www.oecd.org/corruption-integrity/reports/trade-in-counterfeit-and-pirated-goods-9789264252653-en.html. [Accessed: 04-Feb-2023].
2. Abra, “Conquer crypto”, Abra, 2022. Available at: https://www.abra.com/ [Accessed: 04-Feb-2023].
3. N. Anjum and P. Dutta, “Identifying counterfeit products using blockchain technology in supply chain system,” in 2022 16th International Conference on Ubiquitous Information Management and Communication (IMCOM), IEEE, 2022.
4. M. Attaran, “Critical success factors and challenges of implementing RFID in supply chain management”, Csupom.com, 2012. Available at: https://www.csupom.com/uploads/1/1/4/8/114895679/jscom_2012-1-11.pdf [Accessed: 06-Feb-2023].
5. P. Blaettchen, A. Calmon, and G. Hall, “Traceability technology adoption in supply chain networks,” SSRN Electron. J., 2021.
6. J. Bulchand-Gidumal and S. Melián-González, “Fighting fake reviews with blockchain-enabled consumer-generated reviews,” Curr. Issues Tourism, pp. 1–15, 2023, Press.
7. CryptoKitties, “CryptoKitties, CryptoKitties”, 2017. Available at: https://www.cryptokitties.co/. [Accessed: 06-Feb-2023].
8. L. Insights, “Luxury blockchain consortium from LVMH, Prada, Cartier appoints leader, Ledger Insights - blockchain for enterprise”. Ledger Insights, 2021. Available at: https://www.ledgerinsights.com/luxury-blockchain-consortium-from-lvmh-prada-cartier-appoints-leader/ [Accessed: 06-Feb-2023].
9. S. Kalpana Devi, K. Samy Durai, K. M. Shri Balaji, and J. Ravi Kumar, “Fake product identification with the help of blockchain technology,” in 2021 Innovations in Power and Advanced Computing Technologies (i-PACT), IEEE, 2021.
10. R. Kumar and R. Tripathi, “Traceability of counterfeit medicine supply chain through Blockchain,” in 2019 11th International Conference on Communication Systems & Networks (COMSNETS), IEEE, 2019.
11. J. Ma, S.-Y. Lin, X. Chen, H.-M. Sun, Y.-C. Chen, and H. Wang, “A blockchain-based application system for product anti-counterfeiting,” IEEE Access, vol. 8, pp. 77642–77652, 2020.
12. Mallegowda et al., “Fake product identification system using blockchain,” in 2022 4th International Conference on Circuits, Control, Communication and Computing (I4C), IEEE, pp. 163–167, 2022.
13. S. Musale et al. “Authentify - Blockchain Based Counterfeit Product Detection - IRE journals,” IRE Journals, vol. 6, no. 10, pp. 595–599, 2023.
14. Y. Rawal, “Blockchain-based solutions to prevent counterfeit drugs”, Akeo, 2020. Available at: https://medium.com/akeo-tech/blockchain-based-solutions-to-prevent-counterfeit-drugs-6e1ebae8c14a [Accessed: 06-Feb-2023].
15. N. Saxena, I. Thomas, P. Gope, P. Burnap, and N. Kumar, “PharmaCrypt: Blockchain for the critical pharmaceutical industry to counterfeit drugs,” Computer (Long Beach Calif.), vol. 53, no. 7, pp. 29–44, 2020.
16. C. Singh and S. Shandilya, “Counterfeited product identification in a Supply Chain using blockchain technology, ” Res,” Res. Br. Inf. Commun. Technol. Evol, vol. 7, no. 3, pp. 1–15, 2021.
17. D. Sivaganesan, A. S. Kareshmmaa, A. K. S. Shankar and A. P. B, "PharmaSafe - Blockchain-Based Counterfeit Detection in the Pharmaceutical Sector," 2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS), Coimbatore, India, pp. 151-156, 2023, doi: 10.1109/ICISCoIS56541.2023.10100382.
18. 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," in IEEE Access, vol. 5, pp. 17465-17477, 2017, doi: 10.1109/ACCESS.2017.2720760.
19. B. R. Tukamuhabwa, M. Stevenson, J. Busby, and M. Zorzini, “Supply chain resilience: definition, review and theoretical foundations for further study,” Int. J. Prod. Res., vol. 53, no. 18, pp. 5592–5623, 2015.
20. A. Wahane and B. Patil, “Blockchains to curb Fake News in an Online World,” in 2022 International Conference for Advancement in Technology (ICONAT), IEEE, pp. 1–6, 2022.
21. Mallegowda et al., “Fake product identification system using blockchain,” in 2022 4th International Conference on Circuits, Control, Communication and Computing (I4C), IEEE, 2022.