IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

Fake Product Identification

Abhi Jain, Gaurav Pal, Abhinav Das Lodhi
Department of CSE-Data Science
Raj Kumar Goel Institute of Technology, Ghaziabad, U.P., India
abhijn.2002@gmail.com, gauravpalmrt13@gmail.com, Abhinav.abss@gmail.com

Abstract: *Products that are designed to seem exactly like the real thing but are constructed using inferior materials lower their overall quality and are therefore considered counterfeit. Customers frequently fail to identify these counterfeit goods' poor quality at first glance, despite the fact that they may look similar to the real ones. Customers find it very challenging to determine if the product they are buying is genuine or counterfeit as a result. Only a few techniques are available to confirm a product's uniqueness. As a result, consumers frequently pause before buying because they are ill-equipped to verify the legitimacy of a product. Both the client and the business may suffer large losses as a result of this circumstance. Additionally, it may erode consumers' faith in the brand.Blockchain technology can be used for efficient product tracking to avoid such problems. Blockchain enables safe and impenetrable product tracking because of its well-known immutability and transparency. The primary objective is to develop a system that uses the Blockchain network to store crucial product data, such as the product ID, manufacturing date, location, and manufacturer's name. Peer-to-peer transactions and a decentralized, immutable record would be guaranteed. Customers can quickly validate the product's legitimacy by scanning a QR code after receiving it, enabling them to determine whether or not it is authentic*

Keywords: Blockchain technology, Decentralized system, Counterfeit prevention, immutability, transparency, product verification.

I. INTRODUCTION

Numerous industries, including luxury handbags, medical supplies, auto parts, mobile gadgets, and more, can generate counterfeit goods. Consumers frequently unintentionally buy these counterfeit goods because they think they are real, which costs them money. The growing prevalence of fake goods has raised serious concerns for both customers and legitimate companies. According to the results of several research, counterfeit goods account for about 3.3% of worldwide trade. China is the nation that produces the most counterfeit goods, followed by Singapore, India, and Turkey.

Blockchain technology can be used to increase transparency and confidence in the product manufacturing and supply chain, from the initial manufacturer to the final consumer. Blockchain is renowned for its distinct characteristics, which include transparency, immutability, and a decentralized peer-to-peer network. Every piece of information is safely saved in blocks on a blockchain, where each one is transformed into a hash value. Along with the hash of the block before it, each block keeps its own data. Since this chain of blocks keeps going, it is impossible to make changes without also changing the chain as a whole. Any changes will be immediately apparent since the blocks' link will be broken.

This study suggests a method that uses blockchain technology to track and record a product's complete journey, from manufacturing to customer delivery. By doing this, the consumer is guaranteed to be able to confirm that the item they have got is indeed from the original manufacturer. Blockchain technology guarantees openness and stops product details from being altered after they are saved. Consumers can quickly obtain this information by using their mobile device to scan a QR code on the product or by seeing the information on an IPFS-enabled website. This technique aids in determining if a product is genuine or fake.

DOI: 10.48175/IJARSCT-26673

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

II.BACKGROUND

IPFS Overview

By storing all data in the form of files or blocks within a decentralized peer-to-peer network, IPFS can perform functions similar to those of Blockchain.

Peer-to-peer transactions, blockchain's decentralized structure, and its capacity to avoid data duplication are some of its primary features. All of these features are also offered by IPFS, which makes it appropriate for this project in order to guarantee decentralization and preserve the previously listed advantages. The technology known as IPFS, or Interplanetary File System, is used to store a variety of data kinds, including documents, photos, apps, websites, and more. It locates material by using its hash value. The Keccak-256 hashing method is used to transform each file into a distinct hash code before it is saved in IPFS. This project uses IPFS to store crucial product information on the blockchain, including the product ID, production date, image, etc.

Since IPFS is decentralized by design, it naturally offers a high level of security and also ensures data uniqueness by preventing duplication within the system.

Because IPFS files are shared and dispersed over several network nodes, it is very difficult for a single node group to interfere with or take down the entire network.

Sharing files through IPFS is more convenient and efficient. Unlike the traditional HTTP protocol, which uses location-based addressing to find files, IPFS uses content-based addressing. This method allows IPFS to quickly and easily locate files within the network by using their unique content hash, making the process faster and less time-consuming.

III. KECCAK-256 ALGORITHM

A cryptographic hash function that generates a 256-bit hash value, Keccak-256 is essential for many applications. Keccak-256, a member of the SHA-3 family, is a great option for guaranteeing the authenticity and integrity of data since it is built to offer strong security features.

One of the primary uses of Keccak-256 is in digital signatures, where it helps verify the authenticity of messages or documents. By generating a unique hash value for a given input, Keccak-256 enables the creation of digital signatures that are both secure and verifiable.

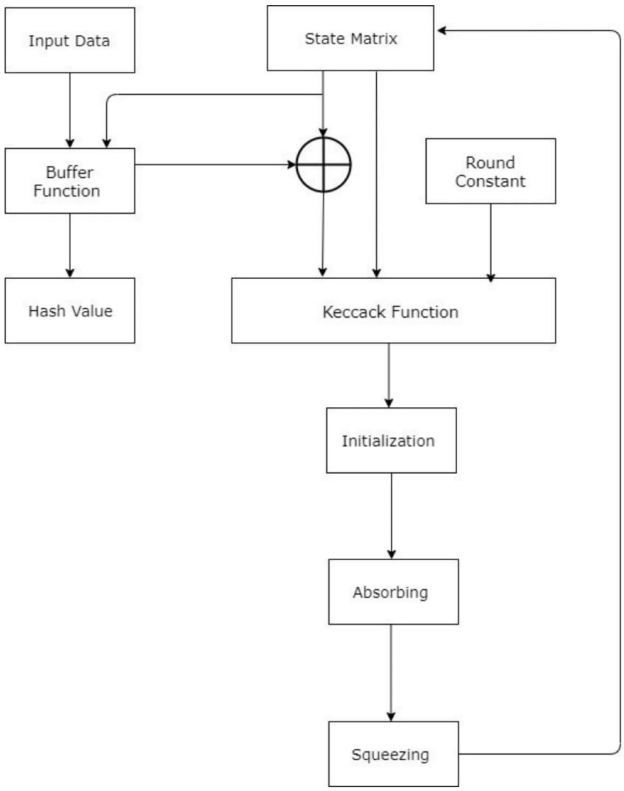
Keccak-256 is also frequently used in data integrity verification to make sure that information hasn't been changed or tampered with while being sent or stored. Users may check the integrity of their data and identify any possible manipulation by comparing the predicted hash value with the actual hash value.

In addition to its applications in digital signatures and data integrity verification, Keccak-256 is also used in cryptocurrencies like Ethereum. Here, it plays a critical role in securing transactions and ensuring the integrity of the blockchain.

Keccak-256's security properties make it a desirable option for a range of applications. Its ability to withstand collision and preimage attacks guarantees that the produced hash values are unique and difficult to duplicate. Additionally, Keccak-256's adaptability makes it suitable for a variety of uses, including digital forensics and safe data storage.

Overall, Keccak-256 is a powerful cryptographic hash function that provides robust security features and flexibility, making it an essential tool in various applications, including digital signatures, data integrity verification, and cryptocurrencies. Its ability to generate unique and secure hash values ensures the authenticity and integrity of data, making it a vital component of modern cryptographic systems.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67



IV. LITERATURE SURVEY

A While a lot of research has been done to identify counterfeit goods, blockchain technology is still a relatively new and developing use in this field. Recently, a number of researchers have concentrated on using blockchain technology for this.

This paper mainly aims to apply the decentralized concept effectively by using a cost-efficient method that minimizes transaction fees while maintaining accurate records of product information. These details can later be verified by customers using either a web application or by scanning a QR code through their mobile devices.

JINHUA MA et al. [1] suggested how the immutable nature of Blockchain can be leveraged to store product details securely. They utilized Bitcoin for handling transactions. Bitcoin is a virtual currency that operates independently without any central authority or governing body.

Ownership of the product is passed from the producer to the distributor and subsequently to the client, according to a technique presented by M. Lavanya et al. [2]. Every transaction is documented in the Blockchain ledger. A ledger is a mechanism for preserving financial records that keeps track of every transaction. This guarantees accurate documentation and traceability of the product ownership transfer at each stage.

Hash values are generated as proof of work during transactions in the approach proposed by Aman Thakkar et al. [3]. They created hash values using SHA-256 hashing in conjunction with data and counter values, which are subsequently transformed into big numbers. These hash values were stored in BoltDB, an open-source key-value database that facilitates ACID transactions without the need for a specialized database server.

An IoT-based architecture was developed by Chin-Ling Chen et al. [4] as a means of tracking counterfeit medications. Their method uses smart contracts to store the product information on the Blockchain. Self-executing programs that follow preset rules are known as smart contracts.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

A system that applies Blockchain to all stages of the product lifecycle was proposed by Yasmeen Dabbagh et al. [5]. In order to validate transactions and boost system security, their method uses digital signatures from customers. There are rules and algorithms specific to each step of the product journey.

M.C Jayaprasanna et al. [6] introduced a method where product details can be stored and verified using a QR code within a decentralized Blockchain environment. Customers can validate the product by comparing the Blockchain-stored details with their own product information.

A system that integrates Firebase and Blockchain to store product data was put out by Roshan Jadav et al. [7]. By comparing the product details saved in Firebase, users may determine if a product is authentic or fraudulent. Additionally, they created a mobile application using Android Studio that lets users scan QR codes and get product alerts.

To stop fake goods, Yash Madhwal [8] suggested a blockchain-based tokenized approach. Their research, which concentrated on the supply chain for airplanes, showed how Blockchain tokens may be used to monitor and confirm the legitimacy of goods all the way through the supply chain.

V. METHODOLOGY

A thorough overview of the project's methodology is given in this module. The general idea is well understood because to the architectural design. The major goal is to efficiently use Blockchain technology to store manufacturer-provided product-related data while guaranteeing that the data is safe, tamper-proof, and permanent. The manufacturer initiates the Blockchain process and serves as the system's first entity. Once the product is ready for delivery, the manufacturer inputs the product details into the web portal, including the product ID, picture, production date, product type, and quantity produced. The manufacturer has the opportunity to register if this is their first time using the system; after they have done so, their login credentials will provide them access in the future.

After submitting the product details, a Google Chrome extension called MetaMask is utilized. MetaMask is a cryptocurrency wallet that enables users to perform Blockchain-based transactions using digital currencies like Ethereum. In this project, Ganache is used to supply the required Ethereum for these transactions. Every new entry of product details made by the manufacturer into the Blockchain is treated as an individual transaction.

Ethereum from the wallet is utilized during a transaction, and the information is saved in the Blockchain as a distinct hash value inside a particular block. To further improve data security and integrity, the project stores product-related data as hash values over a decentralized network using the InterPlanetary File System (IPFS).

5.1 QR Code Generator

As soon as the manufacturer uploads the product specifications to the Blockchain, the data is secure and unbreakable. The next step is for the administrator to create a QR code for the appropriateproduct. The administrator can examine the list of products supplied by the manufacturer. Once the information is verified, the administrator may generate a QR code for each product. This process for creating QR codes is implemented using the qrcode Python package.

Each of the black and white squares that make up the QR code is a two-dimensional barcode that represents binary values (0 or 1). The qrcode library may be used to build a QR code in a number of ways. The add_data() method is used to add the required data to the QR code, while make() is used to generate the QR structure. The make_image() function is used to produce the QR code as an image, and the save() method is used to save the image file. Both the admin module and the customer interface will display the generated QR code. After the consumer signs in and selects a product, the matching QR code will show up.

By scanning this QR code and comparing the information safely recorded in the Blockchain, the buyer can confirm the product's legitimacy.

5.2 Customer

Customers in this module are in charge of verifying that they receive the proper goods upon delivery by scanning it with the generated QR code. The client will be able to register using their phone number and personal details, such as their birthdate, in a separate logging module. These details can be used for further confirmation. After registering, the

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

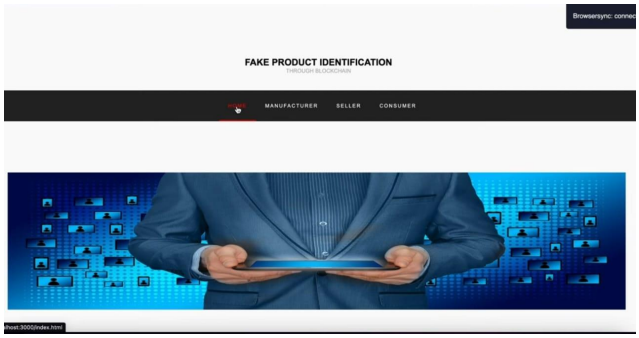
client can use their login information to log in. After completing the login procedure, the customer may browse the product listings and the QR code. These QR codes may be scanned by the Android app to reveal details about the items that the manufacturer has already uploaded.

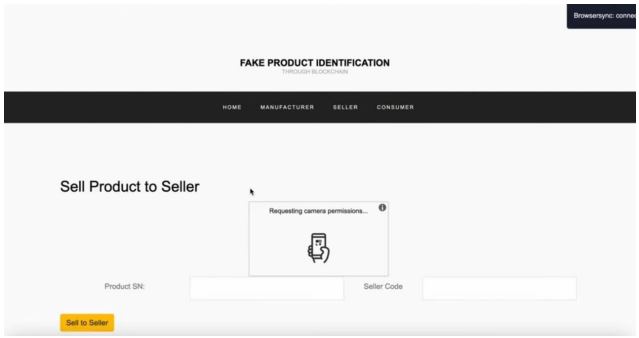
Android Studio is used to create a brief, lightweight application that can connect to the phone and install itself. The phone is ready to scan the QR code after the application has been installed. All of the product data that the manufacturer maintains will be stored in the smart contracts. On the Blockchain, smart contracts—self-executing programs—are triggered when a transaction takes place. Smart contracts utilize if-and-then phrases to carry out preset rules. Once the conditions of the rules are satisfied, the software operates automatically without the need for any outside commands. These smart contracts are created using the Solidity programming language, which is similar to JavaScript. Remix is the IDE used to run these smart contracts.

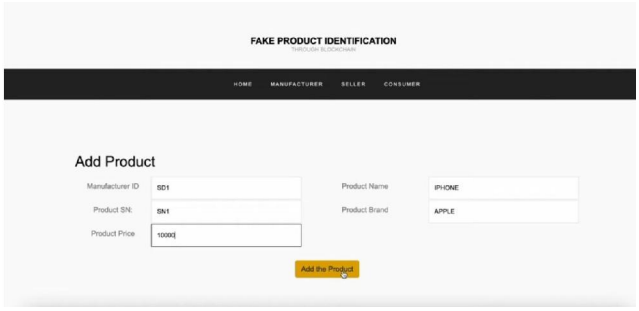
Smart contracts are managed via the web-based platform Remix, which may also be connected to Metamask. After scanning the QR code and learning more about the products, the consumer will be able to tell if the item he received is genuine or fake.

VI. RESULTS AND DISCUSSIONS

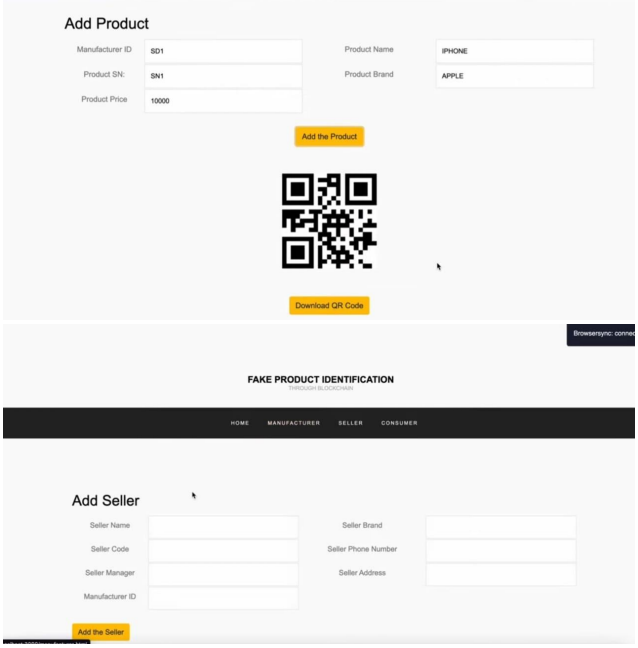
Using a few screenshots and images, this part will provide information about how effective the work that has been done is.







IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67



Language Used

1. Solidity for writing smart contracts (Migrations.sol, product.sol)
2. JavaScript - for writing deployment scripts and interacting with the blockchain (1_initial_migration.js, 2_deploy_contracts.js)
3. HTML/CSS/JS - likely used in the src folder for the frontend (though we can't see exact files here)

Packages & Frameworks

From the file structure and file names, here's what's being used:

1. Truffle - Ethereum development framework used to create, implement, and evaluate smart contracts
Config file: truffle-config.js
2. Node.js & npm - for managing packages
package.json and package-lock.json indicate that npm is being used
3. Web3.js or Ether.js (likely) – for interacting with Ethereum blockchain from JavaScript

Packages Needed:-

Core: 5.6.7; Truffle v5.6.7
Ganache version 7.5.0
Solidity (solc-js) v0.5.16
Version 15.8.0 of Node
Web3.js version 1.7.4
npm 7.5.1

VII. CONCLUSION

Blockchain technology has been emerging as one of the most powerful and innovative technologies in recent years due to its core features like transparency, immutability, and decentralized nature. These features make Blockchain highly reliable for storing sensitive data and maintaining records without the risk of tampering or unauthorized modification. One of the most promising areas where Blockchain can be effectively utilized is in product lifecycle

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

management.Maintaining a safe, transparent, and impenetrable record of each step a product takes, from production to delivery to the final consumer, is made feasible by incorporating Blockchain technology in this field. This ensures that all information pertaining to the product is authentic and cannot be altered or fabricated at any time. The primary focus of this study is the creation of a blockchain-based fake goods identification system. This system aims to solve the rising problem of counterfeit goods in the market by providing a reliable solution that helps manufacturers, distributors, and consumers verify a product's authenticity. By securely keeping product-related data on the Blockchain and making it easily available to customers for verification, the proposed approach aims to improve transparency, build trust, and ensure product uniqueness across the supply chain.

REFERENCES

[1]. Ma, J., Lin, S. Y., Chen, X., Sun, H. M., Chen, Y. C., & Wang, H. (2020). A blockchain-based application system for product anti-counterfeiting. IEEE Access, 8, 77642-77652.

[2]. Shreekumar, T., Mittal, P., Sharma, S., Kamath, R. N., Rajesh, S., & Ganapathy, B. N. (2022). Fake Product Detection Using Blockchain Technology. JOURNAL OF ALGEBRAIC STATISTICS, 13(3), 2815-2821.

[3]. Funde, A., Nahar, P., Khilari, A., Marne, N., & Nerkar, N. (2019). Blockchain Based Fake Product Identification in Supply Chain. International Research Journal of Engineering and Technology (IRJET), 6(5), 5367-5369.

[4]. NABI, S. A., Reddy, K. S., Reddy, M. R., Harish, J., Kumar, D. V., & Manasvi, A. (2023). AUTHENTICATION OF PRODUCT & COUNTERFEITS ELIMINATION USING BLOCK CHAIN. International Journal of Early Childhood Special Education, 15(1).

[5]. Jayaprasanna, M. C., Soundharya, V. A., Suhana, M., & Sujatha, S. (2021, February). A Block Chain based Management System for Detecting Counterfeit Product in Supply Chain. In 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) (pp. 253-257). IEEE.

[6]. Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) (pp. 253-257). IEEE.

[7]. Nakamoto, S., & Bitcoin, A. (2008). A peer-to-peer electronic cash system. Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf, 4(2).

[8]. Al-Shammari, N. K., Syed, T. H., & Syed, M. B. (2021). An Edge–IoT framework and prototype based on blockchain for smart healthcare applications. Engineering, Technology & Applied Science Research, 11(4), 7326-7331

[9]. Beck, R., Czepluch, J. S., Lollike, N., & Malone, S. (2016). Blockchain–the gateway to trust-free cryptographic transactions. In Twenty-Fourth European Conference on Information Systems (ECIS), İstanbul, Turkey, 2016 (pp. 1-14). Springer Publishing Company.

[10]. Yadav, A. S., & Kushwaha, D. S. (2021). Query Optimization in a Blockchain-Based Land Registry Management System. Ingénierie des Systèmes d Inf., 26(1), 13-21