iReplica : Counterfeit Product Detection System

B.Tech Project Report

Submitted by

Rahul Kurkure (20114079), Dheravath Vikas (20114033)
Kudikala Rishikesh (20114046)

for the fulfillment
of
CSN-400A: B.Tech. Project

Under the guidance of

Prof. Pradumn Kumar Pandey

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY ROORKEE

ROORKEE-247667

November 2023

Basic Outlines of the Report:

1. Front Pages
    a. Title page (Performa attached: Enclosure-1)
    b. Candidate's Declaration (Performa attached: Enclosure-2)
    c. Certificate (Performa attached: Enclosure-3)
2. Chapter-1 : Introduction to the Project
    a. The Problem Statement
    b. Introduction
    c. Theoretical Background
    d. Objectives
    e. Motivation
    f. Report outlines and organization
3. Chapter-2
    a. Literature Review
    b. Literature Review (with emphasis to current state-of-art)
    c. Research Gaps (with existing challenges)
    d. Problem Statement
4. Chapter-3
    a. Simulation Modelling/Algorithms/Techniques
    b. Flowcharts
    c. Proposed Algorithm
5. Chapter-4
    a. Results and Discussion
    b. Outcomes/Concluding remarks

6. Chapter-5

a. Conclusion
b. Limitations
c. Future Scope
d. Work done and future deliverables.

Enclosure-2

CANDIDATE’S DECLARATION

I declare that the work carried out in this report entitled “iReplica : Counterfeit Product Detection system” is presented on behalf of the fulfillment of the course CSN-400A submitted to the Department of Computer Science and Engineering, Indian Institute of Technology Roorkee under the supervision and guidance of Prof. Pradumn Kumar Pandey, Dept. of Computer Science and Engineering

I further certify that the work presented in this report has not been submitted anywhere for any kind of certification or award of any other degree/diploma.

Date: 14th November 2023

Place: IIT Roorkee

r. kurkure

Signature

(Rahul Kurkure, 20114079)

Rishikesh

Signature

(Rishikesh kudikala, 20114046)

Signature

(Vikas Dheravath, 20114033)

Enclosure-3

CERTIFICATE

This is to certify that the above statement made by the candidates is correct to the best of my knowledge and belief.

Date: 14th November 2023

Place: IIT Roorkee

(Signature of the Supervisor)

Chapter-1

1.1 Introduction

Suppose there is a person named Sam. He wants to buy a pair of shoes from Adidas, when he went to the market he saw various options, some shoes looked like an obvious copy whereas others looked more genuine. He bought one of genuine looking ones. He used them but after a week he saw that the inner sole of the shoe was starting to tear and that's when he realized that he had been indeed scammed with a counterfeit which he mistook to be a genuine pair. He got very upset. There are many people like Sam, across the globe who got scammed by the businesses believing that the product they are purchasing is real and authentic.

And there are companies such as Adidas, whose Product Reputation is getting damaged, and they are making losses due to people buying counterfeits in the market.

According to an Estimation, the losses which companies are facing due to their counterfeits is about $509 billion across the world in 2016.

To help manufacturers and consumers, We are designing our Project iReplica : A counterfeit Product Detection System. iReplica is a Complete System, Where the Users can Identify that the Product they are purchasing is genuine or not.

1.2 Problem Statement

In recent years, the proliferation of counterfeit products has become a major concern for consumers and businesses alike. Counterfeit products not only damage brand reputation but also pose serious health and safety risks to consumers. To combat this growing problem, a new technology called blockchain is being explored as a potential solution. Blockchain has the potential to create a tamper-proof and transparent system for tracking and verifying the authenticity of products throughout the supply chain. In this report, we will explore the concept of using blockchain for fake product detection and how it can help businesses and consumers alike.

1.3 Motivation

The motivation behind this idea is the need to address the growing problem of counterfeit products, which not only cause significant financial losses for businesses but also pose serious health and safety risks to consumers. Traditional methods for detecting and preventing counterfeit products have proven to be insufficient in the face of increasing sophistication of counterfeiters. Therefore, there is a pressing need for new technologies that can effectively combat this problem.

Blockchain technology has emerged as a promising solution [3] to the problem of counterfeit products due to its unique features such as transparency, immutability, and decentralized nature. However, the use of blockchain in the context of product verification is still in its early stages, and there is a need to evaluate its feasibility, benefits, and challenges. Therefore, this report aims to provide a comprehensive analysis of blockchain-based fake product detection systems to explore the potential solutions derived from this technology in combating the problem of counterfeit products.

1.4 Theoretical Background

Counterfeit products have been a persistent problem for businesses and consumers for many years. The rise of e-commerce and globalization has only exacerbated this issue. According to the Global Brand Counterfeiting Report, the value of counterfeit goods had reached a massive $1.82 trillion in 2020 and this value is only projected to grow further at a rapid rate. This growth is attributed to the increasing sophistication of counterfeiters and their ability to replicate products with high accuracy.

Traditionally, the methods for detecting counterfeit products have been limited to physical inspection and testing. However, these methods are time-consuming and costly, and they may not be effective in detecting sophisticated counterfeit products. In recent years, technology has emerged as a potential solution to this problem.

Blockchain, a decentralized digital ledger technology, has been gaining traction as a potential solution for tracking and verifying the authenticity of products. The unique features of blockchain, such as immutability and transparency, make it an ideal candidate for creating a tamper-proof system for product verification. By using blockchain, businesses can create a secure and transparent system for tracking the movement of products throughout the supply chain, making it easier to detect counterfeit products and prevent their circulation in the market.

1.5 Objectives

The objective behind this project is to explore the potential of blockchain technology in the detection and prevention of counterfeit products. Specifically, we will examine the benefits and challenges of using blockchain for product verification, the technical aspects of implementing a blockchain-based system, and the potential impact of such a system on businesses and consumers. The report aims to provide a comprehensive understanding of the role of blockchain in fake product detection and to evaluate its feasibility as a solution to the growing problem of counterfeit products.

1.6 Report outlines and organization

Within this report, we’ve presented recent research that has been done on the methodologies which are being put to use in our project, along with a basic understanding of those methodologies. At the current stage, we have a prototype of the project in working state. Simulations of said prototype have been described in brief and the inner workings of their said functions.

Descriptive flow charts have been used in our report to establish an improved understanding of the idea and how it would eventually work. We’ve concluded with results achieved till now. We’ve also set expectations for the upcoming work that is to be done on our project to make it fully operational.

Chapter-2

2.1 ERC 721

At the core of our solution, We are using ERC 721 tokens [1], ERC-721 tokens are unique digital tokens that represent ownership or proof of authenticity of a specific asset, such as artwork or collectibles. Each ERC-721 token has a unique identifier that is stored on the Ethereum blockchain, making it transparent and immutable. Once we have created the ERC tokens, we will assign the respective ownerships[9].

2.2 QR Code

QR codes were first developed in 1994 by the Japanese company Denso Wave, as a way to quickly and easily track vehicles during manufacturing. Since then, QR codes have become widely popular for a range of applications, including advertising, ticketing, payments, and inventory management.QR codes are generally considered to be secure, as they use built-in error correction to ensure that data can be accurately read even if the code is partially obscured or damaged[5].

Recent study published in the journal Sensors proposed a new algorithm for encoding data in QR codes using a hybrid genetic algorithm and shuffled frog-leaping algorithm, which resulted in higher efficiency and security compared to traditional encoding methods.

2.3 Research Gaps

While there has been significant research on the use of blockchain for fake product detection, there is still a lack of understanding regarding the scalability and efficiency of these systems. Most of the existing research has been conducted in controlled environments, with limited data and users. It remains unclear how these systems would perform when implemented at scale, with millions of users and vast amounts of data.

Therefore, there is a need to investigate the scalability and efficiency of blockchain-based fake product detection systems in a real-world setting. This research could include evaluating the performance of these systems in detecting and preventing the sale of fake products across multiple industries, such as fashion, electronics, and pharmaceuticals. The study could also examine the impact of various factors, such as network congestion and the number of users, on the effectiveness and efficiency of these systems.

2.4 Problem Statement

Blockchain has the potential to create robust systems to verify the authenticity of products throughout the supply chain. Through thorough research we’ve been able to identify a mechanism that uses blockchain at its core and application of QR’s to put a stop to the counterfeit market.

Chapter-3

3.1 Proposed Methodology

The Algorithm consists of mainly two phases but before that we need to know some prerequisite about metamask wallets to better understand the phases of the algorithm.

3.1.1 Metamask Wallet

MetaMask allows users to store and manage account keys, broadcast transactions, send and receive Ethereum-based cryptocurrencies and tokens, and securely connect to decentralized applications through a compatible web browser or the mobile app's built-in browser. It is very similar to the E-wallets we use in current times for eg: Google Pay.

Points to Note : Every User has his unique metamask wallet address.

When a seller logs in to our site through metamask, our system will have his wallet's address. We will use this seller's wallet address as one of the key factors to identify the true owner of the product.

3.1.2 Product Registration

Firstly the manufacturer has to register his targeted product for which is to be prevented from counterfeiting.

Steps of Registration

1. Manufacturer will have to Log in through his metamask account once he logs in through it, we will have his metamask wallet address.
2. We will start from product id = 1, and increment this after every new product registration, to always get a new product id.
3. Using this Product ID as input we will generate a unique ERC token, this token is stored on Ethereum Blockchain. This Ethereum blockchain stores the history of ownership of the given Token, that means we can track all the past owners and the current owner of the given token.
4. Using the Token ID as key we will generate a hash which will be embedded on the product.
5. We will map this hash with the token ID and store this in the database.
6. Then a single object with attributes like Product ID, Token ID, Token Hash,Product type will be stored in a centralized database. With Token Hash as Primary Key.

3.1.3 Product Verification

After Product after Registration we need to cross-verify the product from the consumers end using a decentralized ERC token from block.

Steps of Product Verification

1. Firstly the user who claims to own the product should log in through his metamask wallet, now we have the metamask wallet address.
2. We will scan the product image, then get the token hash.
3. Using this token hash we will fetch the token ID, from our database[8].

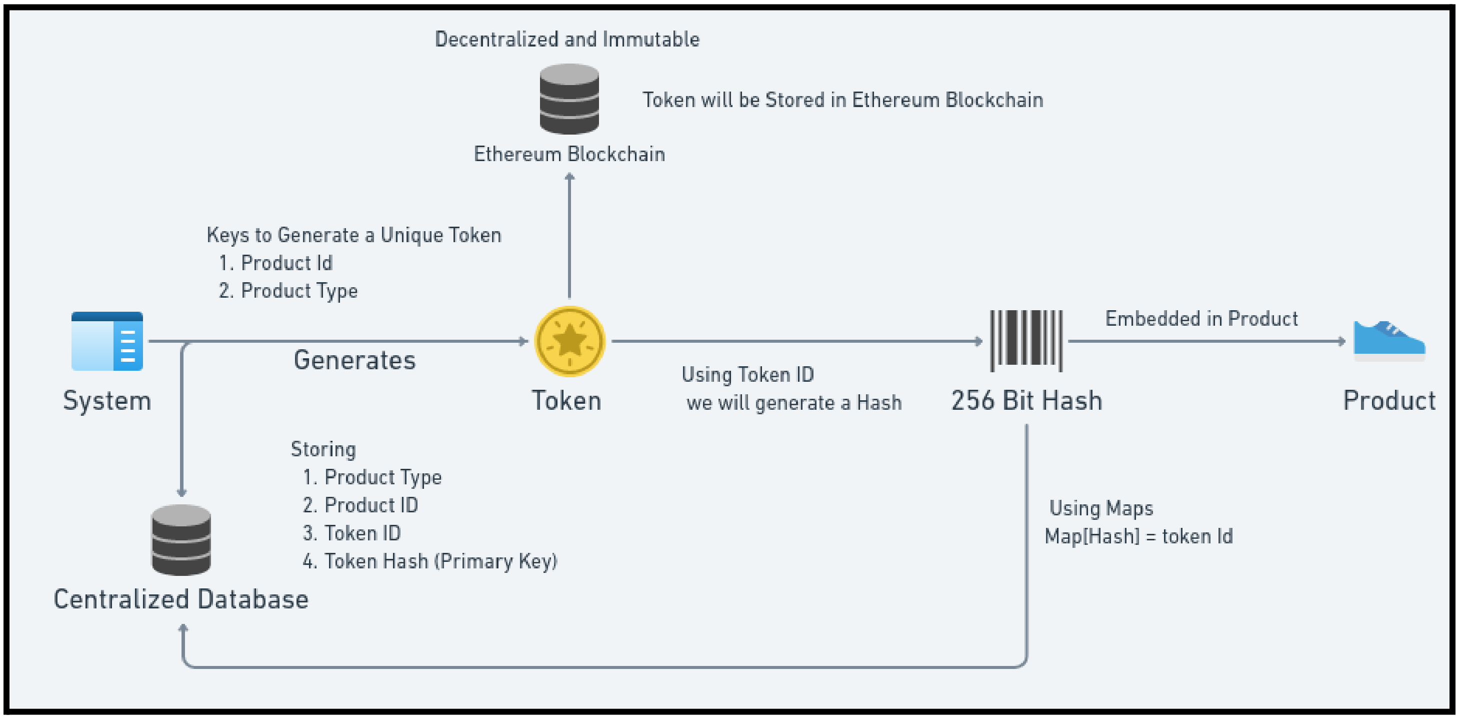
4. Through this Token ID we will fetch, History of all the owners of the product and the address of current owner of the product from the Blockchain.
5. Now we will compare the User's wallet address(step 1) and Owner's wallet address(step 3) if both the address matches then the User is The REAL OWNER of the product.

3.1.4 Security

Even if someone copies our hash embedded in the product, when it comes to selling the product or showing it to someone, his metamask wallet address will be different and hence he can't prove that his product copy is valid.

3.1.5 The Flow Charts

Product Registration : Manufacturer to Register the targeted product



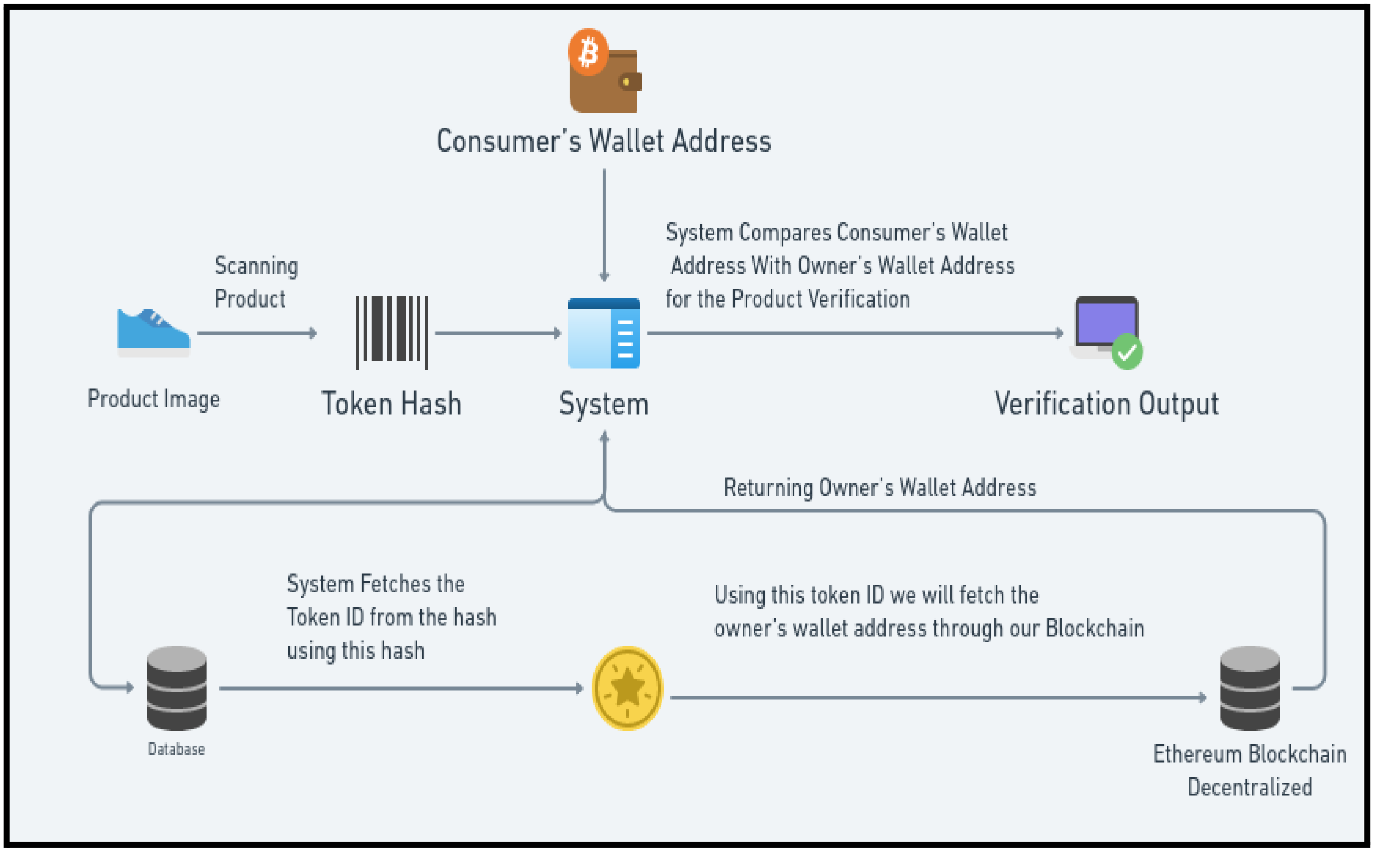
Here the System generates a ERC 721 Token and using that token id, the system generates a 256 bit Hash, which is supposed to be embedded with a QR-link on the product.

The ERC 721 Token here is stored in Ethereum Blockchain (Decentralized Blockchain).

All the information, along with token Id we will be stored on a Centralized server to give the meta-data of the product.

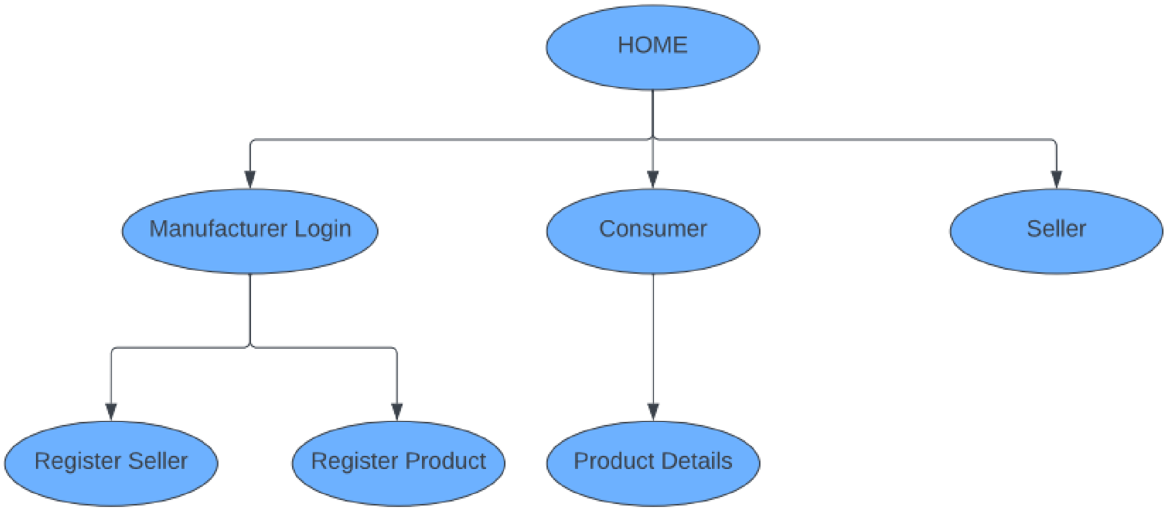
And the 256 Bit Hash here will be embedded on the product.

Product Verification : Consumer’s Point of view


Consumer’s Wallet Address
Scanning Product
System Compares Consumer's Wallet Address With Owner's Wallet Address for the Product Verification
Product Image
Token Hash
System
Verification Output
Returning Owner's Wallet Address
System Fetches the Token ID from the hash using this hash
Using this token ID we will fetch the owner's wallet address through our Blockchain
Database
Ethereum Blockchain Decentralized

These are the required flow charts based on the algorithm.

Here the Product Image will be scanned, and the QR code along with token Hash will be extracted from the image and passed to the system. On getting the token hash, our system will give its respective token id, and with the help of this token id, we will be able to get the wallet address of the actual owner of the product. And through the actual owner of the product we will get the seller id and all seller information.



Chapter-4

4.1 Results and Discussion

Following the research we did in our duration on the project, we've now ended with a stern solution to the counterfeit problem.
The current algorithm helps us to detect fake products, that said, we've noticed multiple workarounds to counterfeit a product, which are able to pass our 1st iteration of the solution. Following includes some of the discussion we've had surrounding the issues and potential solutions:

1. The Seller is selling a counterfeit product, with a different hashcode of the product which is not stored in the blockchain, this can be detected as that hash code could not be fetched by database.
2. In context 1st point, if the hash codes will be the same, it will be fetched from the database but to sell the product to the consumer, his metamask address should be matched with the owner's wallet address, which is not possible as metamask wallet addresses are always unique.
3. If the seller has copied the hash and he owns the product too, and tries to sell a counterfeit with the same hash code, we will set a verified sellers section, that needs to be sure that the seller who is selling our product is genuine.

4.2 Concluding remarks

Working on a Security algorithm so that no one can copy our product as this problem is very big. It is supposed to take a sufficient amount of time and work to ensure the security of our product. This is still undergoing as there exists some loopholes in the algorithm.

All we had to do was reduce the expenses of using the blockchain as we know distributed peer to peer networks require a lot of computing power and hence we have to use blockchain efficiently by using minimal resources. So we learned how to use blockchain smart contracts efficiently to minimize expenses.

Learned Standard Blockchain Concepts which tell us how blockchain is secure. Learned Solidity Language to write smart contracts for generating ERC-721 tokens and verifying token ownership. After Improving the algorithm we had started the coding phase of our project too. We had Coded the Basic API for the product registration and verification. Then we had coded the Smart Contract and the deployment which will be used for generating the ERC token will be used to check the ownership of the product.

Chapter-5

Conclusion

5.1 Conclusion

We have Concluded our algorithm and started our coding phase, the Basic API for Registration Protocol and Frontend has been created and the Smart Contracts code is also completed.

5.2 Limitations

People's sentiment towards metamask wallet, Though metamask wallet is a must have in terms of cryptocurrency and trading or simply logging to a market place or to make a transaction, but depending on the users who want to buy a product, might not be using any crypto wallets, but to buy expensive products, and be sure that their product is genuine, it can be a good reason to use these wallets.

5.3 Future Scope

There can be many possibilities depending on the exploration of new counterfeiting methods. And Additionally we can

provide further features which ensure a some special case like online payments etc. or Supply Chain management

5.3.1 Product Ownership Transfer Mechanism for Online transactions.

When selling the product from manufacturer to the consumer we will transfer the ownership from manufacturer's side to consumer.

5.3.2 History of Owners Feature

We can use this feature to sell the products which are related to the owner of the product. Eg: Lebron James's Sneakers, Cristiano Ronaldo's Shoes, are sold heavily in the market in the name that these players had used those products.

5.4 Work Done Till Now

Working on a Security algorithm so that no one can copy our product as this problem is very big. It is supposed to take a sufficient amount of time and work to ensure the security of our product. This is still undergoing as there exists some loopholes in the algorithm.
Learned working of IPFS and Standard Blockchain Concepts which tell us how blockchain is secure.
Learned Solidity Language to write smart contracts for generating ERC-721 tokens and verifying token ownership.
After Improving the algorithm we started the coding phase of our project.
The Basic API for the product registration and verification has been implemented along with the login-through-metamask feature.
Then we had coded the Smart Contract and the deployment which will be used for generating the ERC token will be used to check the ownership of the product.
Along with the aforementioned, we've also implemented a basic frontend for our web-app.

5.5 Work to be Done

As of now, we are going per the initial plan to implement the core algorithm and coding the rest according to that. Following are a set of deliverables set for the next session:

- Code the Verification algorithm as mentioned above.
- We’ll need to integrate our frontend with our backend.
- Embedding Technique for Embedding the digital signature on our product.
- Scanner for Scanning the digital signature from the product.

References

[1] Bauer, D. P. (2022). ERC-721 Nonfungible Tokens. In *Getting Started with Ethereum: A Step-by-Step Guide to Becoming a Blockchain Developer* (pp. 55-74). Berkeley, CA: Apress.

[2] Lavanya, P. M., Ananthi, N., Kumaran, K., Abinaya, M., Kalaivani, B., Krithika, V., & Rahul, S. S. (2021, December). Fake Product Detection using Blockchain. In *2021 4th International Conference on Computing and Communications Technologies (ICCCT)* (pp. 133-137). IEEE.

[3] 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.

[4] Bauer, D. P. (2022). ERC-721 Nonfungible Tokens. In *Getting Started with Ethereum: A Step-by-Step Guide to Becoming a Blockchain Developer* (pp. 55-74). Berkeley, CA: Apress.

[5] Krombholz, K., Frühwirt, P., Kieseberg, P., Kapsalis, I., Huber, M., & Weippl, E. (2014). QR code security: A survey of attacks and challenges for usable security. In *Human Aspects of Information Security, Privacy, and Trust: Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014. Proceedings 2* (pp. 79-90). Springer International Publishing.

[6] Syed, T. A., Alzahrani, A., Jan, S., Siddiqui, M. S., Nadeem, A., & Alghamdi, T. (2019). A comparative analysis of blockchain architecture and its applications: Problems and recommendations. *IEEE access*, *7*, 176838-176869.

[7] Cachin, C. (2016, July). Architecture of the hyperledger blockchain fabric. In *Workshop on distributed cryptocurrencies and consensus ledgers* (Vol. 310, No. 4, pp. 1-4).

[8] Truica, C. O., Radulescu, F., Boicea, A., & Bucur, I. (2015, May). Performance evaluation for CRUD operations in asynchronously replicated document oriented database. In *2015 20th International Conference on Control Systems and Computer Science* (pp. 191-196). IEEE.

[9] Koirala, R. C., Dahal, K., & Matalonga, S. (2019, January). Supply chain using smart contract: a blockchain enabled model with traceability and ownership management. In *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 538-544). IEEE.