Fake Product Identification using Blockchain Technology

G. Neeraj[1], D. Rahul[2], P. Anurag[3], V. Pranav[4]

[1] Graduate, Dept. of Computer Science Engineering, Matrusri Engineering College, Telangana, India
[2] Graduate, Dept. of Electronics and Communication Engineering, Sreenidhi Institute of Science and Technology, Telangana, India
[3] Graduate, Dept. of Computer Science Engineering, Matrusri Engineering College, Telangana, India
[4] Graduate, Dept. of Computer Science Engineering, Matrusri Engineering College, Telangana, India

Abstract - *Counterfeit products have been quickly expanding in recent years, as we all know. Counterfeiting is a global problem that affects social and economic growth worldwide, accounting for 3.3% of global commerce, according to OECD figures. These items are sometimes referred to as "first copies," and they can be marketed in place of original products. We have various online purchasing platforms such as Flipkart, Amazon, and others where customers buy things, which are then sent by the manufacturer and delivered to the consumer. However, many third parties are engaged in the process between manufacturing and delivery, such as warehouses. Because these third parties are engaged, unlawful product tampering may occur, resulting in losses for both the corporation and the customer. The primary goal of this project is to identify counterfeit items and ensure efficient product delivery processes. Counterfeiting may be dangerous in some businesses, such as the medical industry, thus identifying counterfeit items and stopping them from being sold is critical. A blockchain is a decentralized ledger that records all peer-to-peer transactions. Participants can confirm transactions without the requirement for a centralized authority using this technology. Fund transfers, trade settlement, voting, and a variety of other challenges are all possible uses. We are attempting to introduce this immutable technology to identify counterfeit products in this project. QR codes are also used to store hash codes and determine their authenticity.*

Key Words: **Blockchain, QR codes, Fake Products, Tamper, Ledger**

1. INTRODUCTION

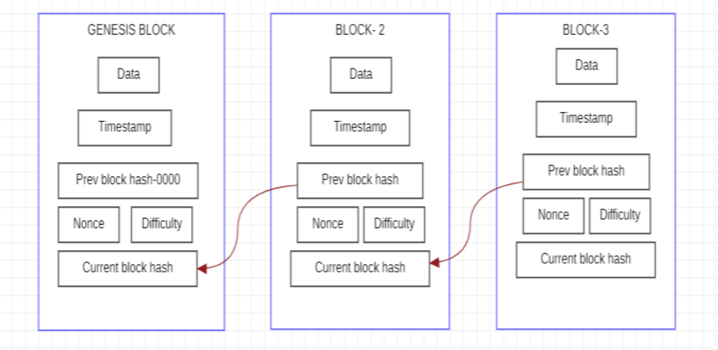
Fake products have a significant detrimental influence on the market for both consumers and sellers. The sellers fail to provide the goods as per the buyers' expectations, and the consumers begin to suspect the company's quality and standards, resulting in poor marketing of the brand whose counterfeit items are being distributed in the market. The most dangerous aspect of counterfeit items is that they may be extremely detrimental to users. Because fake or counterfeit items are not limited to any single area of the market, we must recognize these products and find a strategy to keep them out of the market. When we examine dominating sectors like pharmaceuticals and food supplies, these items may be quite risky. To address such issues, we must retain data that is freely available to customers, allowing them to check product details and establish a level of trust in the product's legitimacy. Counterfeit items must be identified in the supply chain since, in the pharmaceutical industry, if this is not done, the customer may be put at grave risk.

To avoid this, we are employing blockchain technology, which is immutable and decentralized and may be very useful in detecting fake products. If a third party is involved in tampering with the data, we can easily identify it using this technology. We also implemented a QR code that the consumer scans to evaluate if the product is genuine or counterfeit.

1.1 Blockchain:

A blockchain is a continual record, known as a block, that is cryptographically linked together. A cryptographic hash of the preceding block, a timestamp, and transaction data are all included in each block. The timestamp verifies that the transaction data existed at the moment the block was released, allowing the hash to be calculated. Because each block contains information about the one before it, they create a chain, with each new block strengthening the preceding ones.

As a result, blockchains are resistant to data tampering since the data in any one block, once recorded, cannot be changed retrospectively without affecting all subsequent blocks.



2. METHODOLOGY

This project is primarily separated into two modules:

1) Manufacturer

2)Consumer/user

After logging in, the manufacturer will input product data such as product id, name, and company name. The information entered by the manufacturer is saved in blocks. The SHA-256 algorithm is used to generate the hash code when this information is included. This hash code is used to generate a QR code, which is printed on the merchandise. The user will receive this QR code after purchasing the product, which he may scan with a web camera or a QR-code scanner that was previously imported.

If the hash code within the blockchain and the hash code generated after scanning is the same, the product is considered to be original, and the consumer will be presented with product data otherwise, it detects that the product is counterfeit.

This way, we'll know where the product was tampered with and who was accountable.

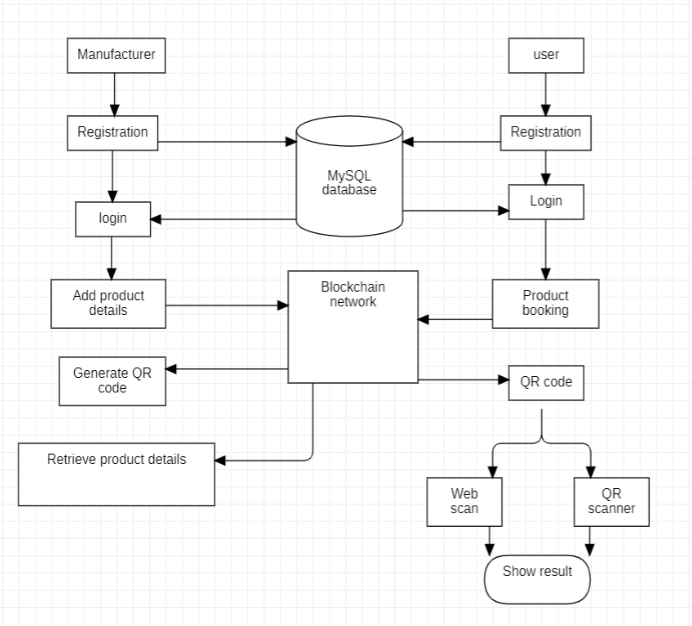


Fig.1 System Architecture Diagram

We have implemented our project using python, Tkinter as UI, MySQL database and XAMPP local server.

We have implemented blockchain using the following steps:

- The information will be saved in the JSON format, which is characterised by its simplicity both in terms of its implementation and its readability. A block is used to store the data, and inside that block are numerous copies of the data. Every minute, many blocks are added, and to distinguish one from the other, we will use fingerprinting to distinguish between them.
- This process is carried out using hash, and the SHA256 hashing method will be used in particular for this purpose. Every block will have its unique hash, as well as the hash of the function that came before it, making it impossible for the data to be manipulated.
- Current block hash will be the previous hash for the next block and so on this way blocks are connected to form a chain

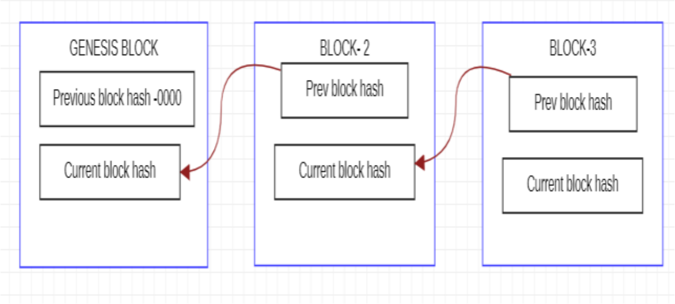


Fig.2 Chaining of Blocks in Blockchain

- Proof of work method is included, making it way more difficult to perform operations to create a new block and add it to the chain. This indicates that anybody who edits a prior block will need to repeat the work associated with that block as well as the work associated with all of the blocks that follow it. We can restrict it furthermore by increasing the difficulty associated with creating blocks.

List of important libraries imported:

Libraries required for UI:

from Tkinter import message box

from tkinter import *

from tkinter import simpledialog

import tkinter

from tkinter import filedialog

from tkinter.filedialog

import askopenfilename

Importing blockchain and block files:

from Block import *

from Blockchain import *

Importing SHA-256 for hashing:

from hashlib import sha256

Importing functions related to QR-code:

import qrcode

import qrtools

3. RESULTS:

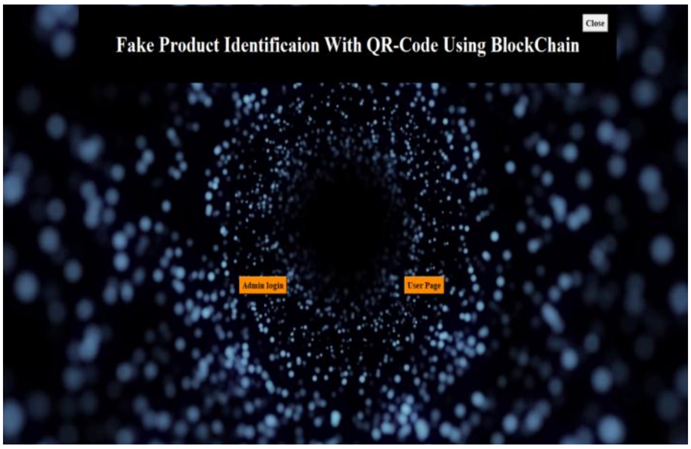


Fig.3 Output Module

This is the main module, where u get two modules included. i.e., Admin module and user module

3.1 Admin Module

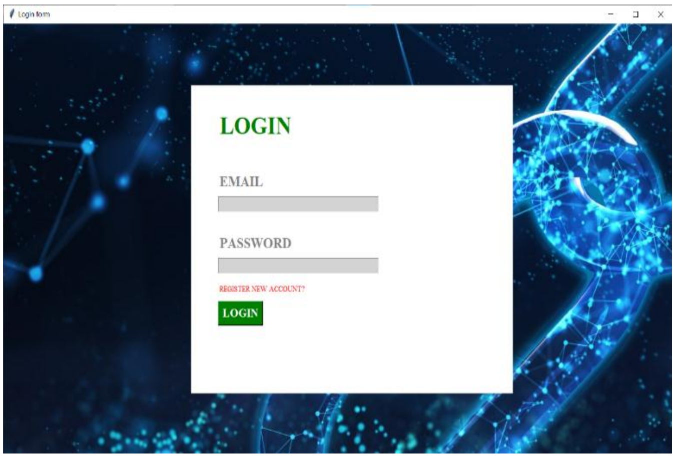


Fig:3.1.1-Admin Module

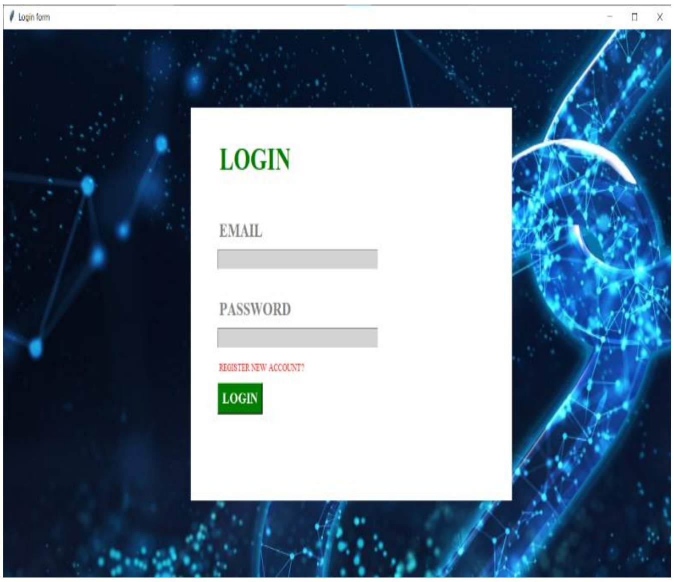


Fig 3.1.2 Login Page

- Before getting into the admin module, u need to log in with valid credentials.
- If you have not registered before then u can register yourself with valid proofs!

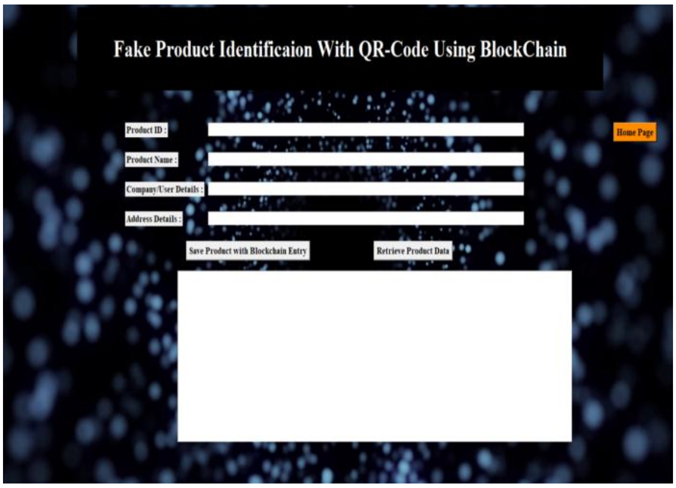
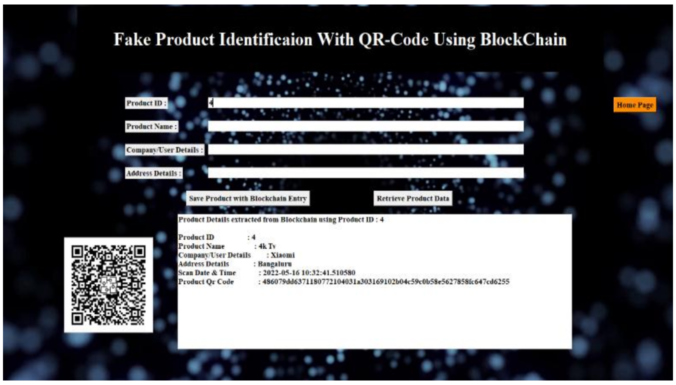


Fig 3.1.3 Information Page

After login, u get into the admin module w you(the manufacturer) add the product details with a unique product ID. This information is stored in a single block and that block adds up to the existing blockchain.



Product ID : 4

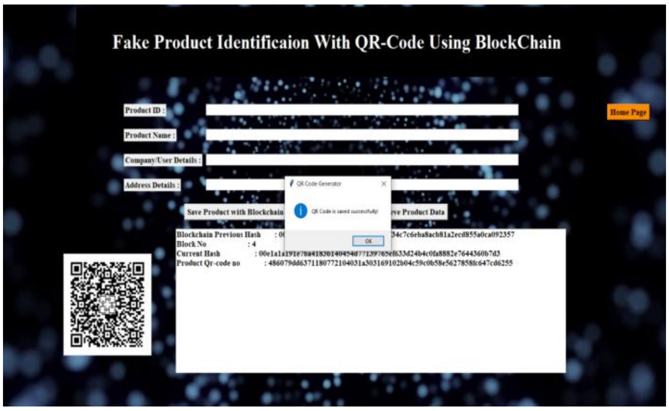
```
Product Details extracted from Blockchain using Product ID : 4

Product ID           : 4
Product Name         : 4k Tv
Company/User Details : Xiaomi
Address Details      : Bangaluru
Scan Date & Time     : 2022-05-16 10:32:41.510580
Product Qr Code      : 486079dd6371180772104031a303169102b04c59c0b58e5627858fc647cd6255
```

Fig 3.1.4

After adding the product details by the manufacturer in the admin module, a respected QR code is generated and stored in the local system and also displayed on the module screen.

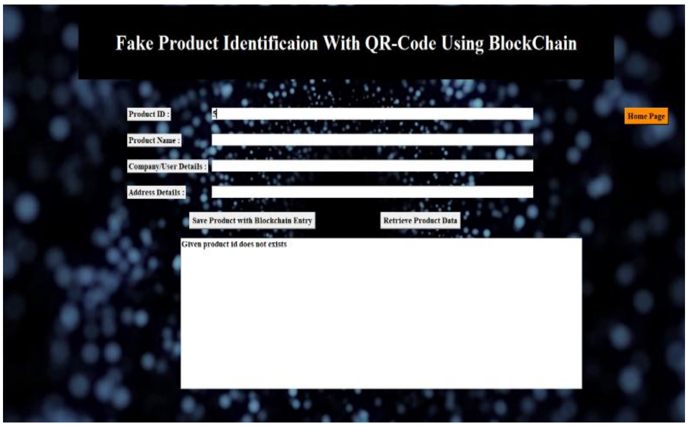
This QR code is nothing but the hash of the product block which is added to the blockchain.



QR Code is saved successfully!

```
Blockchain Previous Hash   : 0(                34c7c6eba8acb81a2ecd855a0ca092357
Block No                   : 4
Current Hash               : 00e1a1a191e78a41836140454d77139765ef633d24b4c0fa8882e7644360b7d3
Product Qr-code no         : 486079dd6371180772104031a303169102b04c59c0b58e5627858fc647cd6255
```

Fig 3.1.5



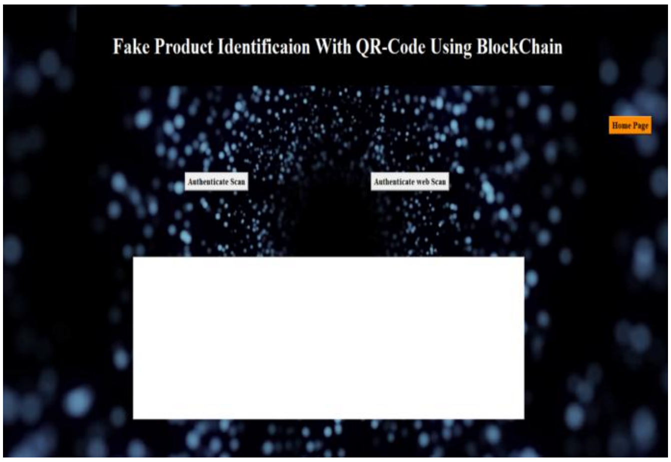
Given product id does not exists

Fig 3.1.6

We can also retrieve the data using ProductID from the blockchain in the Admin module.

- Fig 3.1.5 - When we retrieve the valid ProductID, we get the details with the respected QR code displayed on the screen.
- Fig 3.1.6 - If we try to retrieve with fake ProductID, then we get an error saying that the given product ID doesn't exist.

3.2 User Module



After the product is added to the blockchain, the user can use the user module to validate the product with a QR code!!

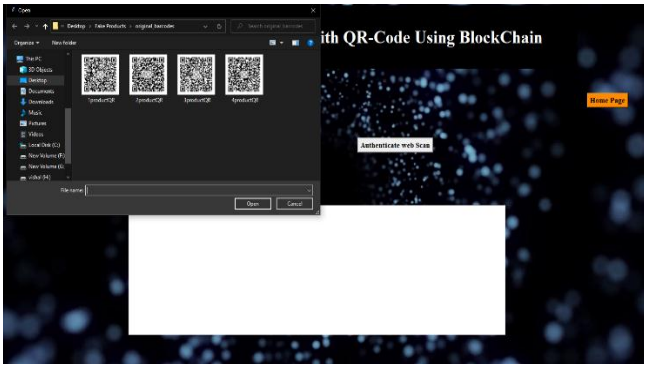
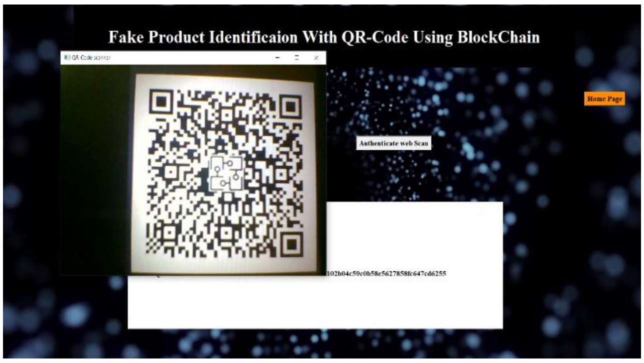


Fig-3.2.1

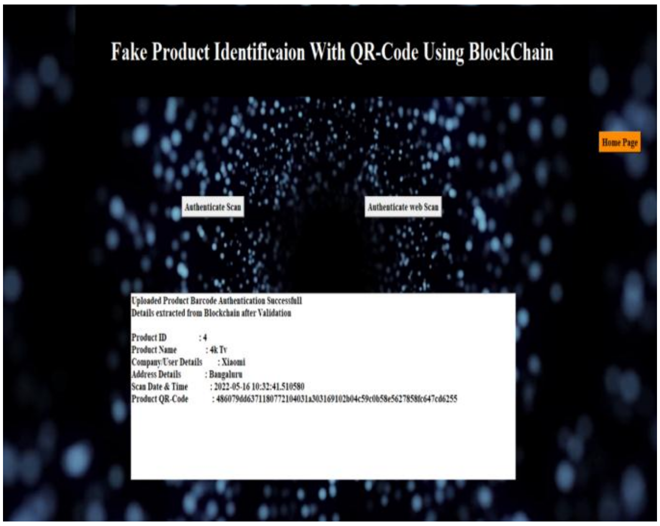


102b04c59c0b58e5627858fc647cd6255

Fig 3.2.2

Here we have two ways to Authenticate the product with a QR code!

- Fig 3.2.1 - Using the system stored QR codes
- Fig 3.2.2 - Using the webcam/camera to scan the QR codes


Fake Product Identificaion With QR-Code Using BlockChain

Uploaded Product Barcode Authentication Successfull
Details extracted from Blockchain after Validation

```
Product ID              : 4
Product Name            : 4k Tv
Company/User Details    : Xiaomi
Address Details         : Bangaluru
Scan Date & Time        : 2022-05-16 10:32:41.510580
Product QR-Code         : 486079dd63711807721040311a303169102b04c59c0b58e5627858fc647cd6255
```

Fig – 3.2.3

If the Validation was successful, then the details gonna retrieve from the blockchain and displayed in the module.

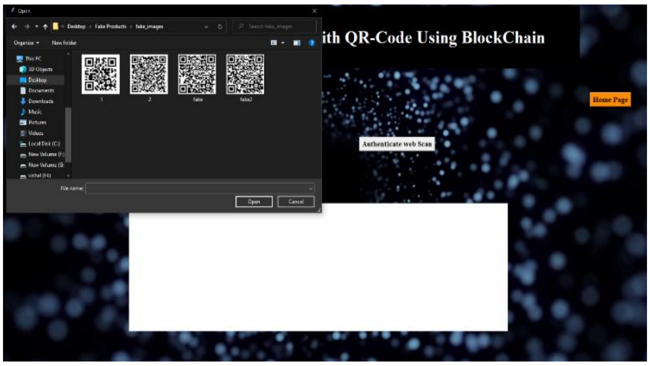
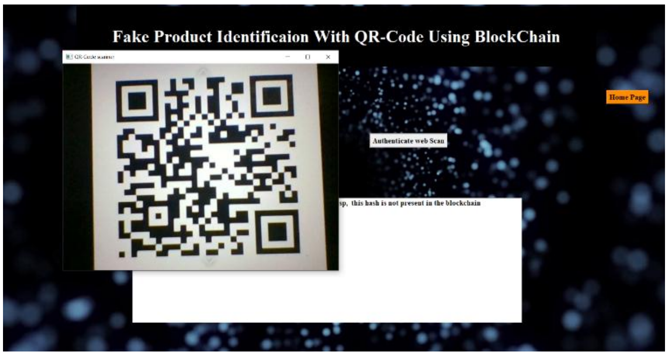

ith QR-Code Using BlockChain

Fig-3.2.4

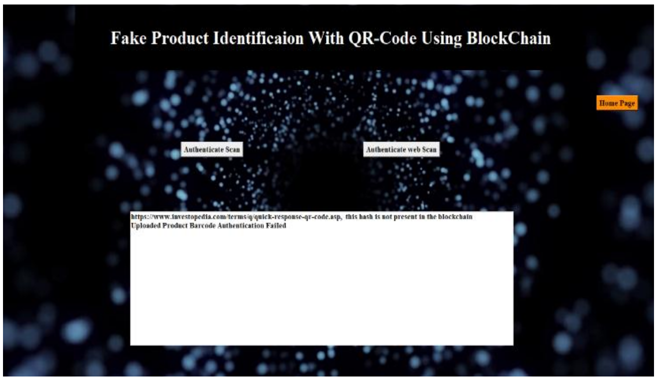

Fake Product Identificaion With QR-Code Using BlockChain

sp, this hash is not present in the blockchain

Fig – 3.2.5

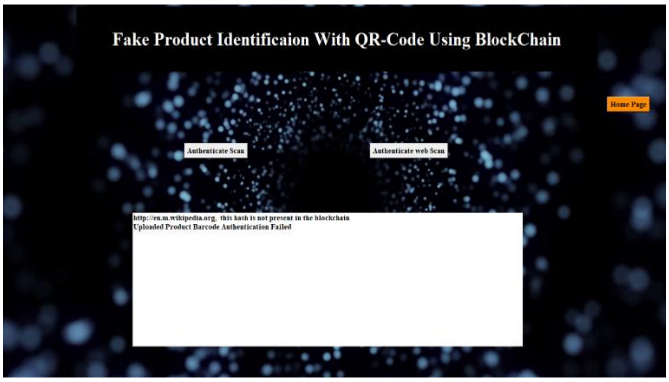
If we try to validate with the fake QR codes

- Fig 3.2.4 - Validating with a fake QR code which is stored in the system.
- Fig 3.2.5 - Validating the fake QR code with the Webcam/camera


Fake Product Identificaion With QR-Code Using BlockChain

https://www.investopedia.com/terms/q/quick-response-qr-code.asp, this hash is not present in the blockchain
Uploaded Product Barcode Authentication Failed

Fig 3.2.6


Fake Product Identificaion With QR-Code Using BlockChain

http://en.m.wikipedia.org, this hash is not present in the blockchain
Uploaded Product Barcode Authentication Failed

Fig 3.2.7

Then we get the result that the hash is not present in the blockchain with the data in that QR code respectively.

- Fig 3.2.6 - Validating with fake QR code we got the respected data present in the QR code (i.e., website called Investopedia) and also an error, as the hash is not present in the blockchain.
- Fig 3.2.7-Validating the fake QR code with the Webcam/camera code we got the respected data present in the QR code (i.e., a website called Wikipedia) and also an error as the hash is not present in the blockchain.

4. CONCLUSION:

With the use of this technology, the path that a product takes from the factory to the end user may be documented, and the user would have the peace of mind of knowing that the scans were not falsified. The manufacturer can demonstrate that their product is genuine and is also in a position to trace the course of the product. The configuration is simple to build and uses fewer references to keep running. It is very important to implement this product in health-related markets to prevent fraudsters from producing harmful products that can be harmful.

5. REFERENCES:

[1] Satoshi Nakamoto, ―Bitcoin: A Peer-to-Peer Electronic Cash System‖, 2008

[2] Hyperledger, ―Hyperledger Blockchain Performance Metrics‖, V1.01, October 2018

[3] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[4] Armin Ronacher, ―Flask Docs‖, http://flask.pocoo.org/docs/‖

[5] G. Wood, ‗Ethereum: A secure decentralised generalized transaction ledger,'' Tech. Rep., 2014.

[6] OECD (2016), Illicit Trade: Converging Criminal Networks, OECD Reviews of Risk Management Policies, OECDPublishing,Paris,https://doi.org/10.1787/9789264251847-en.

[7] M. Castro and B. Liskov, ‗Practical byzantine fault tolerance and proactive recovery,'' ACM Trans. Comput. Syst., vol. 20, no. 4, pp. 398–461, Nov. 2002.

[8] Clement, E. Wong, L. Alvisi, M. Dahlin, and M. Marchetti, ‗Making byzantine fault tolerant systems tolerate byzantine faults,'' in Proc. 6th USENIX Symp. Netw. Syst. Design Implement., 2009, pp. 153–168.

[9] Cachin, ‗Architecture of the hyper ledger blockchain fabric,'' Tech. Rep., Jul. 2016.

[10] S. Underwood, ―Blockchain Beyond Bitcoin‖, in Communications of the ACM, vol. 59, no. 11, p. 15-17, 2016.

[11] Deloitte, Israel: A Hotspot for Blockchain Innovation, 2016.[Online].Available: https://www2.deloitte.com/content/dam/ Deloitte/il/Documents/financial-services/israel_a_hotspot_for_blockchain_innovation_ feb2016_1.1.pdf. [Accessed: 2.11.2016].

[12] G. Greenspan and M. Zehavi, Will Provenance Be the Blockchain‗s Break Out Use Case in 2016? 7.1.2016. [Online]. Available: http://www.coindesk.com/ provenance-blockchain-tech-app/. [Accessed: 12.12.2016].

[13] Counterfeit medicines. QA counterfeit. World Health Organization (WHO) 2009. Available from: http://www.who.int/medicines/ services/counterfeit/faqs/QACounterfeit-october2009.pdf [last cited on 2010 Jun 12].

BIOGRAPHIES

G . Neeraj is a Computer Science Graduate student from Matrusri Engineering College. After Graduation, he is working as Machine Learning Engineer at Quantiphi, Bengaluru, India

Deevanapalli Rahul is an Electronics and Communication Engineering Graduate Student from Sreenidhi Institute of Science and Technology, Hyderabad, Telangana.

Pittala Anurag Sharma is a Computer Science Graduate student from Matrusri Engineering College. After Graduation, he is working at HSBC as a Software Engineer, in Pune, India.

Pranav Vuppala is a Computer Science Graduate student from Matrusri Engineering College. After Graduation, He is working as an Assistant Graduate System engineer trainee at Tata consultancy services, Hyderabad, India.