International Journal of All Research Education and Scientific Methods (IJARESM), ISSN: 2455-6211
Volume 10, Issue 6, June-2022, Impact Factor: 7.429, Available online at: www.ijaresm.com

Authentication of Product and Counterfeits Elimination Using Blockchain

Ms. K. Shirisha[1], Ms. S Navya Akshitha[2], Ms. Sk. Nasreen[3]

Department of Computer Science & Engineering, Mahatma Gandhi Institute of Technology-Hyderabad,
Affiliated to JNTUH, India

---*****************---

ABSTRACT

Blockchain technologies have gained interest over the last years. While the most explored use case is financial transactions, it has the capability to agitate other markets. Blockchain remove the need for trusted intermediaries, can facilitate faster transactions and add more transparency. It explores the possibility to deflate counterfeit using blockchain technology. It provides an overview of different solutions in the anti-counterfeit area, different blockchain technologies and what characteristics make blockchain especially interesting for the use case. We have developed three different concepts and the expansion of an existing system concept, is pursued further. It is shown, that reducing counterfeits cannot be achieved by using technological means only. Increasing awareness, fighting counterfeiters on a legal level, a good alert system, and having tamper-proof packaging are all important aspects. These factors combined with blockchain technology can lead to an efficient and comprehensive approach to reduce counterfeiting

Keywords – Authentication, Blockchain, Encrypt

I.INTRODUCTION

Authentication, the act of establishing or conforming something as genuine. Authentication is of utmost importance because the use of counterfeit medicines can be harmful to the health and wellbeing of the patients. Their use may result in treatment failure or even death. Authentication is generally done through the overt or covert features upon the product. We now have more fakes than real drugs in the market.Christophe Zimmermann, the anti-counterfeiting and piracy coordinator of the World Customs Organization. Current anti-counterfeiting supply chains rely on a centralized authority to combat counterfeit products.Blockchain technology has emerged to provide a promising solution for such issues. In this paper, we propose the block-supply chain, a new decentralized supply chain that detects counterfeiting attacks using blockchain and Near Field Communication (NFC) technologies. Block-supply chain replaces the centralized supply chain design and utilizes a new proposed consensus protocol that is, unlike existing protocols, fully decentralized and balances between efficiency and security.

II.LITERATURE SURVEY

“Elimination of Counterfeit Products using Blockchain” is developed by Dr. J. Satheesh Kumar,G.Praveen, M. Kesavan, D. Naveen. It was published in 2021.They have usedKeccak256 algorithm. The problem with this approach was it no longer feasible and complex and difficult to audit.[1]

“Counterfeited Product Identification in a Supply Chain using Blockchain Technology” is developed by Shivam Singh, Gaurav Choudhary. It was published in 2020.They have used PBFT algorithm.The approach had the drawbacks that it was Scaling, due to its documentation overhead.[2]

“Fake Product Identification Using Blockchain Technology” is developed by Tarannum J. Sayyad It was published in 2019. They have used DPos consensus. The problem with this approach was hard to maintain, Centralisation due to low participation.[3]

“Managing the Product-Counterfeiting Problem with a Blockchain-Supported E-Commerce Platform” is developed byJi Jiang and Jin Chen.It was published in 2018. They have used Consensus Algorithm. The approach had the drawbacks that it requires high-capacity costs and low reliability.[4]

“A Peer-to-Peer Electronic Cash System” is developed by Satoshi Nakamoto.It was published in 2018.Without passing via a banking institution, a peer-to-peer version of electronic cash would allow internet payments to be transmitted directly from one party to another. Digital signatures are part of the solution, but if a trusted third party is still required to avoid double-spending, the major benefits are lost. Using a peer-to-peer network, we suggest a solution to the double-spending problem. Transactions are hashed into an ongoing chain of hash-based proof-of-work on the network, establishing a record that cannot be modified without redoing the proof-of-work. The longest chain not only proves the sequence of events, but it also proves that it came from the most powerful pool of CPU power. As long as nodes that are not cooperating to attack the network hold the bulk of CPU power, they will produce the longest chain and overtake attackers. [5]

III. PROPOSED SYSTEM & APPROACHED ARCHITECTURE

Blockchain technology does not require the engagement of a third party, and verification will be carried out by a software algorithm without the need for a third party. To avoid forging counterfeits, we are converting all product details/barcodes into digital signatures, which will be stored in a Blockchain server, which supports tamperproof data storage, meaning that no one can hack or alter its data, and if its data is altered by chance, verification will fail at the next block storage, and the user will be notified. In Blockchain technology, the same transaction data is saved on many servers with hash code verification, and if the data on one server changes, it will be noticed on the other servers since the hash code for the same data would change.

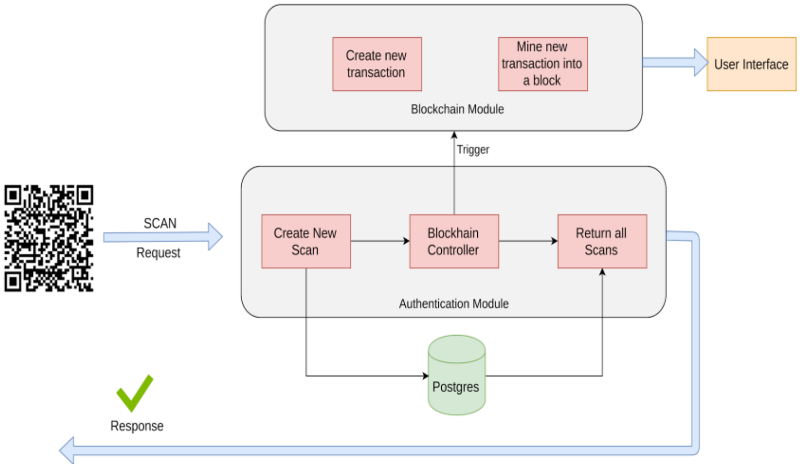


Fig.1. General workflow of the Application.

SYSTEM ARCHITECHTURE:

In Blockchain each data will be stored by verifying old hash codes and if old hash codes remain unchanged then data will be considered as original and unchanged and then new transaction data will be appended to Blockchain as new block. For each new data storage all blocks hash code will be verified.Service that sits between the Blockchain module and the user. It handles the product data and can create product transactions in database & blockchain, initiate new block creation, retrieve product data, authenticate scans and notify if genuine. Figure.1 Demonstrates the system architecture of the proposed system.

REQUIRED LIBRARIES IN PROPOSED WORK

Python

Python is a general programming language, interpreted, high-level. With its noticeable use of important whitespace, Python's design philosophy emphasizes code readability. Its structures of the language and object-oriented approach are intended to allow programmers to write simple, logical code for large and small projects. Python is collected with complex typing and garbage. It supports several paradigms of programming, including method, object, and functional programming. Because of its robust standard library, Python is often defined as "batteries including".

Tensor Flow

TensorFlow is a free and open-source software library for dataflow and differentiable programming across a range of tasks. It is a symbolic math library, and is also used for machine learning applications such as neural networks. It is used for both research and production at Google. TensorFlow was developed by the Google Brain team for internal Google use. It was released under the Apache 2.0 open-source license on November 9, 2015.

Numpy

NumPy is a library for the Python programming language that supports large, multi-dimensional arrays and matrices, as well as a large group of high-level mathematical functions. It aims at Python, a non-optimizing byte code interpreter C Python,'s reference implementation. For this edition of Python, the mathematical algorithms are always slower than those that have been compiled.

SkLearn

Scikit-learn is a Python programming free software learning machine (formerly Scikits.learnand also known as sklearn). The libraries NumPy and SciPy in Python have been developed to deal with different classification algorithms, regression and clustering, including vector machines, random forests, gradient boosts, K-means and DBSCAN.

Matplotlib

Matplotlib is a Python programming library and its NumPy extension of numeric mathematics. It offers the object-oriented API for integrating plots into applications using GUI-toolkits for general purposes such as Tkinter, wxPython, Qt or GTK+. A procedural pylab interface based on a state machine is also available (such as OpenGL), which closely resembles MATLAB but discourages its use.

PROJECT FEATURES

Modules:
We created the following modules for this project.

1) Save Product with Blockchain Entry: In this module, the user enters product details, then uploads a product barcode image, generates a digital signature on the barcode, and finally saves the transaction details in Blockchain. Before storing a transaction, Blockchain will validate all previous transactions, and if they pass, a new transaction block will be created.

2) Retrieve Product Data: This module allows the user to search for existing product information by entering the product id.

3) Authenticate Scan: Because we don't have a scanner in this module, we're uploading actual or false bar code images, which Blockchain will compare to previously stored bar codes. If a match is found, Blockchain will extract all details and display to the user; otherwise, authentication will fail.

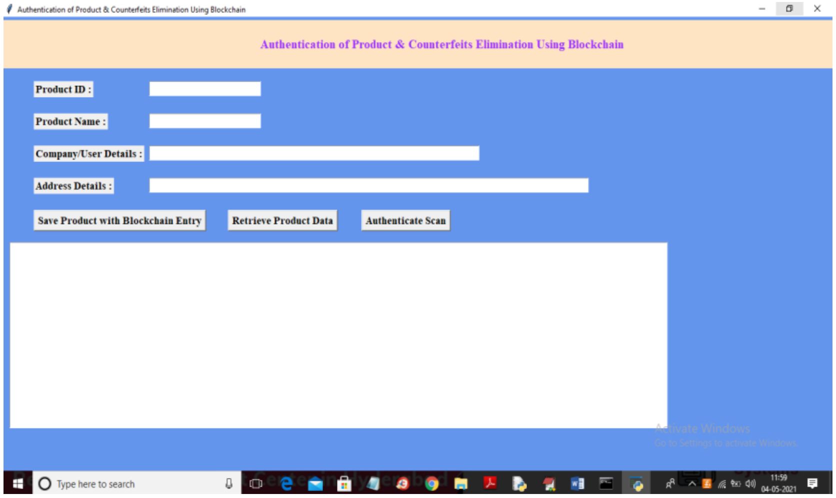
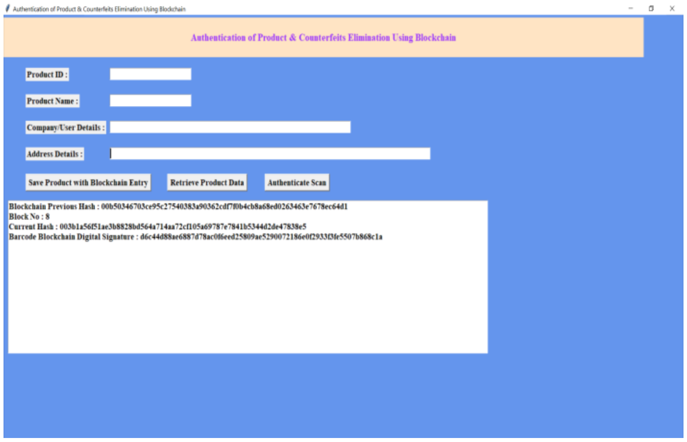

Authentication of Product & Counterfeits Elimination Using Blockchain
Authentication of Product & Counterfeits Elimination Using Blockchain
Product ID :
Product Name :
Company/User Details :
Address Details :
Save Product with Blockchain Entry
Retrieve Product Data
Authenticate Scan
Type here to search

Fig.2.Graphical User Interface of Authentication of Product and Counterfeit Elimination.

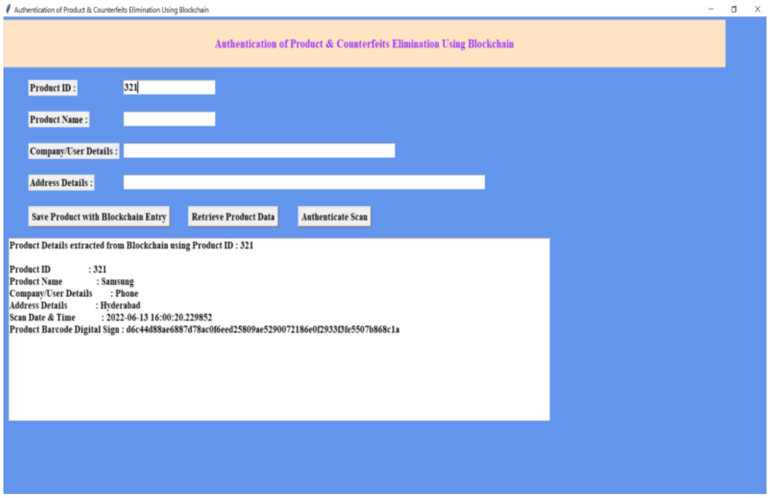
In Fig.2 consists of product id, name, company details, address details and it also consists of three modules like Save Products with Blockchain Entry, Retrieve Product Details and Authentication Scan.


Authentication of Product & Counterfeits Elimination Using Blockchain
Authentication of Product & Counterfeits Elimination Using Blockchain
Product ID :
Product Name :
Company/User Details :
Address Details :
Save Product with Blockchain Entry
Retrieve Product Data
Authenticate Scan

```
Blockchain Previous Hash : 00b50346703ce95c27540383a90362cdf7f0b4cb8a68ed0263463e7678ec64d1
Block No : 8
Current Hash : 003b1a56f51ae3b8828bd564a714aa72cf105a69787e7841b5344d2de47838e5
Barcode Blockchain Digital Signature : d6c44d88ae6887d78ac0f6eed25809ae5290072186e0f2933f3fe5507b868c1a
```

Fig.3: Save Product with Block chain entry

In Fig.3 the screenshot consists of Blockchain generated new Block with id 8 and we can see blockchain hash code of old and new transaction with uploaded bar code digital signature and all these details will saved inside Blockchain.


Authentication of Product & Counterfeits Elimination Using Blockchain
Authentication of Product & Counterfeits Elimination Using Blockchain
Product ID :
Product Name :
Company/User Details :
Address Details :
Save Product with Blockchain Entry
Retrieve Product Data
Authenticate Scan

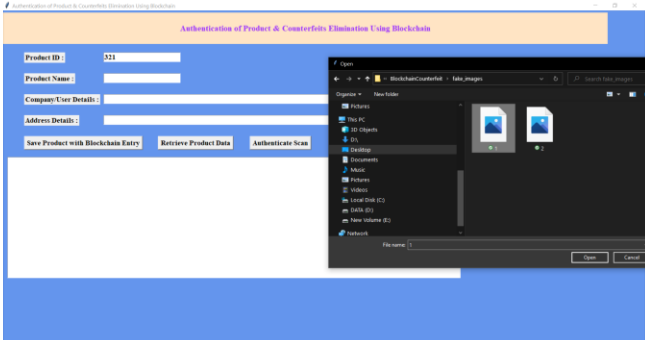
Product ID : 321

```
Product Details extracted from Blockchain using Product ID : 321

Product ID             : 321
Product Name             : Samsung
Company/User Details       : Phone
Address Details           : Hyderabad
Scan Date & Time          : 2022-06-13 16:00:20.229852
Product Barcode Digital Sign : d6c44d88ae6887d78ac0f6eed25809ae5290072186e0f2933f3fe5507b868c1a
```

Fig.4: Retrieve Product Data

In Fig.4, enter the product id and then click on 'Retrieve Product Data' button to get product details like product id, product name,user/companydetails, address details, scan date & time and product barcode digital sign.

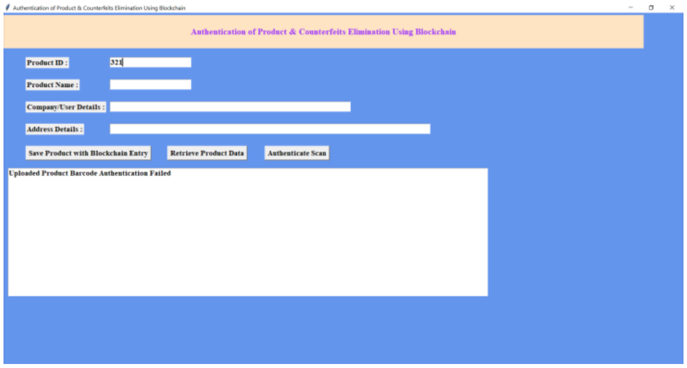


Product ID : 321

File name: 1

Fig.5: Authentication Scan

Checking with fake barcode by uploading from 'fake bar code' folder.The below screen shows the uploading the fake barcode. The above figure Fig.5 shows the screenshot of uploading the fake barcode.



Authentication of Product & Counterfeits Elimination Using Blockchain

Authentication of Product & Counterfeits Elimination Using Blockchain

Product ID : 321

Product Name :

Company/User Details :

Address Details :

Uploaded Product Barcode Authentication Failed

Fig. 6.Authentication Failed

Uploading a fake barcode for the product then an error message failed will be show on the screen. The above figure Fig.6. shows the error message of authentication failed.

CONCLUSION

To avoid forging counterfeits, we are converting all product details/barcodes into digital signatures, which will be stored in a Blockchain server, which supports tamper-proof data storage, and no one can hack or alter its data. If its data is altered by chance, verification will fail at the next block storage, and the user will be notified. In Blockchain technology, the same transaction data is saved on many servers with hash code verification, and if the data on one server changes, it will be noticed on the other servers since the hash code for the same data would change. In Blockchain technology, for example, data will be stored on multiple servers, and if malicious users alter data on one server, the hash code will be changed on one server while the other servers remain unchanged, and this changed hash code will be detected at verification time, preventing future malicious user changes.

***Future scope* -** Multiple techniques to reducing counterfeits were examined in this thesis. These improvements were considered, and their impact on minimising counterfeits was assessed, in order to be less reliant on external variables. Due to time constraints and the fact that several other system changes were also required, it was not possible to implement all of the suggested changes. The finalisation of these implementations for the proposed system, as well as the potential of running pilots, are among the next steps. The concept for reducing counterfeits in the humanitarian supply chain is currently being developed, as is the execution.

REFERENCES

[1] https://www.irjet.net/archives/V8/i3/IRJET-V8I3279.pdf Dr. J. Satheesh Kumar, G.Praveen, M. Kesavan, D. Naveen, Hindusthan College of Engineering and Technology, Tamil Nadu, India

[2] https://www.researchgate.net/publication/353971876_Counterfeited_Product_Identification_in_a_Supply_Chain_using_Blockchain_TechnologyShivamSingh , Gaurav Choudhary , Shishir Kumar Shandilya , Vikas Sihag , and Arjun Choudhary School of Computer Science and Engineering (SCSE),VIT Bhopal University, India

[3] http://www.sersc.org/journals/index.php/IJFGCN/article/view/35822Tarannum J. Sayyad Computer Science and Engineering Department Karmaveer Bhaurao Patil College of Engineering, Satara. Satara, Maharashtra, India

[4] https://www.mdpi.com/2071-1050/13/11/6016/pdf Ji Jiang * and JinChen,School of Information Technology and Management, University of International Business and Economics, Beijing 100029, China

[5] https://www.semanticscholar.org/paper/A-Blockchain-Based-Application-System-for-Product-Ma-Lin/35fc3218b0ec93341175e4156d7745e1b827eee2 JINHUA MA1 , SHIH-YA LIN2 , XIN CHEN3 , Fujian Provincial Key Laboratory of Network Security and Cryptology College of Mathematics and Informatics, Fujian Normal University, China