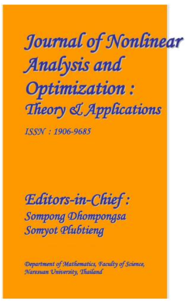
Journal of Nonlinear Analysis and Optimization
Vol. 15, Issue. 1, No.15 : 2024
ISSN : **1906-9685**



Journal of Nonlinear Analysis and Optimization : Theory & Applications
ISSN : 1906-9685
Editors-in-Chief :
Sompong Dhompongsa
Somyot Plubtieng
Department of Mathematics, Faculty of Science, Naresuan University, Thailand

AUTHENTICATION OF PRODUCT & COUNTERFEITS ELIMINATION USING BLOCKCHAIN

Y.Anil Kumar, ***Associate Professor CSE, Vaagdevi College of Engineering (Autonomous), India***
R.Ramya, ***UG Student, CSE, Vaagdevi College of Engineering (Autonomous), India***
S.Vamshi, ***UG Student, CSE, Vaagdevi College of Engineering (Autonomous), India***
R.Rakesh, ***UG Student, CSE, Vaagdevi College of Engineering (Autonomous), India***
A.Karthik, ***UG Student, CSE, Vaagdevi College of Engineering (Autonomous), 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. This paper explores the possibility to deflate counterfeit using blockchain technology. This paper 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.

1. INTRODUCTION

Although it may seem like a faroff idea, we are surrounded by a lot of counterfeits. From fashion and retail products to software, digital media, electronics, piracy, and intellectual property[1], [2] reports put the cost of counterfeiting somewhere around $600bn a year in the US alone. In fact, the International Chamber of Commerce predicts that the negative impacts of counterfeiting and piracy are projected to drain US$4.2 trillion from the global economy and put 5.4 million legitimate jobs at risk by 2022.

In Pharmaceuticals, the counterfeit medicine market is now responsible for around 1 million deaths per year, in an industry estimated to be worth $75bn annually. In fact, the counterfeit medicine industry is estimated to be growing at twice the rate of legitimate pharmaceuticals, making it up to 25 times more lucrative than the global narcotics trade. Trust is a central element in all transactions. No matter if sending money or exchanging goods, it becomes difficult if there is no trust between the entities involved. It becomes even more difficult, as with many transactions, third parties are involved, such as banks.[3] Often, not only one third-party is involved in a transaction, but multiple. An international money transfer does not only include the bank of the sender, the bank of the receiver, but also multiple intermediary entities such as clearing houses. The entities involved in the transaction do not only have to trust each other, but also the third parties. Removing these third parties can decrease transaction cost, facilitate faster transactions and add more transparency. Bitcoin has successfully shown that removing such third-parties is possible.

The cryptocurrency permits direct sending coins to a transaction partner, without the need to use banks and clearing houses[4]. The assets are directly transferred from one account to another. There are no intermediaries and thereby no need to trust third parties. In addition, the question if a transaction is valid is not answered by an institution, but by algorithms used. Therefore, it completely removes the need to trust any third party. The technology behind Bitcoin, the blockchain, can however not only be used for financial transactions and crypto currencies in general. The technology has potential to ―[5]redefine the digital economy because it allows immutable transactions, which can be checked at all times from everyone. This is because the information is publicly available and distributed globally. It is ‐chronologically updated and cryptographically sealed.

2. LITERATURE SURVEY

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures [6] provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible,[7] since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

This is the first white paper from the Hyperledger Performance and Scale Working Group. The purpose of this document is to define the basic terms and key metrics that should be used to evaluate the performance of a blockchain and then communicate the results. This paper also serves as a platform-agnostic resource for technical blockchain developers and managers interested in using industry-standard nomenclature.[8]

While we appreciate that there may be discrete definitions for the terms “blockchain” and “Distributed Ledger Technology (DLT)” [9],[10] for the purposes of this paper we will treat both terms synonymously and use the term “blockchain” throughout.

This document provides some guidance on selecting and evaluating workloads. We expect that refinements to these definitions and new blockchain-specific metrics will warrant future revisions of this document.

New cryptographic protocols which take full advantage of the unique properties of public key cryptosystems are now evolving[11]. Several protocols for public key distribution and for digital signatures are briefly compared with each other and with the conventional alternative.

The blockchain paradigm when coupled with cryptographically-secured transactions has demonstrated its utility through a number of projects, with Bitcoin being one of the most notable ones. Each such project can be seen as a simple application on a decentralised, but singleton, compute resource. We can call this paradigm a transactional singleton machine with shared-state. Ethereum implements this paradigm in a generalised manner. Furthermore it provides a plurality of such resources, each with a distinct state and operating code but able to interact through a message-passing framework with others. We discuss its design, implementation issues[12], the opportunities it provides and the future hurdles we envisage.

Our growing reliance on online services accessible on the Internet demands highly available systems that provide correct service without interruptions. Software bugs, operator mistakes, and malicious attacks are a major cause of service interruptions and they can cause arbitrary behavior, that is, Byzantine faults. This article describes a new replication algorithm, BFT, that can be used to build highly available systems that tolerate Byzantine faults[18]-[19]. BFT can be used in practice to implement real services: it performs well, it is safe in asynchronous environments such as the Internet, it incorporates mechanisms to defend against Byzantine-faulty clients, and it recovers replicas proactively. The recovery mechanism allows the algorithm to tolerate any number of faults over the lifetime of the system provided fewer than 1/3 of the replicas become faulty within a small window of vulnerability. BFT has been implemented as a generic program library with a simple interface. We used the library to implement the first Byzantine-fault-tolerant NFS file system, [13] BFS. The BFT library and BFS perform well because the library incorporates several important optimizations, the most important of which is the use of symmetric cryptography to authenticate messages. The performance results show that BFS performs 2% faster to 24% slower than production implementations of the NFS protocol that are not replicated. This supports our claim that the BFT library can be used to build practical systems that tolerate Byzantine faults.

This paper argues for a new approach to building Byzantine fault tolerant replication systems. We observe that although recently developed BFT state machine replication protocols are quite fast, they don't tolerate Byzantine faults very well: a single faulty client or server is capable of rendering PBFT, Q/U, HQ, and Zyzzyva virtually unusable. In this paper, we (1) demonstrate that existing protocols are dangerously fragile, (2) define a set of principles for constructing BFT services that remain useful even when Byzantine faults occur, and (3) apply these principles to construct a new protocol, Aardvark. Aardvark can achieve peak performance within 40% of that of the best existing protocol in our tests and provide a significant fraction of that performance when up to f servers and any number of clients are faulty. We observe useful throughputs between 11706 and 38667 requests per second for a broad range of injected faults.

3. PROBLEM STATEMENT

Approaches which help to identify counterfeits do not help, if there is no awareness of the issue with counterfeits. Especially critical for pharmaceuticals, the public must be aware of such products. Support of the analytics : If a product is suspected to be a counterfeit, it should be analyzed as soon as possible. This typically starts with a visual inspection of the packaging, the packaging content (such as leaflets) and the medicine itself. If the product turns out to be counterfeited, the risk should be evaluated and patients informed. Furthermore, law agencies should take the requisite steps to identify were the counterfeit has come from and act upon it. [14] This fights counterfeit by increasing awareness and by fighting criminal organizations introducing counterfeits.Not only supply chain any other online transaction require third party to complete transaction and peoples has to trust on third parties to complete their transaction and sometime this third parties can make fraud transaction or misuse user data.

3.2 LIMITATIONS

1. Not able identify counterfeits
2. So counterfeits product are increasing in markets
3. People may loss with these products

4. PROPOSED SYSTEM

In perspective of a user, a user is able to do the following thing in the specified order to check the authenticity of the product. (i) Scan QR/NFC tag of the Product using any scanner present on a mobile phone. (ii) The scan will open a page in the browser, The product info is requested from the Authentication Module. Authentication module verifies if it is a genuine request, if yes, it creates a new entry of scan in the database and blockchain and sends response with the Product data and its scan history. (iii) Browser shows if the product [15] is authentic and shows its scan history. User is able to view the scan history to check for any anomalous scan history. In supply chain also all products barcode digital Blockchain signatures [16] will be stored and if any third party distributor make clone of barcode then its signature will be mismatch and counterfeit will be detected.

4.2 ADVANTAGES

1. Detecting counterfeit
2. Avoid of spreading counterfeit products

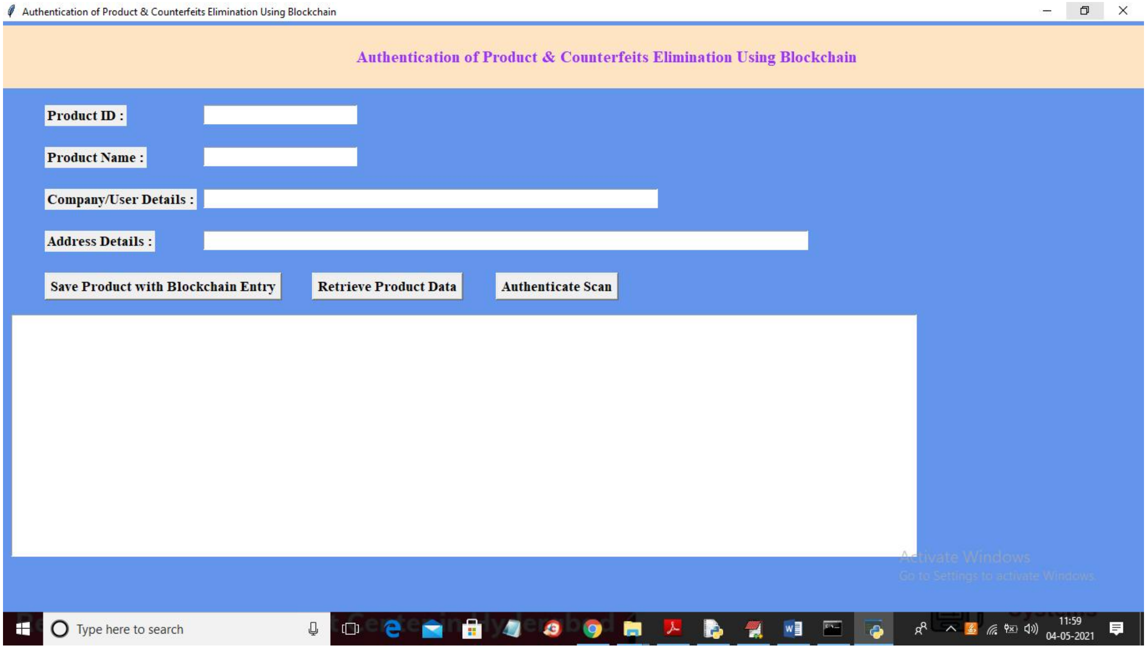
5. IMPLEMENTATIONS

1. **Save Product with Blockchain Entry:** In this module user will enter product details and then upload product bar code image and then digital signature will be generated on uploaded barcode and then this transaction details will be store in Blockchain[17]. Before storing transaction Blockchain will verify all old transaction and upon successful verification new transaction block will be store
2. **Retrieve Product Data:** Using this module user can search existing product details by entering product id

3. **Authenticate Scan:** Here in this module we don’t have any scanner so we are uploading original or fake bar code images and then Blockchain will verify digital signature of uploaded bar code with already store bar codes and if match found then Blockchain will extract all details and display to user else authentication will be failed.

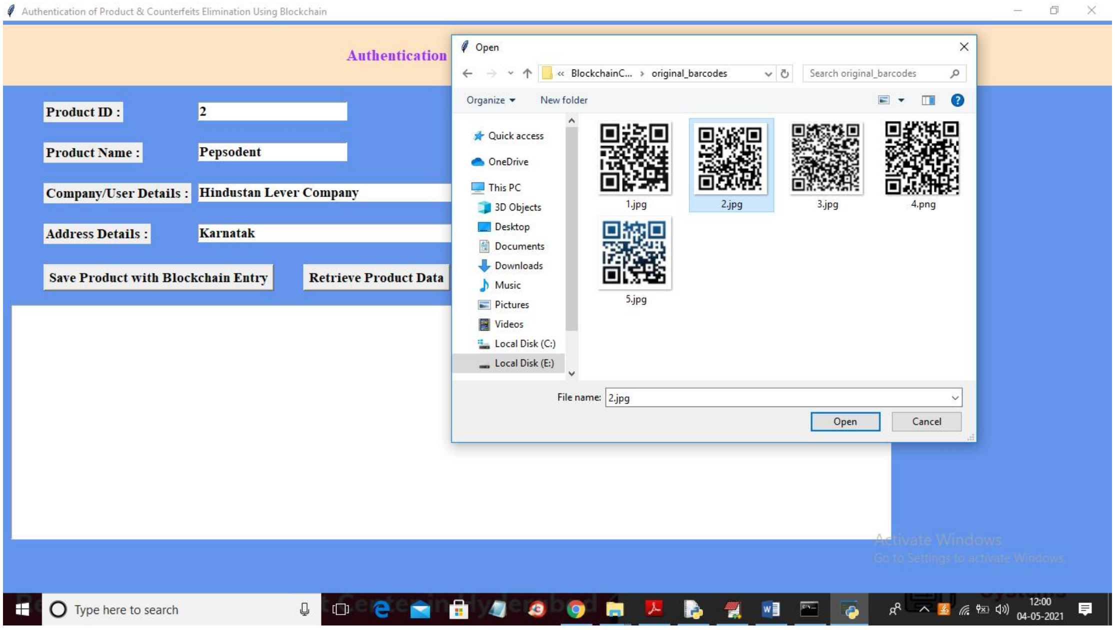
6. EXPECTED OUTCOMES

USER PAGE


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
Activate Windows
Go to Settings to activate Windows.
Type here to search
11:59
04-05-2021

User interface

In above screen enter product details and then click on ‘Save Products with Blockchain Entry’button to store product details in Blockchain



Product ID : 2

Product Name : Pepsodent

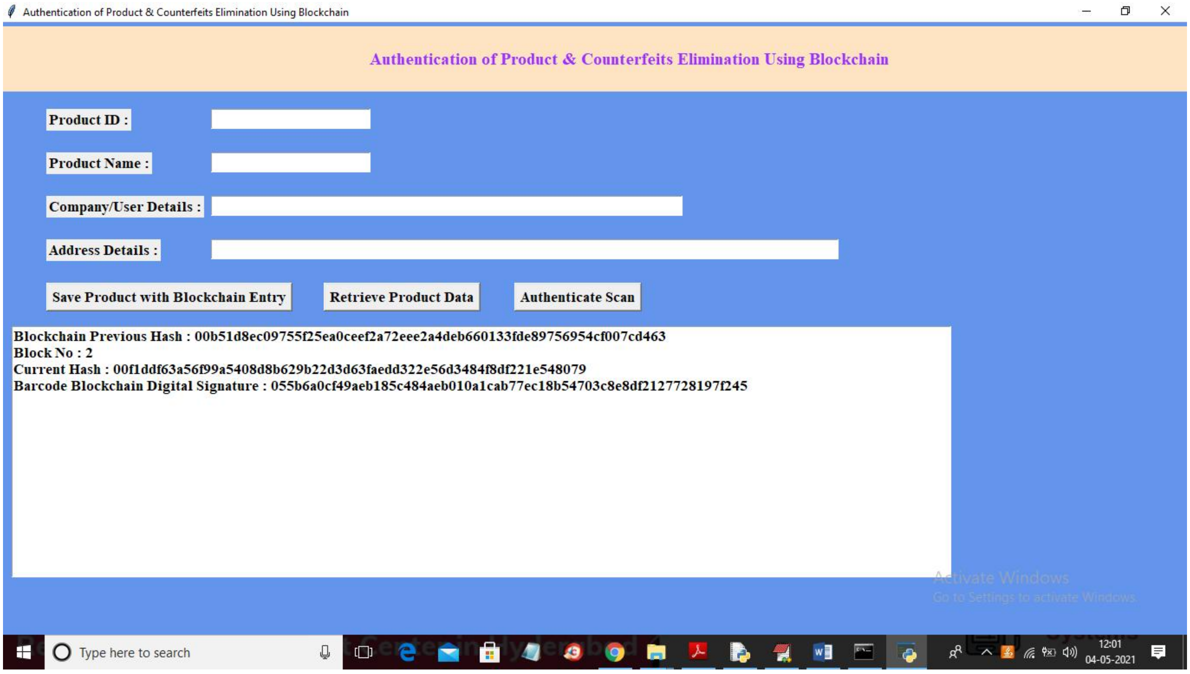
Company/User Details : Hindustan Lever Company

Address Details : Karnatak

File name: 2.jpg

User Associated Barcode

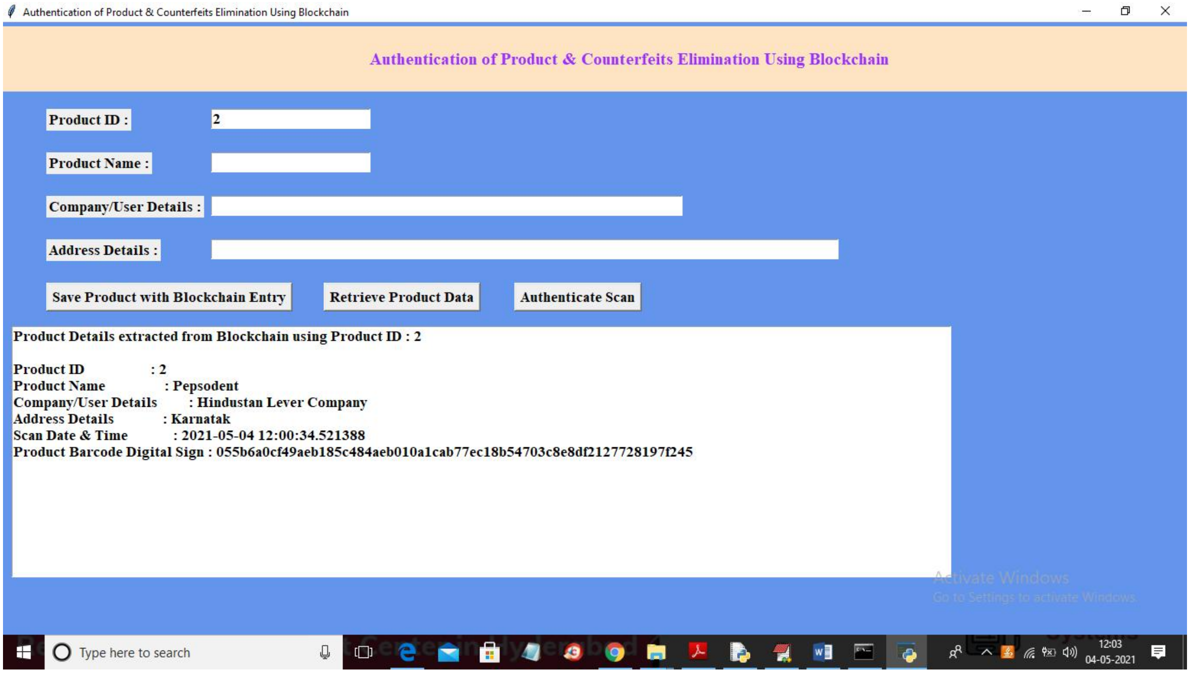
In above screen I entered product details and then selecting and uploading associated BARCODE image and then click on 'Open' button to get below result.


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
12:01
04-05-2021

```
Blockchain Previous Hash : 00b51d8ec09755f25ea0ceef2a72eee2a4deb660133fde89756954cf007cd463
Block No : 2
Current Hash : 00f1ddf63a56f99a5408d8b629b22d3d63faedd322e56d3484f8df221e548079
Barcode Blockchain Digital Signature : 055b6a0cf49aeb185c484aeb010a1cab77ec18b54703c8e8df2127728197f245
```

Figure-10: Blockchain hash code

In above screen Blockchain generated new Block with id 2 and we can see Blockchain hash code of old and new transaction with uploaded bar code digital signature and all this details will saved inside Blockchain and now to search product details click on 'Retrieve Product Data' button to get below details


Authentication of Product & Counterfeits Elimination Using Blockchain
Authentication of Product & Counterfeits Elimination Using Blockchain
Product Name :
Company/User Details :
Address Details :
Save Product with Blockchain Entry
Retrieve Product Data
Authenticate Scan
Type here to search
12:03
04-05-2021

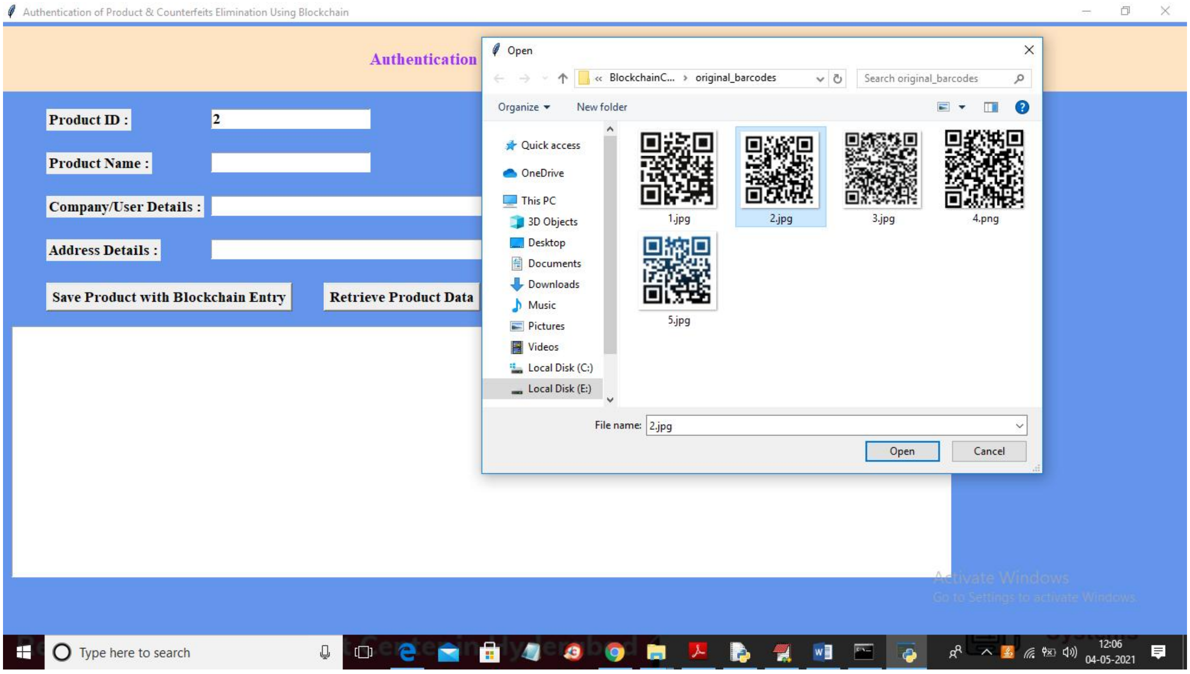
Product ID : 2

```
Product Details extracted from Blockchain using Product ID : 2

Product ID              : 2
Product Name            : Pepsodent
Company/User Details      : Hindustan Lever Company
Address Details          : Karnatak
Scan Date & Time          : 2021-05-04 12:00:34.521388
Product Barcode Digital Sign : 055b6a0cf49aeb185c484aeb010a1cab77ec18b54703c8e8df2127728197f245
```

Figure-11: Retrieve product data to get Details

In above screen I entered product id as 2 and then click on 'Retrieve Product Data' button to get above details. Now click on 'Authenticate Scan' button to upload product Barcode and then Blockchain will match this uploaded Barcode signature with available stored signatures and if match found then authentication will be successful else failed.



Product ID : 2

Product Name :

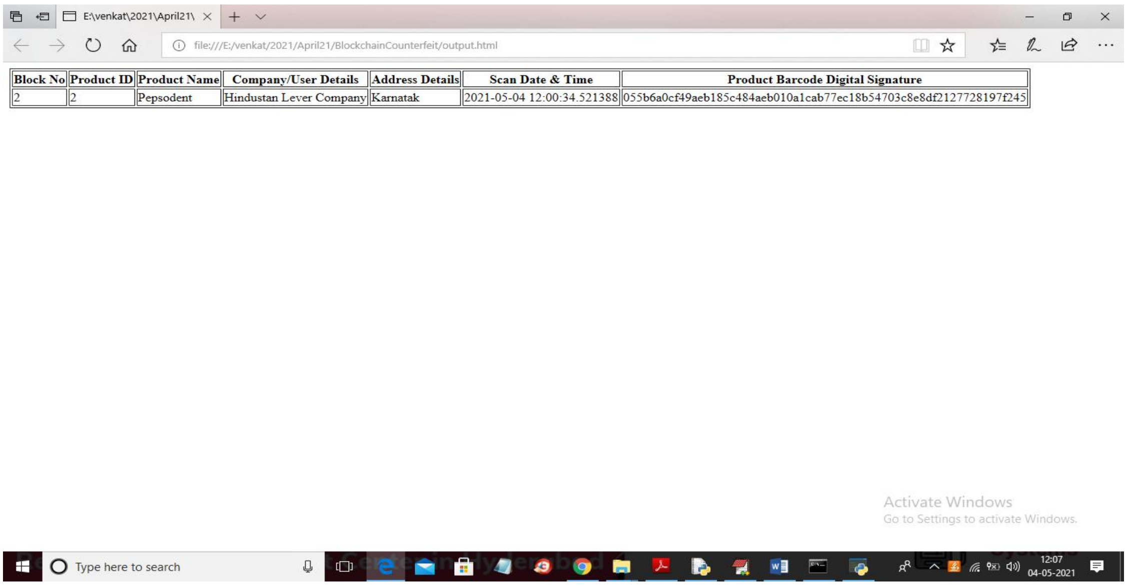
Company/User Details :

Address Details :

File name: 2.jpg

Figure-12: Retrieve Data by Uploading barcode

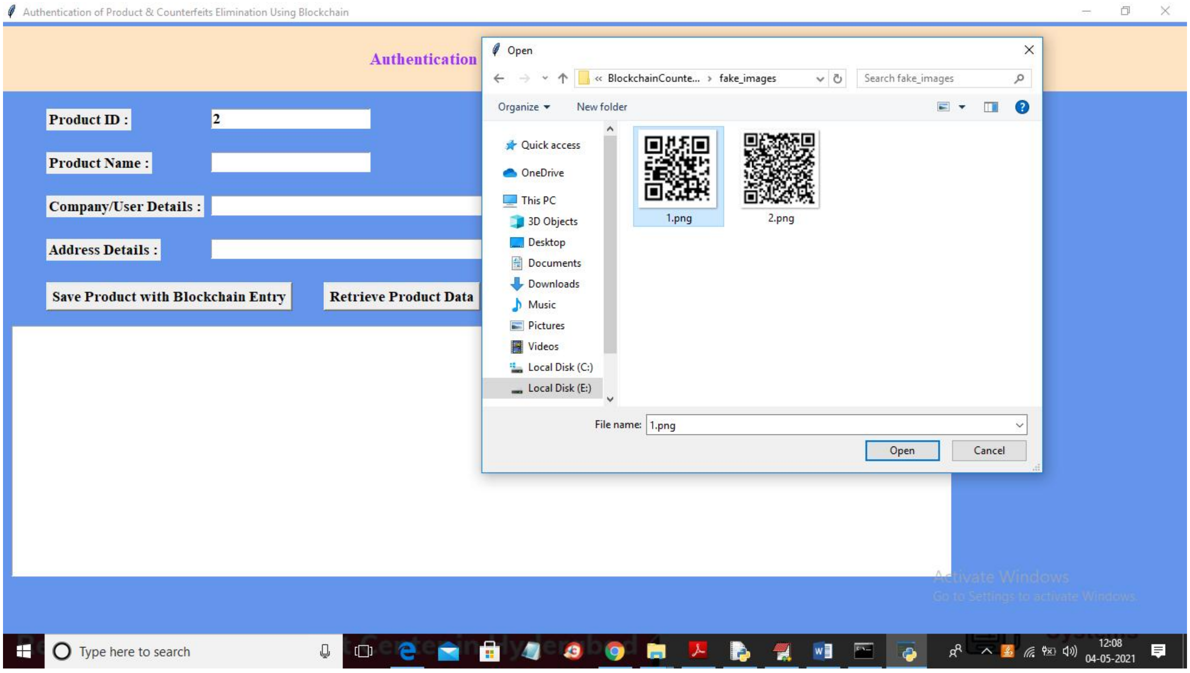
In above screen I am selecting and uploading '2.jpg' file and then click on 'Open' button to get below result


E:\venkat\2021\April21\
file:///E:/venkat/2021/April21/BlockchainCounterfeit/output.html
Type here to search

Block No	Product ID	Product Name	Company/User Details	Address Details	Scan Date & Time	Product Barcode Digital Signature
2	2	Pepsodent	Hindustan Lever Company	Karnatak	2021-05-04 12:00:34.521388	055b6a0cf49aeb185c484aeb010a1cab77ec18b54703c8e8df2127728197f245

Figure-13: WebPage Output

In above screen in browser author can see all authentication details uploaded product bar code. Now check with fake barcode by uploading from 'fake bar code' folder.



Authentication of Product & Counterfeits Elimination Using Blockchain

Product ID : 2

Product Name :

Company/User Details :

Address Details :

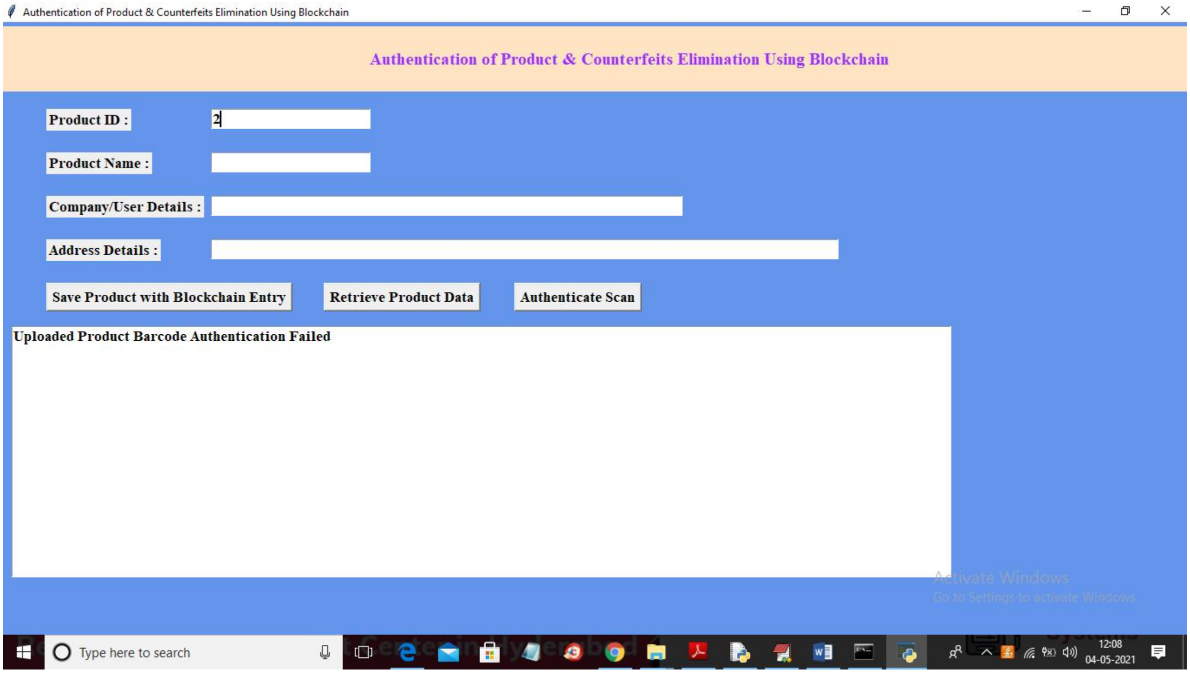
Open

BlockchainCounte... › fake_images

File name: 1.png

Figure-14: uploading Fake Barcodes

In above screen uploading barcode from fake folder and below is the result.



Authentication of Product & Counterfeits Elimination Using Blockchain

Product ID : 2

Product Name :

Company/User Details :

Address Details :

Uploaded Product Barcode Authentication Failed

Figure-15: Retrieve Data Failed

In above screen in text area we can see uploaded bar code authentication failed.

7. CONCLUSION

With this system, the products journey from manufacturing to customer can be recorded, and the customer is assured that the scans weren‘t faked. Manufacture is able to prove their product is authentic and is also able to track their product‘s pathway. The setup is easy to implement and requires less operation cost. Manufacturer can also adopt RFID or NFC tokens instead of QR codes to further strengthen their system.

7.2 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.

8. 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, OECD Publishing, 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 hyperledger 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].

[14] An ICC initiative Business Action to Stop Counterfeiting and Piracy (BASCAP). Brand protection directory. The World Business Organization. Available from: http://www.iccwbo.org/bascap [last cited on 2010 Jun 10].

[15] L. Li, ―Technology designed to combat fakes in the global supply chain‖, in Business Horizons, vol. 56, no. 2, p. 167-177, 2013.

[16] White paper. Dhar R. Anti counterfeit packaging technologies. A strategic need for the Indian industry. Confederation of Indian Industry 2009:1-47. Available from: http://www.bilcare.com/pdf/CII_anti_counterfeit_pkg_technologies_report.pdf [last cited on 2010 Oct 29].

[17] Berman, ―Strategies to detect and reduce counterfeiting activity‖, in Business Horizons, vol. 51, no. 3, p. 191-199, 2008.

[18] K. D´egardin, Y. Roggo and P. Margot. ―Understanding and fighting the medicine counterfeit market‖, in Journal of Pharmaceutical and Biomedical Analysis, vol. 87, p. 167-175, 2013

[19] [19]R. C. Merkle, ‗‗A digital signature based on a conventional encryption function,'' in Proc. Conf. Theory Appl. Cryptogr. Techn., 1987, pp. 369–378