Journal of Engineering Sciences
Vol 13, Issue 03, MARCH/2022
ISSN NO:0377-9254

AUTHENTICATION OF PRODUCT & COUNTERFEITS ELIMINATION USING BLOCK CHAIN

Anusha Kollu,Asst. Professor,Department of CSE,anusha.kollu87@gmail.com

Sai Srujan Kandukuri,Department of CSE,kandukurisrujan7@gmail.com

Venkat Deepak Mundra,Department of CSE,mundradeepak58@gmail.com

Abhishek Yerram,Department of CSE,abhishekyerram7@gmail.com

Sai Gopala Krishna Deekshith Challa,Department of CSE,saidixitchalla@gmail.com

ABSTRACT: Over the last few years, blockchain technologies have gotten a lot of attention. While financial transactions are the most well-studied use, it has the potential to agitate other markets. Blockchain eliminates the need for trusted intermediaries, speeds up transactions, and increases transparency. This research investigates the use of blockchain technology to deflate counterfeit goods. This paper presents an overview of several anti-counterfeiting solutions, as well as various blockchain technologies and the qualities that make blockchain particularly appealing for the use case. Three separate concepts have been created, and the growth of an existing system concept is being pursued further. It has been demonstrated that decreasing counterfeits cannot be accomplished solely through technological means. Increasing public awareness, battling counterfeiters on a legal level, having a robust alert system, and having tamper-proof packaging are all crucial. These elements, when paired with blockchain technology, can result in a cost-effective and comprehensive strategy to counterfeiting reduction.

Keywords: Authentication, Blockchain, Encryption.

1. INTRODUCTION

We are surrounded by a lot of counterfeits, despite the fact that it may appear like a far-fetched concept. The cost of counterfeiting in the United States is estimated to be approximately $600 billion per year, ranging from fashion and retail products to software, digital media, electronics, piracy, and intellectual property. By 2022, the International Chamber of Commerce estimates that the negative effects of counterfeiting and piracy will drain US$4.2 trillion from the global economy and threaten 5.4 million genuine jobs. In the pharmaceutical business, the counterfeit drug market now accounts for roughly 1

million deaths each year, in a $75 billion industry. In fact, it is projected that the counterfeit drug sector is developing at twice the rate of legal pharmaceuticals, making it up to 25 times more profitable than the worldwide narcotics trade. In all dealings, trust is essential. It becomes difficult to send money or exchange items if there is a lack of confidence between the parties involved. It gets much more complicated because other parties, such as banks, are engaged in many transactions. A transaction frequently involves not just one, but several third parties. An international money transfer involves not only the sender's and receiver's banks, but also a number of intermediary firms such as clearing houses. Not only do the people participating in the transaction have to trust each other, but they also have to trust third parties. By eliminating these third parties, transaction costs can be reduced, transactions can be completed faster, and there is more transparency. Bitcoin has successfully demonstrated that such third-parties can be eliminated. Without the use of banks or clearing institutions, the cryptocurrency allows you to send coins directly to a transaction partner. The funds are sent immediately from one account to another. There are no middlemen, thus there is no need to rely on third parties. Furthermore, the question of whether a transaction is genuine is answered by algorithms rather than by institutions. As a result, it eliminates the need to rely on any third party.

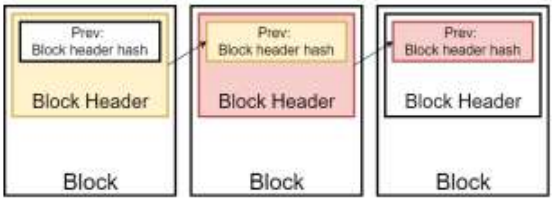

Fig.1: Connections between blocks in blockchain

The blockchain, which underpins Bitcoin, can be utilised for more than only financial transactions and crypto currencies in general. Because it allows immutable transactions that can be reviewed at any moment by anybody, the technology has the ability to "redefine the digital economy" [10]. This is due to the fact that the information is publicly available and widely disseminated. It has been updated chronologically and cryptographically [11]. The whole spectrum of possible applications for this technology must be explored, but tracking product ownership and history is undoubtedly one among them [12]. This research investigates the use of blockchain technology to reduce counterfeiting.

2. EXISTING SYSTEM

Many businesses rely on third-party vendors. Because the outsourced supplier has access to all of the original assets, there is a risk that they will not only make legitimate products, but also counterfeits. Outsourcers should be vetted and managed carefully. Another alternative is to not outsource the entire product to a single firm, but to divide the manufacturing of the product among several companies or to keep some of the production in-house. This ensures that no single foreign firm has all of the resources necessary to manufacture counterfeit goods.

Fig.2: Challenges in counterfeit elimination

It must also be verified that all assets are returned to the outsourcing business at the end of the contract. To authenticate supply chain products because these products may be supplied by multiple third-party distributors, and these distributors can create clones/fakes/counterfeits of this product's BAR CODE and then manufacture fake products with this counterfeit label, resulting in huge financial and human losses if fake medicine is manufactured. Not only does the supply chain require a third party to complete the transaction, but all online transactions must as well. People must trust third parties to complete their transactions, and these third parties can sometimes commit fraud or misuse customer data.

DRAWBACKS:

Because the outsourced supplier has access to all of the original assets, there is a risk that they will not only make legitimate products, but also counterfeits. Online transactions necessitate the employment of a third party to complete the transaction, and customers must trust these third parties to complete their transactions. However, these third parties can sometimes commit fraud or misuse user data.

3. PROPOSED SYSTEM

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 tamper-proof 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. 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.

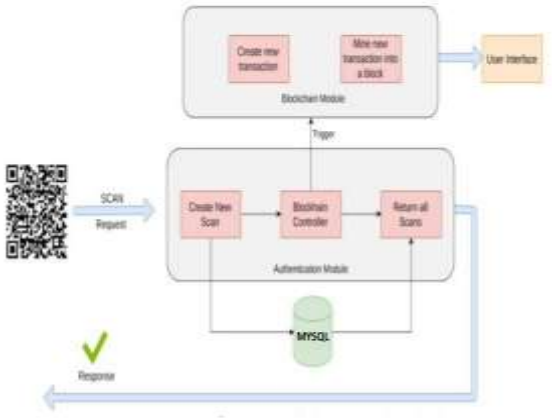

Fig.3: Core Architecture: Authentication module connecting database and blockchain

All items' barcode digital Blockchain signatures will be maintained in the supply chain, and if a third-party distributor creates a clone of the barcode, the signatures will be mismatched, and counterfeit will be identified.

ADVANTAGES:

Each data will be recorded in Blockchain by checking old hash codes; if the old hash codes remain unchanged, the data will be considered original and unchanged, and new transaction data will be added to the Blockchain as a new block. For each new data storage, the hash code of all blocks will be validated.

4. RELATED WORK

4.1 A Peer-to-Peer Electronic Cash System.

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. The network itself necessitates a bare minimum of organisation. Nodes can leave and rejoin the network at any time, accepting the longest proof-of-work chain as verification of what happened while they were gone.

4.2 Performance Evaluation of Blockchain Systems: A Systematic Survey:

Blockchain has been hailed as a game-changing technology with applications in a variety of fields. As more and more blockchain platforms develop, it's critical to evaluate their effectiveness in a variety of scenarios and use cases. We undertake a systematic survey on blockchain performance evaluation in this research by dividing all examined solutions into two broad categories: empirical analysis and analytical modelling. We compare and contrast current empirical blockchain assessment approaches, such as benchmarking, monitoring, experimental analysis, and simulation, in the empirical analysis. In analytical modelling, we look at stochastic models that have been used to evaluate the performance of popular blockchain consensus methods. We extract crucial criteria for selecting the most appropriate evaluation approach for enhancing the performance of blockchain systems based on their identified bottlenecks by contrasting, comparing, and combining diverse methodologies together.

4.3 Understanding and fighting the medicine counterfeit market:

Medicine counterfeiting is a huge global problem that involves manufacturing and distribution networks that are a part of organised crime in the industrialised world. Legal sanctions are frequently improper or simply not imposed, despite the potentially disastrous health consequences. The difficulty in agreeing on a definition of counterfeiting, as well as the enormous profits made by counterfeiters and the market's complexity, are the key reasons for the phenomenon's widespread prevalence. To combat the rise of counterfeiting, international collaboration is essential. Furthermore, legal, enforcement, and scientific efforts are also urgently needed. Pharmaceutical businesses and government agencies have created safeguards to protect medications while also allowing for quick and accurate investigation of questionable products. Analysts today have a variety of tools at their disposal to distinguish between genuine and counterfeit products, most of which are based on chromatography and spectroscopy.

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.

5. ALGORITHMS USED

Blockchain Hash Function:

The hash algorithm has a few distinguishing characteristics: It generates a one-of-a-kind result (or hash). It's a function that only works in one direction. The properties of

this cryptographic hash function are used by the blockchain in the consensus mechanism of crypto currencies like Bitcoin. A digest or digital fingerprint of a given quantity of data is referred to as a cryptographic hash. Cryptographic hash functions take transactions as input and run them through a hashing algorithm that produces a fixed-size output. There is no way to retrieve the complete text from the created hash because the Hash function is a one-way function.

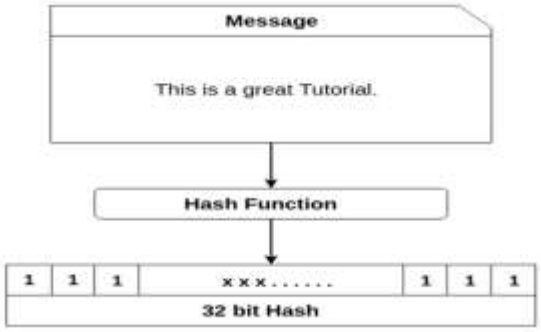

Fig.4: Hash function representation

6. EXPERIMENTAL RESULTS

Fig.5: Home screen

Fig.6: Save Products with Blockchain Entry

Fig.7: Retrieve product data

Fig.8: Authenticate scan

7. CONCLUSION

We create projects based on online transactions that involve the use of a third party to complete the transaction. People must trust third parties to complete their transactions, and third parties can sometimes commit fraud or misuse user data. To

circumvent this issue, the author has chosen Blockchain technology, which does not require the involvement of a third party and allows for verification to be carried out by a software algorithm without the involvement of 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 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.

8. 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] 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.