DETECTION OF COUNTERFEITS AND ELIMINATION USING BLOCK CHAIN

K.Neha Nandini[1]., C.Sai Anusha[2].,K.Poojasri[3].,E.Akhila[4].,K.Supritha[5]
1 Assistant Professor, Department Of CSE., Malla Reddy College Of Engineering For Women., Maisammaguda.,
Medchal., Ts, India (✉nehanandini.kella@gmail.Com)
2, 3, 4, 5 B.Tech CSE, (19RG1A0566, 19RG1A0583, 19RG1A0568, 19RG1A0590),
Malla Reddy College Of Engineering For Women., Maisammaguda., Medchal., Ts, India

ABSTRACT:

The previous several years have been quite fruitful for blockchain technology. The most researched use is in financial transactions, but it might also cause disruptions in other areas.

Blockchain reduces transaction times, improves traceability, and does away with middlemen. In this study, we look at the possibility of using blockchain technology to devalue fake products. In this paper, we provide an overview of many anticounterfeiting solutions, as well as several blockchain technologies and the features that make blockchain especially interesting for the use case. There are now three distinct ideas, and a fourth is being developed via the expansion of an existing system concept. It has been shown that technology solutions alone will not be sufficient to reduce counterfeits. It is critical to educate the public, take legal action against counterfeiters, implement a reliable alarm system, and use tamper-evident packaging. Combine these with blockchain technology, and you have a complete and efficient plan to combat counterfeiting.

FIRST, AN OVERVIEW

Although the idea of being surrounded by fakes may seem far-fetched, the reality is that we are. From clothing and other retail items to software, digital media, electronics, piracy, and intellectual property, the cost of counterfeiting in the United States is estimated at over $600 billion annually. According to the International Chamber of Commerce, counterfeiting and piracy will cost the world economy US$4.2 trillion by 2022 and jeopardize 5.4 million legitimate employment. About one million people per year are killed by the counterfeit drug market, which is a $75 billion business. It is estimated that the counterfeit medication industry is growing at a pace of two to five times that of the legitimate pharmaceutical industry, making it much more lucrative than the global narcotics trade. Building trust is crucial in every relationship. When trust is low, it's hard to do business together, whether that's sending money or exchanging goods. Adding to the complexity is the involvement of other parties, such as banks, in many transactions. Multiple parties, rather than just one, are often involved in a transaction. Banks on both ends of an international money transfer are necessary, but there are also many other companies, such clearing houses, that play a role in the transaction. Participants in a transaction must trust not just one another, but also neutral third parties. The removal of these

middlemen allows for lower transaction fees, quicker settlement times, and more openness. Bitcoin has shown that it is possible to remove such middlemen. You may transmit bitcoin to a business partner directly, bypassing intermediaries like banks. Immediately, the money is transferred from one account to another. Because there are no go-betweens, no outside parties are required.

And rather than relying on human authorities to determine the legitimacy of a transaction, modern systems use algorithms. This means that no outside party is required.

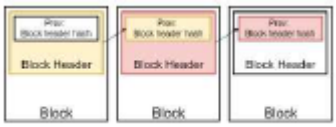

Fig.1: Connections between blocks in Blockchain

Bitcoin's underlying blockchain technology has applications outside the banking sector and the crypto currency market. The technology has the potential to "redefine the digital economy" [10] since it permits immutable transactions that can be inspected at any time by everyone. This is because the data has already been extensively shared with the public. Both the date and encryption have been updated [11].

The whole range of uses for this technology should be investigated, but one obvious one is keeping tabs on product ownership and history [12]. The purpose of this study is to explore the potential of blockchain technology in the fight against counterfeiting.

Second, the PRESENT SETUP

Third-party suppliers are essential for many companies. There is a chance that the outsourced supplier will produce both genuine and counterfeit goods since they have access to all of the original assets.

Careful screening and management of outsourcing partners is essential. It's also possible to maintain part of the production in-house or to split it up among many organizations rather than outsourcing everything. This disperses the power, ensuring that no one foreign company has all it needs to produce fake products.

Fig.2: Challenges in counterfeit elimination

All assets must be returned to the outsourced company, and this must be confirmed as well. In order to prevent massive financial and human losses caused by the production of counterfeit medicines, it is important to verify the authenticity of products throughout the supply chain. This is because these products may be supplied by multiple third-party distributors, and these distributors may create clones/fakes/counterfeits of this product's BAR CODE and then manufacture fake products with this counterfeit label. All online transactions, including those in the supply chain, need the involvement of a third party. In order to execute financial transactions, individuals must place their faith in a third party, who may or may not operate in the best interests of their customers.

CONS

The outsourced provider may produce both genuine and counterfeit goods since they have access to the original assets. Customers must put their faith in these intermediaries since they must engage them to execute their online purchases. However, fraud and data misuse by third parties are possible.

3. THE SUGGESTIVE SYSTEM

With blockchain technology, there is no need to involve a third party in the verification process since it is handled entirely by a computer algorithm. To prevent the creation of fake products, we are converting all product details/barcodes into digital signatures that will be stored in a Blockchain server. This type of server is capable of tamper-proof data storage, meaning that no one can hack or alter its data.

If the data on one server changes, it will be picked up by the other servers because the hash code for the same data would change. This is how Blockchain technology works. In Blockchain technology, for instance, data is stored on multiple servers, and if malicious users alter data on one server while the other servers remain unchanged, the hash code on the tampered server is changed, and this is detected at verification time, preventing future malicious user changes.

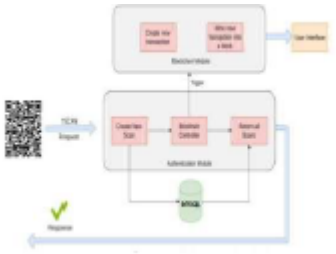

Fig.3: Core Architecture: Authentication module connecting database and blockchain

Digital Blockchain signatures of all barcodes will be stored in the supply chain; if a third-party distributor replicates the barcode, the resulting signatures will be incompatible, revealing the fake product.

IF THE OLD HASH CODES DO NOT CHANGE, THEN THE DATA IS CONSIDERED ORIGINAL AND UNCHANGED, AND THE NEW TRANSACTION DATA IS ADDED TO THE BLOCKCHAIN AS A NEW BLOCK. The hash values of all stored blocks are checked before any more data is added.

4. CONNECTED TEXTS

4.1 A Distributed Electronic Cash Network.

A peer-to-peer form of electronic currency would enable internet payments to be delivered directly from one party to another without going through a financial institution. Even if digital signatures are used, the significant advantages will be nullified if a trusted third party is also needed to prevent duplicate spending. We propose addressing the issue of duplicate spending via the use of a P2P network. Hash-based proof-of-work on the network maintains a running chain of transactions that cannot be altered without re-working

the proof-of-work. The longest chain not only confirms the order of events, but also indicates that it originated from the most potent computational resource. As long as non-collaborating nodes have more CPU power, they will generate the longest chain and eventually defeat the attackers. The network itself requires little management. The longest proof-of-work chain is accepted as confirmation of events that occurred while a node was disconnected from the network.

4.2 A Systematic Survey of Methods for Evaluating Blockchain Systems' Performance

Blockchain is a promising new technology that has the potential to revolutionize many different industries. There is a growing need to assess the performance of existing blockchain systems across a range of environments and use cases. In this study, we conduct a comprehensive literature review on the topic of blockchain performance assessment, classifying the many approaches we looked at into either empirical analysis or analytical modeling. In the empirical study, we contrast and analyze several existing methods for evaluating blockchain technologies, such as benchmarking, monitoring, experimental analysis, and simulation. In this section, we analyze the performance of well-known blockchain consensus algorithms using stochastic models. By contrasting, comparing, and blending several approaches, we are able to extract essential criteria for choosing the most effective assessment methodology for boosting the performance of blockchain systems depending on their identified bottlenecks.

4.3 Recognizing the Problem and Countering Counterfeit Medicines:

In the industrialized world, organized criminal groups often operate manufacturing and distribution networks that produce and sell fake medicines.

The potentially catastrophic health repercussions are often overlooked due to incorrect or non-existent legal punishments. The complexity of the market, the tremendous profits gained by counterfeiters, and the difficulty in agreeing on a definition of counterfeiting all contribute to the problem's pervasiveness.

The rising tide of counterfeiting calls for concerted efforts on a global scale to stem the tide.

Additionally, there is an immediate requirement for legal, enforcement, and scientific efforts.

Businesses in the pharmaceutical industry and regulatory bodies have developed protections to prevent damage to pharmaceuticals while facilitating efficient and thorough investigations of potentially dangerous ones. These days, most methods used by analysts to determine if a product is authentic or not are based on chromatography or spectroscopy.

The following are the modules that we developed for this undertaking.

First, the user enters product information, uploads a picture of the product's barcode, creates a digital signature on the barcode,

and finally saves the transaction details in Blockchain. Before committing a transaction to the ledger, Blockchain verifies that it is consistent with all prior transactions.

Second, users may input a product id to get previously recorded details about that item.

Because this module does not contain a scanner, we are instead providing Blockchain with images of real and fake bar codes to check against its database. When a user enters their credentials, Blockchain checks them against their existing ones and, if a match is discovered, displays all relevant information.

Hash Function in Blockchain:

5. ALGORITHMs Employed

There are a few unique features of the hash algorithm: It produces a unique output (hash). It's a unidirectional function, therefore it can only be used in one way. The blockchain, the consensus mechanism behind cryptocurrencies like Bitcoin, makes use of the features of this cryptographic hash function. A cryptographic hash is a digest or digital fingerprint of a certain amount of data.

To generate a fixed-size output, cryptographic hash functions feed transactions into a hashing process. Since the Hash function is unidirectional, it is impossible to reconstruct the original text from the generated hash.

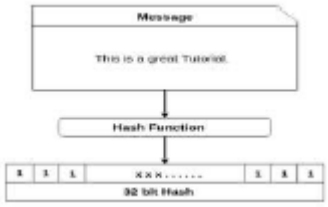

Fig.4: Hash function representation

6. EXPERIMENTAL RESULTS

Fig.5: Home screen

Fig.6: Save Products with Blockchain Entry

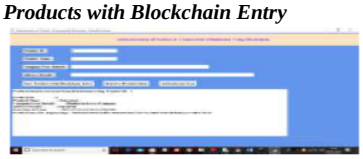

Fig.7: Retrieve product data

Fig.8: Authenticate scan

7. CONCLUSION

We develop our initiatives around the concept of online transactions that need the help of an intermediary service. To complete their transactions, consumers must place their faith in third parties; yet, these companies are not without their own risks, including fraud and data exploitation. The author has selected Blockchain technology because it eliminates the need for a trusted third party and instead enables verification to be performed by a computer algorithm. All product information and barcodes are being converted into digital signatures and then stored on a Blockchain server, which provides secure, unhackable data storage

to prevent the sale of fake goods. The next time it is stored in a block, verification will fail if the data has been tampered with, and the user will be informed. In Blockchain technology, identical transaction records are stored across multiple servers, each of which has its own unique hash code that is used to verify the integrity of the record. In Blockchain technology, for instance, data is stored on multiple servers, and if malicious users alter data on one server while the other servers remain unchanged, the hash code on the tampered-with server is changed, and this is detected at verification time, preventing further malicious user changes.

OUTLOOK NO. 8

This thesis analyzed a wide variety of strategies for combating counterfeits. To reduce reliance on external factors, these enhancements were explored, and their effect on reducing counterfeits was evaluated. It was not feasible to implement all of the proposed improvements due to time restrictions and the fact that various other system upgrades were also necessary. In the future, we may complete these implementations for the proposed system and perhaps conduct pilots. The plan to cut down on fake goods in the humanitarian supply chain is still in the works.

REFERENCES

"Bitcoin: A Peer-to-Peer Electronic Cash System" (Satoshi Nakamoto, 2008) [1] Performance Metrics for Hyperledger Blockchain, Version 1.01, October 2018 [2] Hyperledger

Protocols for public-key cryptosystems, by R.C. Merkle; published in Proceedings of the 1980 Symposium on Security and Privacy of the IEEE Computer Society; pages 121–133; April 1980.

Here's a link to Flask Docs written by Armin Ronacher: http://flask.pocoo.org/docs/.

Tech. Rep., 2014; G. Wood, "Ethereum: A secure decentralized generalized transaction ledger."

A Converging Criminal Network Approach to Illicit Trade, OECD Reviews of Risk Management Policies, OECD Publishing, Paris, 2016, https://doi.org/10.1787/9789264251847-en.

[7] "Practical byzantine fault tolerance and proactive recovery," ACM Trans. Comput. Syst., volume 20, issue 4, pages 398-461, November 2002. Authors: M. Castro and B. Liskov.

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

Architecture of the hyperledger blockchain fabric, Technical Report, July 2016 [9] Cachin.

According to [10] S. Underwood's "Blockchain Beyond Bitcoin," which appeared in the November 2016 issue of Communications of the ACM, pages 15–17.

Israel Is a Booming Market for Blockchain Technology, Deloitte Reports. [Online].

This report can be found online at https://www2.deloitte.com/content/dam/Deloitte/il/Documents/financialservices/israel_a_hotspot_for_blockchain_innovation_feb2016_1.1.pdf. [Accessed: 2.11.2016].

[12] G. Greenspan and M. Zehavi, "Will Provenance Be the Break Out Use Case of the Blockchain in 2016?," 7.1.2016. [Online].

Provenance Blockchain Technology App, Found at: http://www.coindesk.com/. [Last Reviewed: December 12, 2016].

The counterfeit pharmaceutical industry (Qatar).

The 2009 WHO World Health Report.

Medicines and Health Services/Counterfeit/Frequently Asked

Questions/QACounterfeitoctober2009. pdf [referenced last on June 12th, 2010].
Business Action to Combat Piracy and Counterfeiting (BASCAP) [14] is an ICC program.
Catalog of brand safety measures. Global Business Network. The document may be seen at http://www.iccwbo.org/bascap. [refereed to latest on 2010-06-10].
Technology developed to counter counterfeits in international trade, by L. Li, Business Horizons, volume 56, issue 2, pages 167-177, 2013.