



AUTHENTICATION OF PRODUCT & COUNTERFEITS ELIMINATION

USING BLOCKCHAIN

CH VENKATESH

Assistant Professor, Dept of CSE, ARJUN COLLEGE OF TECHNOLOGY AND SCIENCE,
mount opera premises, near ramoji film City, Hyderabad, TS, 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.

Keywords: *Block Chain, bit coin, High efficiency, QR code, RFID.*

1. INTRODUCTION:

Although it may seem like a far off idea, we are surrounded by a lot of counterfeits. From fashion and retail products to software, digital media, electronics, piracy, and intellectual property, 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



International Journal For Advanced Research In Science & Technology

A peer reviewed international journal

www.ijarst.in

IJARST

ISSN: 2457-0362

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. 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. 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 —redefine the digital economy [10], 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 [11]. The full range of applicable use cases for this technology has to be seen, but tracking ownership and history of a product is surely one of them [12]. This paper explores the possibility to reduce counterfeit using blockchain technology. 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 [6]. Current anti-counterfeiting supply chains rely on a centralized authority to combat counterfeit products. This architecture results in issues such as single point processing, storage, and failure. 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. Our simulations show that the proposed protocol offers remarkable performance with a satisfactory level of security compared to the state of the art consensus protocol Tendermint.

2. LITERATURE SURVEY:

[1] JINHUA MA , SHIH-YA LIN , XIN CHEN , HUNG-MIN SUN , YEH-CHENG CHEN AND HUAXIONG WANG proposed the paper “A Blockchain-Based Application System for Product Anti-Counterfeiting”,2020 describe a decentralized Blockchain system with products ant counterfeiting, in that way manufacturers canuse this system to provide genuine products without having to manage direct-operated stores, which can significantly reduce the cost of product quality assurance and can assure that the consumers getting genuine products without the involvement of trusted intermediaries. [2]HOAI LUAN PHAM, THI HONG TRAN and YASUHIKO NAKASIMA proposed the paper

“Practical Anti-Counterfeit Medicine management System Based on Technology”,2019 which describes a novel Blockchain based product ownership management method for product ownership management method for anti-counterfeit medicine system to resist the cloning of drug and improve the practical applicability. Analysys and evaluation results of our proposed system outperform the related proposals based on criteria about a practical application, anti-clone, low cost oriented, and scalability. Furthermore, experimental implementation on a small scale shows that our proposed system works appropriately in a real environment.

Anti-counterfeiting solutions should protect organizations from financial and reputation losses, and, especially in the case of pharmaceutical products, customer safety. [15] argues that good anti-counterfeiting techniques should generally be simple to apply, but difficult to imitate and have four main features: They should be difficult to duplicate, it should be possible to identify them without special equipment, it should be difficult to re-use them, and it should be visible if they were tampered with. From a product perspective, there are three general technologies to reduce counterfeits [15]: Overt (Visible) Features expected to assist the users to confirm the genuineness of a pack. Such



features will be significantly visible, and complex or expensive to reproduce.[16] . This includes holograms, color shifting inks, security threads, water marks etc. The advantage of overt technologies is that they can be checked by the end consumer. Covert (Hidden) Features the rationale of a covert feature is to aid the brand owner to recognize a counterfeit product. The general public will not be aware of its presence nor will have the resources to confirm it. This includes UV, bi-fluorescent and pen-reactive ink, as well as digital watermarks and hidden printed messages. Covert technologies help to identify counterfeits in the supply-chain and are especially efficient combined with overt technologies. Track and trace includes Radio Frequency Identification (RFID) tags, Electronic Product Codes (EPCs) and barcodes. Track and trace technologies allow for simpler tracing of products, thereby enabling the reduction of counterfeits, as the history of a product is available. The tag or barcode is included by the manufacturer. Distributors scan the identification, enabling them to check the authenticity of the product and update the status. Finally, retailers can also scan the product, to check the history and authenticity of the product. This approach does not only tackle the counterfeit problem, but also enables track and trace through the whole product lifecycle.

Existing System:

Existing In this paper author is using Blockchain technology to authenticate supply chain products as this products may be supplied from multiple third party distributors and this distributors can make clone/fake/counterfeits of this product BAR CODE and then manufacture fake products and add this counterfeit label to fake product and this fake products can cause huge loss of financial and lives if fake medicine manufacture. 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. METHODOLOGY

To avoid this problem author using Blockchain technology which does not require any third party and verification will be done by software algorithm itself without involvement of any third party. In this to avoid forge counterfeit we are converting all products details/barcode into digital signatures and this digital signatures will be stored in Blockchain server as this Blockchain server support tamper proof data storage and nobody can hack or alter its data and if by an chance if its data alter then verification get failed at next block storage and user may get intimation about data alter.

WORKING:

In this paper author is using Blockchain technology to authenticate supply chain products as this products may be supplied from multiple third party distributors and this distributors can make clone/fake/counterfeits of this product BAR CODE and then manufacture fake products and add this counterfeit label to fake product and this fake products can cause huge loss of financial and lives if fake medicine manufacture.

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.

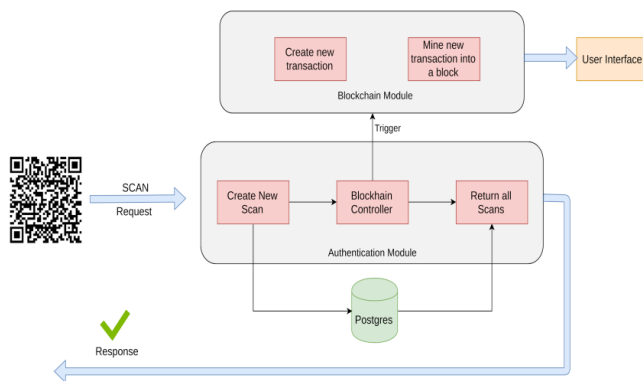
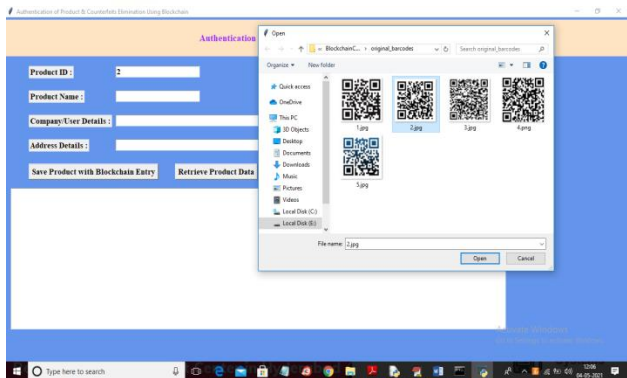


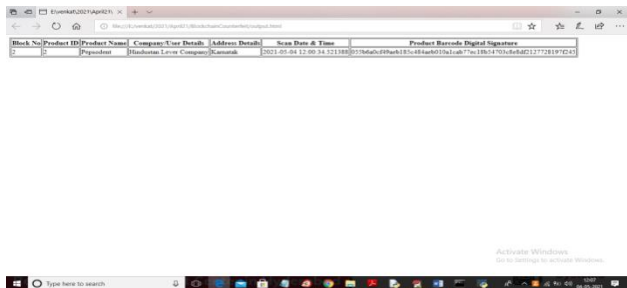
Fig.3.1. System Design model.

To avoid this problem author using Blockchain technology which does not require any third party and verification will be done by software algorithm itself without involvement of any third party. In this to avoid forge counterfeit

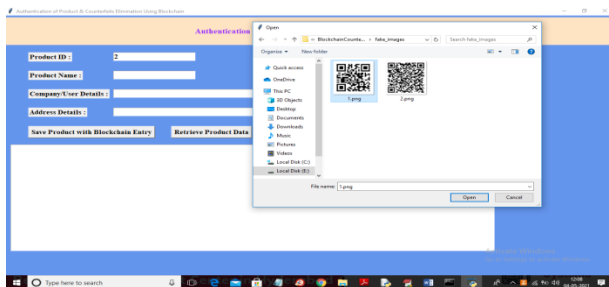
we are converting all products details/barcode into digital signatures and this digital signatures will be stored in Blockchain server as this Blockchain server support tamper proof data storage and nobody can hack or alter its data and if by an chance if its data alter then verification get failed at next block storage and user may get intimation about data alter. In Blockchain technology same transaction data stored at multiple server with hash code verification and if data alter at one server then it will detected from other server as for same data hash code will get different. For example in Blockchain technology data will be stored at multiple servers and if malicious users alter data at one server then its hash code will get changed in one server and other servers left unchanged and this changed hash code will be detected at verification time and future malicious user changes can be prevented. In supply chain also all products barcode digital Blockchain signatures will be stored and if any third party distributor make clone of barcode then its signature will be mismatch and counterfeit will be detected. In Blockchain each data will be stored by verifying old hash codes and if old hash codes remain unchanged then data will be consider 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.



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



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



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



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

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.

REFERANCES

- [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].