ISSN [Online]: 2583-2654

Counterfeit Product Identification using Blockchain Technology

[1]Leelavathy S R,[2]Manoj Kumar KN, [3]Naveen Sai Kumar, [4]Praveen R
Department of Computer Science and Engineering,
Dr. TTIT

***Abstract*:** Block chain technology is an open distributed ledger that can record transaction of peers. As it is distributed, Block chain is typically managed by peer-to-peer network. Working simultaneously to solve complex mathematical problems in order to validate new blocks. In Block chain each block will be hashed and that hash value will be used for linking new block, even transactions of the block also get hashed and Merkle tree is used to keep track of hash values of transaction by making all hash values of tractions into single hash value.The proposed system is capable of detecting the counterfeit products, using the QR code which is embedded on the product which provides the information of the product by using block chain technology. We described block chain with product anti-counterfeiting in that way manufactures can use this system to provide genuine product without having to manage direct operated stores.Now a day's fake products are floating a lot in the market. They are sold at cheaper rates than original products. Sometimes, they are even sold at the same rate. Block chain has a way to prevent such malpractices too.

Keywords: Block chain technology, peer to peer network, hash value, Merkle tree, QR code, counterfeit, anti-counterfeiting, malpractices.

I. INTRODUCTION

1.1 *Blockchain*

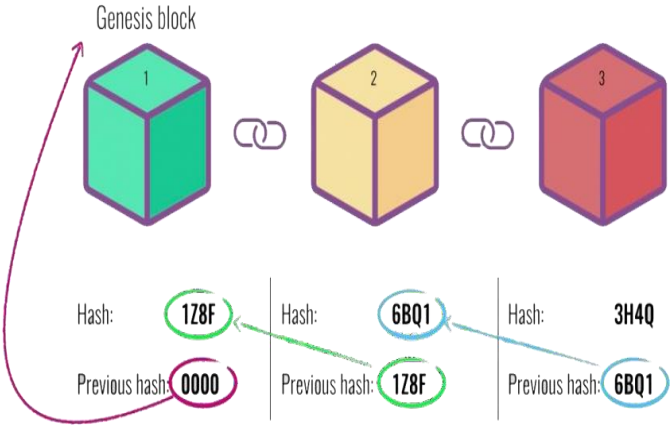
Blockchain[1][2][3]is a growing list of records, called blocks, connected using cryptography. [1][6] Each block contains a cryptographic hash of the previous block, [6] a timestamp, and a transaction. By design, blockchain is resistant to modification of its data. This is because once recorded, the data in any given block cannot be converted systematically without modification of all subsequent blocks. For use as a distributed ledger, the blockchain is simply managed by a peer-to-peer network that adheres to the inter-node communication protocol and secures new blocks. Although blockchain records are unchanged, blockchains can be considered secure by design and serve as an example of a highly distributed Byzantine computer program with high tolerance. The blockchain has been described as an "open, distributed ledger that can record transactions between two parties efficiently and in a guaranteed and permanent manner".

A blockchain is a duplicate, distributed, and often public, a digital document containing blocks called records that are used to record transactions on multiple computers so that any block involved can be converted backward, without having to change all the following blocks. [1][17] This allows participants to verify and evaluate the process independently and inexpensively. [18] The blockchain website is independently managed using a peer-to-peer network and a distributed timestamp server. They are evidenced by the multiplicity of interactions powered by collective desires. [9] Such a design facilitates robust performance where participant uncertainty regarding data security is limited. The use of a blockchain removes the element of unlimited production in digital assets. It ensures that each unit of value is transferred only once, solving a problem that has long been used twice. The blockchain is defined as the exchange rate protocol. The blockchain can retain title rights because, when properly set up to provide information on an exchange agreement, it provides a record that enforces the offer and acceptance.

Blocks that hold a set of valid missions are missing and coded in the Merkle tree. [1] Each block inserts a cryptographic hash of the previous block into the blockchain, which links the two. Connected blocks form a series. [1] This repetition process ensures the integrity of the previous block, all the way back to the original block, known as the genesis

ISSN [Online]: 2583-2654

block.Sometimes different blocks can be made at the same time, forming a temporary fork. In addition to hash-based secure history, any blockchain has a specific algorithm for hitting different versions of history so that a person with high scores can be selected over others. Blocks that are not selected for chain placement are called orphan blocks. Peer-supported peer-to-peer database has different types of



history from time to time. They maintain only the highest quality database known to them.

Fig.1: Block chain

1.2 *History of Blockchain*

Cryptographer David Chaum first proposed a blockchain-like rule in his 1982 book "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups". [10] Additional work on a series of over-guaranteed blocks was described in 1991 by Stuart Haber and W Scott Stornetta. They wanted to use a system where the time stamps of the texts were not disturbed. In 1992, Haber, Stornetta, and Dave Bayer incorporated Merkle Trees into the project, which improved their performance by allowing several text certificates to be collected in one block.

The first blockchain was invented by a man (or group of people) known as Satoshi Nakamoto in 2008. Nakamoto has improved the design in a significant way using Hashcash as a way to make time stairs without having to sign a trustworthy team and introduce a difficulty parameter to stabilize the rate at which the blocks are placed in the chain. The design was launched the following year by Nakamoto as a major component of the cryptocurrency bitcoin, where it serves as a public logger of everything that is done on the network.

In August 2014, the file size of the bitcoin blockchain, which contained records of everything done on the network, reached 20 GB (gigabytes). By January 2015, the size had grown to almost 30 GB, and from January 2016 to January 2017, the bitcoin blockchain grew from 50 GB to 100 GB in size. Lower size exceeded 200 GB by early 2020.The words block and series were used separately in Satoshi Nakamoto's first paper but became known as a single word, blockchain, in 2016.

According to Accenture, the application for the spread of innovation theory suggests that blockchains acquired a 13.5% acquisition rate within financial services in 2016, thus reaching the first phase of adoption. Industrial trade groups have joined the creation of the Global Blockchain Forum in 2016, which is an initiative of the Chamber of Digital Commerce.

In May 2018, Gartner found that only 1% of CIOs their organizations, and only 8% of CIOs were in a short period of time "planning or [considering] active blockchain testing". [16]

II. LITERATURE SURVEY

Satoshi Nakamoto [1] 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 network itself requires minimal structure.Ralph C. Merkle [2] proposed a New Cryptographic protocol which take full advantage of the unique properties of public key cryptosystems are now evolving. Several protocols for public key distribution and for digital signatures are briefly compared with each other and with the conventional alternative. Ahmed Kosba [3] present Hawk, a decentralized smart contract system that does not store financial transactions in the clear on the blockchain, thus retaining transactional privacy from the public's view. The formal modeling is of independent interest.Benjamin W. Akins [4] explores the current state of the law as it relates to bitcoins as well as proposed methods for applying existing federal

ISSN [Online]: 2583-2654

income tax laws to the virtual economy. Based upon the current state of the law and the information available on the various systems through which bitcoins may flow, the article sets forth a series of recommendations as to the proper federal income tax treatment of bitcoin transactions and suggests methods for addressing the compliance issues related to these transactions. Hiroshi Watanabe [5] propose a design in which a digitally signing, location-constrained and tamper-evident reader atomically writes an evidence to blockchain along with its reading and writing a tag. This makes it possible to trace authentic logistics information using inexpensive passive RFID tags. Furthermore, by abstracting the reader/writer as a sensor/actuator, this model can be extended to IoT in general. Kentaroh Toyoda [6] propose a novel product ownership management system (POMS) of RFID-attached products for anti-counterfeits that can be used in the post supply chain. For this purpose, we leverage the idea of Bitcoin's blockchain that anyone can check the proof of possession of balance.Jinhua Ma [7] uses the decentralized Blockchain technology approach to ensure that consumers do not fully rely on the merchants to determine if products are genuine. We describe a decentralized Blockchain system with products anti-counterfeiting, in that way manufacturers can use this system to provide genuine products without having to manage direct-operated stores, which can significantly reduce the cost of product quality assurance.Dong-Her Shih [8] states that Blockchain technology has evolved over the past decade; however, this has also resulted in some malicious attacks.The decentralized system of blockchain enables users to identify and participate in verification of mining sites through Ethereum smart contracts.Ralph C. Merkle [9] proposed A new digital signature based only on a conventional encryption function is described which is as secure as the underlying encryption functionthe security does not depend on the difficulty of factoring and the high computational costs of modular arithmetic are avoided. Pierre Margot [10] state medicine counterfeiting is a serious worldwide issue, involving networks of manufacture and distribution that are an integral part of industrialized organized crime. Despite the potentially devastating health repercussions involved, legal sanctions are often inappropriate or simply not applied.

III. ALGORITHM USED

(a) *Consensus Algorithm*

A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the distributed ledger.In this way, consensus algorithms achieve reliability in the Blockchain network and establish trust between unknown peers in a distributed computing environment.Essentially, the consensus protocol makes sure that every new block that is added to the Blockchain is the one and only version of the truth that is agreed upon by all the nodes in the Blockchain. PoW (Proof of work) is a consensus policy used in the Bitcoin network.Proof of stake (PoS) had mentioned in the primary bitcoin project, but it wasn't used due to robustness and further reasons.

(b) *Proof of Stake*

Proof-of-stake is a method of maintaining the integrity of a cryptocurrency, preventing users from printing extra coins they didn't earn. While a different method, called proof-of-work, is currently used by Bitcoin and Ethereum – the two largest cryptocurrencies by market capitalization – Ethereum has plans to migrate to proof-of-stake to make the platform more scalable and reduce energy consumption of the network.

Both proof-of-work and proof-of-stake are what are called "consensus mechanisms," the method by which a blockchain maintains its integrity. Consensus is what addresses the "double spending" problem of digital money. If there were any way the user of a cryptocurrency could spend their coins more than once, it would undermine the entire system. The currency would be worthless.

(c) *For User Authentication: RSA*

In addition, for some operations it is convenient that the order of the two exponentiations can be changed and that this relation also implies: RSA involves a public key and a private key. The public key can be known by everyone, and it is used for encrypting messages. The intention is that messages encrypted with the public key can only be decrypted in a reasonable amount of time by using the private key. The public key is represented by the integers n and e;

ISSN [Online]: 2583-2654

and, the private key, by the integer d. m represents the message.

(d) *For Block Chain Encryption SHA-256*

Secure Hash Algorithm, also known as SHA256.
These are a family of cryptographic functions designed to keep data secured. It works by transforming the data using a hash function: An algorithm that consists of bitwise operations, modular additions, and compression functions. SHA-256 is one of the successor hash functions to SHA-1 (collectively referred to as SHA-2), and is one of the powerful hash functions available. SHA-256 is not much more complex to code than SHA-1, and has not yet been agreed in any way. The 256-bit key creates it a good partner-function for AES.

(e) *Merkle Tree*

Merkle treealso known as hash tree is a data structure used for data verification and synchronization It is a tree data structure where each non-leaf node 15 a hash of its child nodes All the leaf nodes ate at the same depth and are as far left as possible. Merkle tree is a fundamental part of blockchain technology It Is a mathematical data structure composed of hashes of different blocks of data, and which serves as a summary of all the transactions in a block. Is Also allows for efficient and secure verification of content in a large body of data It also helps to verify the consistency and content of the data. Both Bitcoin and Ethereum use Merkle Trees structure, Merkle Tree is also known as Hash Tree.

IV. ARCHITECTURE

The block diagram describing the activities performed by this project. Before you build a computer, you should conceptualize the purpose and the structure. It's a conceptual method that defines the structure, behavior, and more views of a system. Scan QR Code tag of the Product using any scanner present on a mobile phone. 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**.**

User is able to view the scan history to check for any anomalous scan history.

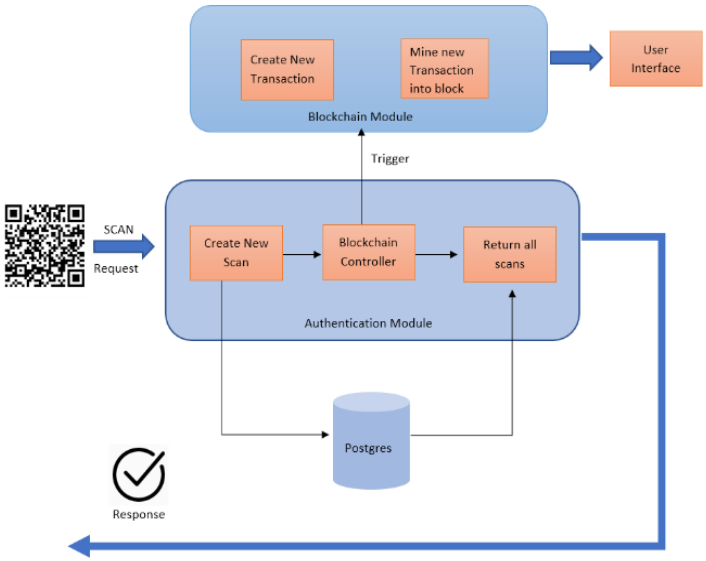


Fig.2: Core Architecture: Authentication module connecting database and blockchain

V. DATA FLOW DIAGRAM

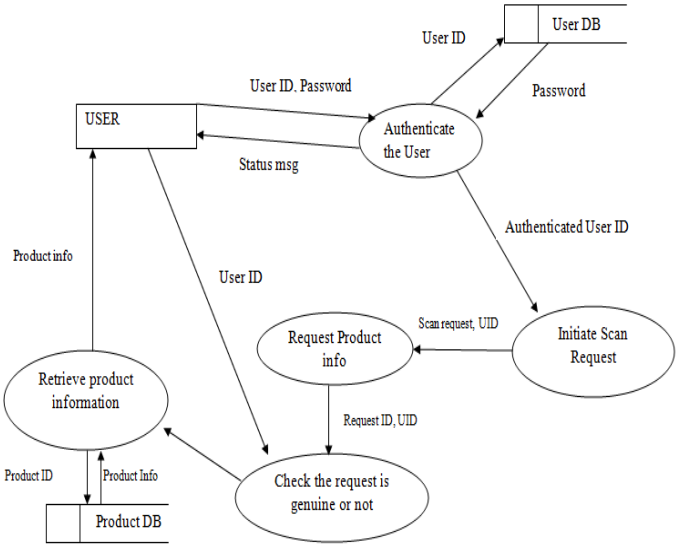


Fig. 3: DataFlowDiagram

VI. METHODOLOGY

The proposed Blockchain technology has emerged to provide a promising solution for such issues. We propose the block-supply chain, a new decentralized supply chain that detects counterfeiting attacks using

ISSN [Online]: 2583-2654

blockchain and QR Code 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.

6.1 *Results*

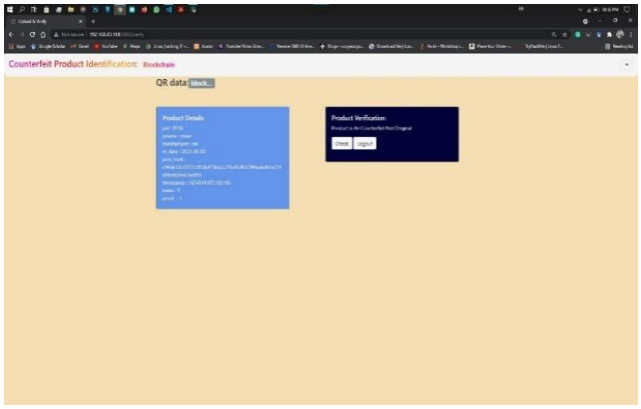


Fig. 4: Verifying the product is original or not

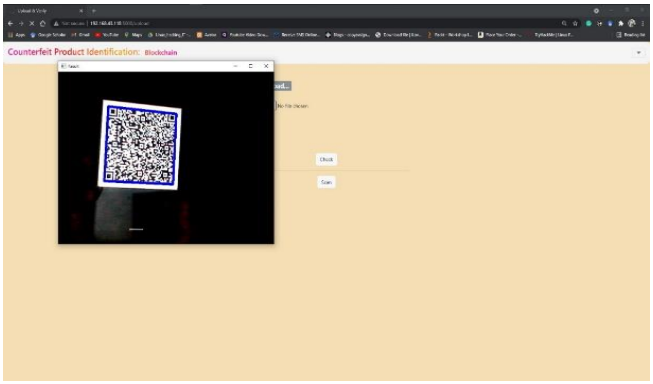


Fig. 5: Scanning QR Code in user device camera

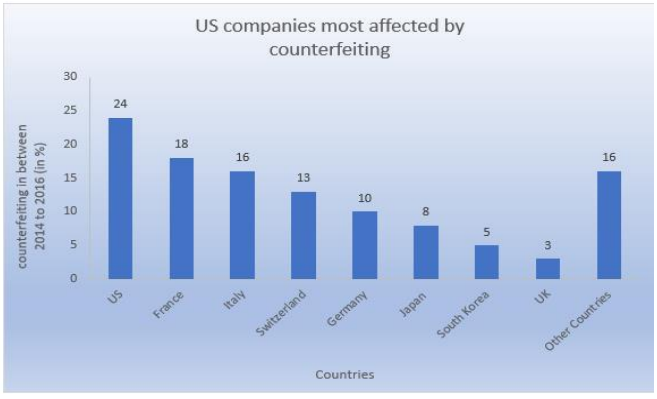


Fig6: The bar graph represents the US companies of other countries which are affected by counterfeiting in terms of percentage in between 2014 to 2016.

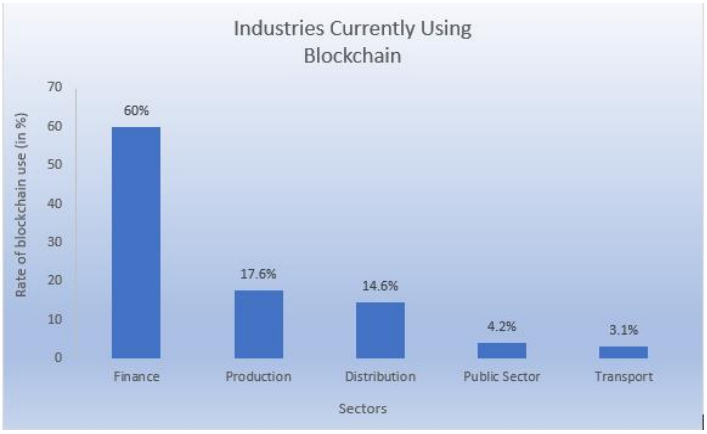


Fig7: The bar graph represents the rate of block chain use in different sectors of the industries.

VII. CONCLUSION

With this system, the products journey from manufacturing to customer can be recorded, and the customer is assured that the scans were not faked. Manufacturer 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.Users must be guaranteed that they only use true Authentication Apps. This use of the blockchain gives power to the user by allowing them to ensure that what they are paying for is authentic product and not counterfeit product. That is value for money.

REFERENCES

[1]. Satoshi Nakamoto, “Bitcoin: A peer-to-peer electronic cash system”, vol. 4, no. 8, pp. 11-14, 2008.

[2]. Ralph C. Merkle, “Protocols for public key cryptosystems”, In 1980 IEEE Symposium on Security and Privacy, pp. 122-122, IEEE, 1980.

[3]. Ahmed Kosba, Miller, A., Shi, E., Wen, Z., & Papamanthou, C., “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts”, IEEE symposium on security and privacy (SP), pp. 839-858, IEEE, 2016.

[4]. Benjamin W. Akins, Jennifer L. Chapman, and Jason M. Gordon, “A whole new world: Income tax considerations of the Bitcoin economy”, Pittsburgh Tax Review, vol. 12, no. 53, pp. 25-40, 2014.

[5]. Hiroshi Watanabe, Kenji Saito, Satoshi Miyazaki, Toshiharu Okada, Hiroyuki Fukuyama, Tsuneo Kato and Katsuo Taniguchi, “Proof of Authenticity of Logistics Information with Passive RFID Tags and Blockchain”, IEEE, vol. 1, no. 42, pp. 54-66, 2020.

ISSN [Online]: 2583-2654

[6]. Kentaroh Toyoda, Mathiopoulos, P.T., Sasase, I. and Ohtsuki, T., "A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain", IEEE, vol. 5, no. 74, pp. 17465-17477, 2017.

[7]. Jinhua Ma, Shih-Ya Lin, Xin Chen, Hung-Min Sun, Yeh-Cheng Chen, and Huaxiong Wang, "A Blockchain Based Application System for Product Anti-Counterfeiting", IEEE, vol. 8, no. 76, pp. 77642-77652, 2020.

[8]. Dong-Her Shih, Ting-Wei Wu, Tzu-Hsin Hsu, Po-Yuan Shih, and David C. Yen, "Verification of Cryptocurrency Mining Using Ethereum", IEEE, vol. 8, no. 35, pp.120351-120360, 2020.

[9]. Ralph C. Merkle, "A digital signature based on a conventional encryption function", In Conference on the theory and application of cryptographic techniques, pp. 369-378, 1987.

[10]. Dégardin, Klara, Yves Roggo, and Pierre Margot, "Understanding and fighting the medicine counterfeit market", Journal of pharmaceutical and biomedical analysis, vol. 87, pp. 167-175, 2014.

[11]. Wood, G, "Ethereum: A secure decentralised generalised transaction ledger". Ethereum project yellow paper, vol. 2, no. 151, pp. 1-32, 2014.

[12]. M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery", ACM Trans. Compute. Syst., vol. 20, no. 4, pp. 398-461, Nov 2002.

[13]. Cachin, C. "Architecture of the hyperledger blockchain fabric". In Workshop on distributed cryptocurrencies and consensus ledgers, vol. 310, no. 4, pp. 255-260, 2016.

[14]. Li, L. "Technology designed to combat fakes in the global supply chain". Business Horizons, vol. 56, no. 2, pp. 167-177, 2013.

[15]. Berman, B. "Strategies to detect and reduce counterfeiting activity". Business Horizons, vol. 3, no. 51, pp. 191-199, 2008.

[16]. Dégardin, K., Roggo, Y., and Margot, P. "Understanding and fighting the medicine counterfeit market". Journal of pharmaceutical and biomedical analysis, vol. 87, no. 11, pp. 167-175,2014.

[17]. Leng, J., Jiang, P., Xu, K., Liu, Q., Zhao, J.L., Bian, Y. and Shi, R., "Makerchain: A blockchain with chemical signature for self-organizing process in social manufacturing". Journal of Cleaner Production, vol. 234, no. 76, pp. 767-778, 2019.

[18]. Alzahrani, Naif, and Nirupama Bulusu. "Block-supply chain: A new anti-counterfeiting supply chain using NFC and blockchain". In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, pp. 30-35, 2018.

[19]. Tian, Feng. "An agri-food supply chain traceability system for China based on RFID & blockchain technology". In 2016 13th international conference on service systems and service management (ICSSSM), pp. 1-6, 2016.