GENUINE PRODUCT VERIFICATION SYSTEM USING BLOCKCHAIN TECHNOLOGY

Dr. N V Shibu[1], Gokulakrishna H[2], Gowtham P[3], KarthickKumar K[4]

[1] *Associate Professor, Department of Computer Science and Engineering, Sri Ramakrishna Institute Of Technology, Tamil Nadu, India*
[2] *Student, Department of Computer Science and Engineering, Sri Ramakrishna Institute Of Technology, Tamil Nadu, India*
[3] *Student, Department of Computer Science and Engineering, Sri Ramakrishna Institute Of Technology, Tamil Nadu, India*
[4] *Student, Department of Computer Science and Engineering, Sri Ramakrishna Institute Of Technology, Tamil Nadu, India*

ABSTRACT

Anti-counterfeit technology has attracted much attention with the development of economy. Many counterfeit products that are difficult for identification have been produced, which extremely damage the interests of consumers. The public's attitude of greedy for petty and cheap has encouraged unscrupulous manufacturers to take advantage of the opportunity to provide low-cost counterfeit products, suppress the profits of legitimate manufacturers, and also make the public lose confidence in the quality of the products. At present, the most widely used anti-counterfeiting system is based on QR codes available in the market. However, existing traceability systems are still mostly built in a centralized manner, and the central agency provides trust guarantees, but the public still has great doubts about the credibility of the central agency. The introduction of blockchain technology can perfectly solve the lack of existing architecture and the environment. To ensure the identification and traceability of real products throughout the supply chain, this project propose a fully functional blockchain system to prevent product counterfeiting. This project proposes the 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. The proposed method can significantly reduce the cost of product quality assurance and validation.

Keyword: - *Anti-counterfeit technology, QR codes, Blockchain technology*

1. INTRODUCTION

Counterfeiting is the manufacture, import, export, distribution, and sale of consumer goods that are not genuine but are designed and branded to look identical to the authentic products. It is done in order to deceive consumers into believing that they are authentic. Counterfeiting also includes affixing the trademark or logo of a well-known consumer brand to a product, even though the product is not actually made or authorized by that brand. In simple terms, counterfeits are imitations of real products that are manufactured without approval from the owner of the

brand. Counterfeit products are usually of substantially lower quality than the authentic goods and can even be dangerous, as they are often poorly made or made using dangerous or toxic chemicals and materials. Counterfeit products range from high-end consumer luxury goods such as watches, perfumes or leather goods, to business-to-business products such as machines, chemicals or spare parts, to common consumer products such as toys, pharmaceuticals, cosmetics and foodstuffs. In fact, any IP-protected product can be counterfeited. Unfortunately, many well-known and successful companies, spanning just about every industry, fall victim to counterfeiting.

1.1 History of Blockchain

Blockchain isn't just a database, it's a new technology stack with 'digital trust' that is revolutionizing the way we exchange value and information across the internet, by taking out the 'gatekeepers' from the process. The first blockchain-like protocol was proposed by cryptographer David Chaum in 1982. Later in 1991, Stuart Haber and W. Scott Stornetta wrote about their work on Consortiums. But it was Satoshi Nakamoto (presumed pseudonym for a person or group of people) who invented and implemented 4 the first blockchain network after deploying the world's first digital currency, Bitcoin. Because blockchain technology is the technology behind the blockchain, it cannot be owned. It's like the internet. But anyone can use the technology to run and own their own blockchains.

1.2 Problem Statement

Counterfeiting is not a victimless crime. Counterfeiters often prey on consumer desire for low prices. Purchasing counterfeit products may seem like a cheap option in place of the real thing, but that low price comes at a high cost to yourself and others. The Manufacturing organizations operating under legal provisions are threatened by counterfeiting because it causes loss in their revenue. Counterfeiting can happen with local as well as branded products. Counterfeit and inferior products disregards the safety of its consumers. Counterfeit products degrades the economy. A vendor-based product verification portal has several limitations including security breaches and inaccessibility in the long run.

1.3 Existing System

Most companies who value their brand and business have track-and-control mechanisms in place to deter, if not eliminate, counterfeit production and distribution. This includes hologram stickers, watermarks, mass communication, surprise checks, controlled distribution systems, and robust ERP system implementations. Counterfeit identification using QR code on smartphones - The solution involves a simple QR code- based identification that can help the end-user and the company salesman to scan and identify the genuineness of the product by using a smartphone. Anti-counterfeit solutions based on NFC technology - The customer can use their smartphones with the NFC feature to tap and read the data on the NFC chip on the product for checking its authenticity. RFID-Based Anti-Counterfeiting Track and Trace Solution - Radio frequency identification is done by using tiny chips which emit electromagnetic fields to automatically identify and track tags attached to objects. Anti-counterfeiting method based on RFID electronic label - According to the method, binding is carried out between an ultrahigh frequency electronic label and a product that needs an anti-counterfeiting process.

1.4 Proposed System

In the proposed Blockchain-based Anti-Counterfeiting, each of the stake- holders (e.g., suppliers, producers, factories, logistics items retailers and consumers, etc.) joins as Blockchain node to make Blockchain transactions as well as participate in keeping Blockchain up to date. On joining the Blockchain, each node is given a public/private keypair to process secure cryptographic operations according to Blockchain architecture. The particular transaction is first created or generated by the system passed to all stakeholders who view and authenticate it. For authentication purposes, the transaction initiator signs the transaction with its private key which is further validated by each other processing node (stakeholder) with the public key of the initiator. Once the transaction is established on the network, the transaction block is added as a new block to the existing blocks in the Blockchain by using a suitable consensus mechanism. In the proposed architecture, it is recommended to use Proof of Supply Chain Share (PoSCS) as a consensus mechanism which is based on Proof of Stake (PoS). The other popular consensus mechanism like Proof of Work (PoW) and PoS may not be suitable for product SCM due to the high demand for computational resources and wealth in the distributed network. Each block in this chain keeps the hash address of the next neighbor. The last block in this data structure does not point to any other block. In creating and authenticating a new block, the previous block of the existing chain points to the newly created block.

We propose a decentralized blockchain with know your product code for our system. In our system there will be four stakeholders including Manufacturer, Distributor, Retailer, Consumer. To participate in the system, every stakeholder needs to generate a keypair of EOA (Externally owned Account) and KYPC.

Know Your Product Code Blockchain-Enabled Product Anti- Counterfeiting - Each and every product will have a pair of global Id and unique Id in the manufacturing unit to identify the product in the Manufacturing Unit generated using KYPC Generator anti-counterfeiting identification code, and other information of the product are added to the blockchain.

Block Genuine verify is powered by an advanced blockchain protocol that ensures secure storage of data on the product's manufacturer and origin. It allows tracking and monitoring products from production lines to distribution centers to the point of sale and the consumers.

A blockchain supply chain can help participants record price, date, location, quality, certification, and other relevant information to more effectively manage the supply chain. The availability of this information within blockchain can increase traceability of material supply chain, lower losses from counterfeit and gray market, improve visibility and compliance over outsourced contract manufacturing, and potentially enhance an organization's position as a leader in responsible manufacturing.

2. LITERATURE REVIEW

[1] "Optimized Combination of e-commerce Platform Sales Model and Blockchain Anti-Counterfeit Traceability Service Strategy", Fangfang Guo, Deqing Ma, Jinsong Hu, Lu Zhang, 2021 - This paper has the limitation of not including wholesale price as a decision variable for suppliers. Also, future research can consider consumer surplus and social welfare based on our model and analyses which case generates higher consumer surplus and social welfare.

[2] "An IoT-Based Anti-Counterfeiting System Using Visual Features on QR Code", Yulong Yan; Zhuo Zou; Hui Xie; Yu Gao; Lirong Zheng, 2021 - The proposed system is affordable and deployable. The generation process of these features can be adapted to the existing assembly line, without extra cost for manufacturers. The easy-to-use verification application can be deployed on consumer level end devices like mobile phones or handheld code readers. The verification approach is fully compatible with the logistic process based on QR codes.

[3] "An IoT-Based Traceable Drug Anti-Counterfeiting Management System", Chin-Ling Chen; Yong-Yuan Deng; Chun-Ta Li; Shunzhi Zhu; Yi-Jui Chiu; Pei-Zhi Chen, 2020 - The framework the author proposes meets the requirements of information security for data integrity, resistance to replay attacks, irreversible information, and nonrepudiation. Through the integration of the Internet of Things and blockchain technology, in addition to achieving the main purpose of the anti-counterfeiting of drugs, it has also achieved the goal of automated management of the overall supply chain.

[4] "Lightweight Authentication Protocol for NFC Based Anti-Counterfeiting System in IoT Infrastructure", Bander A. Alzahrani; Khalid Mahmood; Saru Kumari, 2020 - The scheme helps to check the validity of the drugs. It has been demonstrated that our proposed protocol is able to resist all the known attacks while preserving the novel approaches and functionalities. Furthermore, the security analysis shows that proposed protocol offers a better security and thus protect against most common attacks. The analysis of performance evaluation and formal security indicates that our protocol is also comparably better in term of computation cost and communication overhead. Additionally, the protocol has been evaluated using Py-Charm tool. In general, proposed scheme can be considered suitable for the anti-counterfeited medicines for added security features it provides.

[5] "A Novel RFID-Based Anti-Counterfeiting Scheme for Retail Environments", Ghaith Khalil; Robin Doss; Morshed Chowdhury, 2020 - The motivation for this research is to develop an RFID anti-counterfeiting and anti-theft protocol which will enable a customer to detect any counterfeit goods or materials in a retail environment in a practical, less costly and more convenient manner than the existing schemes.

[6] "Fabrication of Dynamic Holograms on Polymer Surface by Direct Laser Writing for High-Security Anti-Counterfeit Applications", Jiahao Miao; Xinghuo Ding; Shengjun Zhou; Chengqun Gui, 2019 - Finally, a kinematic hologram was fabricated and analysed, kinematic effect of reconstructed image and difference of magnification between normal first order diffraction and negative first order diffraction were theoretically analysed and confirmed by experiment. The kinematic hologram was associated with a video which could be seen in ''Visualization 1'' in the supplementary materials. The characteristics of low cost, difficulty to duplicate, visible and attractive kinematic effect of reconstructed image, and simplicity for recognition made the hologram exhibited great potential in anti-counterfeit applications.

[7] "A Watermarking Technique to Secure Printed Matrix Barcode— Application for Anti-Counterfeit Packaging", Hoai Phuong Nguyen; Florent Retraint; Frédéric Morain-Nicolier; Angès Delahaies, 2019 - Counterfeiters need to have the digital codes and the same printing system as the constructor to produce valid secured codes, which is highly sophisticated. Furthermore, cloning an existing code by scanning and reprinting will change the behaviour of embedded texture, and can be detected. Then, by analysing the embedded texture, we can verify the validity of the printed QR codes, and by consequence, the Genuity of the related product.

[8] "Smart tags for brand protection and anti-counterfeiting in wine industry", Stevan Šandi; Sanja Radonjić; Jovana Drobnjak; Marko Simeunović; Biljana Stamatović; Tomo Popović, 2018 - Smart tags combine the use of QR code, functional ink printing, and advanced 21 Cloud solutions. Photochromic ink is still not widely available which makes counterfeiting hard and most likely unprofitable. Furthermore, the information encoded into the smart tags is combined with historical information about the status of the product in order to create additional layers of the security. In addition to brand protection and anti-counterfeiting, the proposed solution has a potential for additional use cases and applications based on the collected data and two-way interaction with the consumers.

3. REQUIREMENT SPECIFICATIONS

3.1 Software Requirements

- Server Side - Python 3.7.4 (64-bit) or (32-bit)
- Client Side - HTML, CSS, Bootstrap
- Framework - Flask 1.1.1
- Back end - MySQL 5
- Server - WampServer 2i
- BC DLL – PyChain, Node Package Manager, Virtualenv, BlockchainHash

3.2 Hardware Requirements

- Processors - Intel® Core™ i5 processor 4300M at 2.60 GHz or 2.59 GHz (1 socket, 2 cores, 2 threads per core), 8 GB of DRAM
- Disk space: 320 GB
- Operating systems: Windows® 10, macOS*, and Linux*

4. METHODOLOGY

4.1 System Architecture

A system architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system. Below Fig-1 shows System Architecture for Genuine Product Verification System.

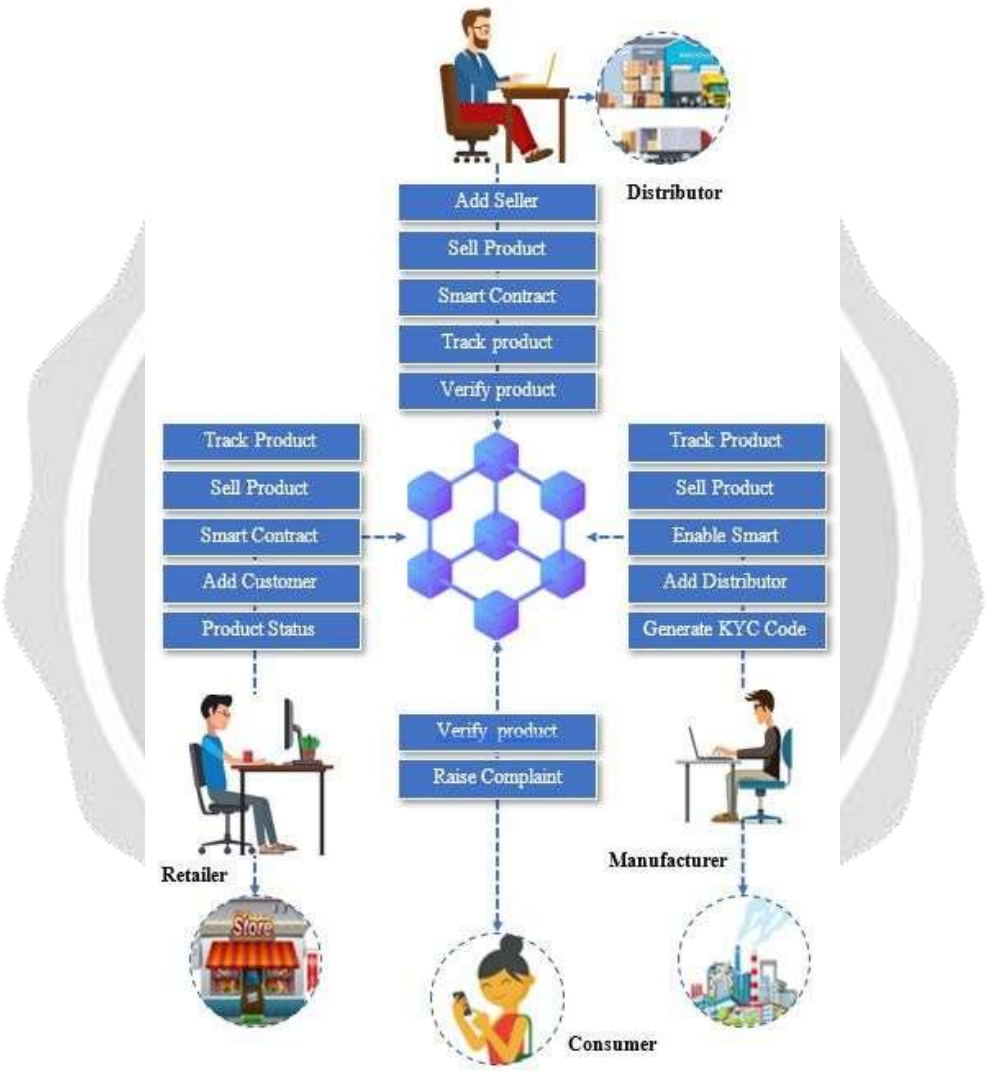


Fig -1: System Architecture of Genuine Product Verification System

4.2 System Flow

System Flows are systems models that show the activities and decisions that systems execute. They are useful for understanding complex system interactions because they visually show the back and forth interactions between systems and complex branching. Below Fig-2 shows System flow for Genuine Product Verification System.

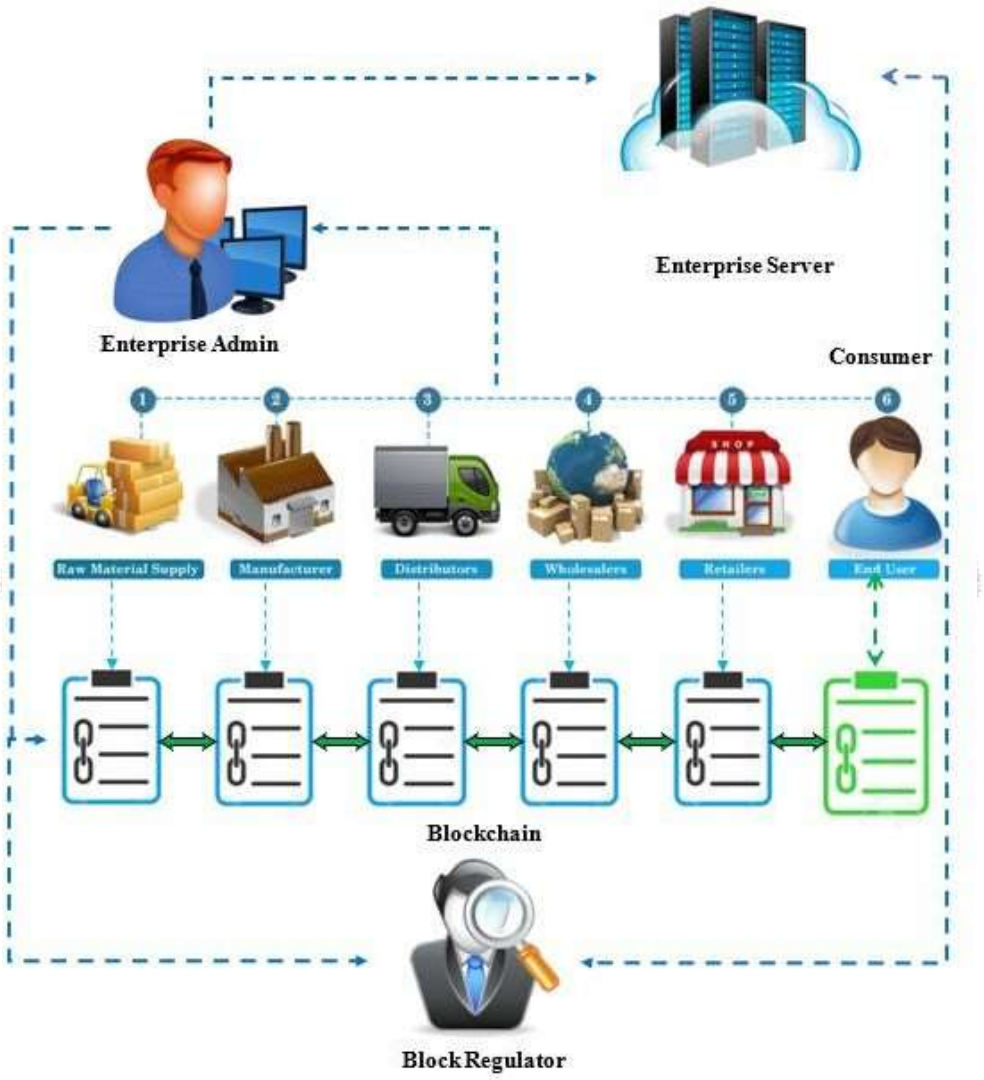
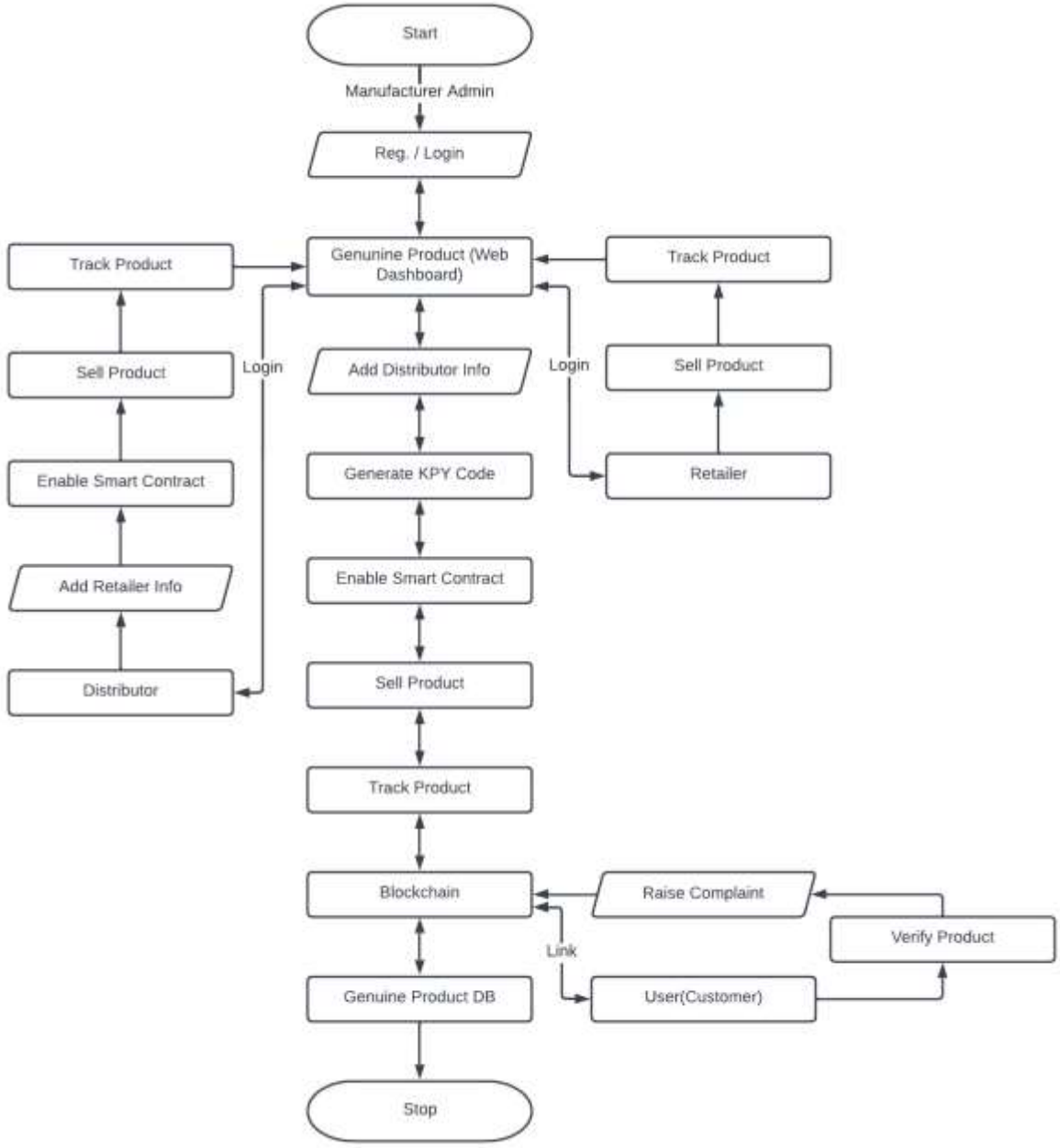


Fig -2: System flow for Genuine Product Verification System

4.3 Flowchart



4.4 Working Description

The Blockchain based systems for anti-counterfeit are realized by developing a portal for anti-counterfeit. The system is used by the manufacturers, retailers, distributors, and customers. Anti-counterfeit portal helps the end users such as distributors, retailers and consumers to check the authenticity of the product packet through computer or mobile device. The status of the product with particular KYPC (Know Your Product Code) can be verified by the customers. If the product with particular KYPC is not already sold and it is in the approved store then the customer is intimated through message that the product is genuine. This successful verification proceeds and the product purchase status is set to sold with the that particular KYPC. However, if the sold status is already found set then customer is immediately intimated that the product you are going to purchase is fake or tempered. Instantly an alert

message is also sent towards the manufacturer about this event. The authentication process is facilitated by a unique KYPC which is placed on each product. These properties help the customers to check whether the status of the product is set as sold in early or not. If the status is set earlier then obviously the drug product is counterfeited so in this way the system gives the warning to the manufacturer and the user. The information about the original product in the system must have to be maintained by manufacturer, so that the authentication is facilitated. Then the system engenders a unique KYPC for each item. The specific database of concerned system is used to keep the product related information. There are two important functions in anti-counterfeiting (1) Authentication (2) KYPC code tracking and generation. In this project, manufacturers can use this system to store relevant information on product sales in Blockchain which is accessible to anyone. The total amount of sales that can be sold by the seller and the number of products currently left by the seller are transparent to users. The user can use the functions provided by our system to immediately perform vendor-side verification, and this verification cannot be made. For retailers, it is possible to prove whether they provide genuine goods by using this anti-counterfeit Blockchain system and no longer have to be concerned about competing with counterfeits sold at low prices.

4.5 Modules

4.5.1 Anti-Counterfeit Web Portal

In order to develop the anti-counterfeit technologies and bring awareness on the corresponding information, an Anti-Counterfeit Portal is designed with multi-tier architecture methodology. In this module web dashboard for Product Anti Counterfeit is developed as a medium for customers to keep track of their products' origin via the Internet. This dashboard is a platform for sharing information within the entire product lifecycle. With the portal, all the product-related information can be decentralized in the blockchain and obtained via a secure web interface. With the KYPC provided by the authentication service provider on each product (which is affixed on the product), the consumers can query with the code provided through the authentication service provider's website to verify the product's information. Furthermore, with the help of log tracking capability, an excessive number of inquiries can identify the potential counterfeiting possibility. Together with the web portal and KYPC technology, it is possible to automate the data entry process and improve the detection of fakes within supply chain. With the fact that most companies plans to adopt Blockchain in their supply chain, numerous research activities focus on designing KYPC-based system for combating counterfeits.

4.5.2 Blockchain Integration

Blockchain module has two functions. One is the data interaction including the upload of key traceability information on blockchain, the request of on-chain information and the verification of event information. The other is to provide options for users to be the full blockchain node or the light-weight blockchain node i.e., to decide whether or not to participate in the maintenance of the blockchain. This module is designed for the link between the client and system, through which it can request information on the blockchain and verify the legitimacy of the information. A light node is chosen for this module to lower user's maintenance cost.

4.5.3 Smart Contract

Similar to a transfer of value on a blockchain, deployment of a smart contract on a blockchain occurs by sending a transaction from a wallet for the blockchain. The transaction includes the compiled code for the smart contract as well as a special receiver address. That transaction must then be included in a block that is added to the blockchain, at which point the smart contract's code will execute to establish the initial state of the smart contract.

4.5.4 End User Module

4.5.4.1 Manufacturer

The manufacturer purchases raw materials from the supplier and processes the raw materials to produce the products. At the same time, the manufacturer supplies products to the distributor, which are sold all over the world by the distributor. As the owner of the product, the manufacturer is responsible for encapsulating the product information and registering it in the system. In the design of this paper, we use the international coding standard KYPC to generate code for the product, and the product has a unique code. We assume that in the process of product

production, the products produced in the same batch are identical in quality and structure, and the difference can be ignored. Products that are produced in different batches need to be re-registered. Therefore, this design updates the product transfer process in batches, and each batch of products uniquely corresponds to a production batch number. For mass-produced products, they have the same batch number; for non-mass-produced products, the batch number represents the individual product.

4.5.4.2 Distributors

As the middleman in the process of transferring goods from the manufacturer to the end consumer, the main role of the distributor is to update the direction of the product flow in this process so that the product information remains uninterrupted during the traceability process.

4.5.4.3 Retailers

The retailer purchases products from the distributor in batches and sells them to consumers in retail, which is a participant that has direct trading relationships with consumers.

4.5.4.4 Consumers

The consumer is the individual who finally buys and uses the product. He can choose to participate in the network as a lightweight node, realizes the product traceability process by querying the data permanently stored in the block, or as a full node to jointly maintain the blockchain ledger data.

4.6 Consumer Traceability

4.6.1 KYPC Traceability Module

This module is designed for the link between the client and system, through which it can request information on the blockchain and verify the legitimacy of the information. A light node is chosen for this module to lower user's maintenance cost.

4.6.2 Information Cache Database

This cache database is built to cache the corresponding Drug traceability data requested by users.

5. RESULT AND DISCUSSION

To alleviate the data explosion problem, we use collaborative management of on-chain and off-chain data to successfully reduce the amount of data of single node. To protect the sensitive business information, we use the enterprise-level blockchain transactions instead of traditional transaction records to save and manage product data as well as verify the identity of enterprise. This project proposes the decentralized Block chain 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. The Customers can verify their product through this application by using the product’s KYPC code.

6. CONCLUSIONS

6.1 Summary

In this project, a genuine product verification system based on blockchain technology is proposed, in which all product transferring histories are perpetually recorded in the unchangeable ledger by using smart contracts on blockchain, and the process of product registration, transferring, tracking through verification is realized through the collaboration of smart contracts. Consumers can also join the network as full nodes or lightweight nodes so that all nodes in the whole supply chain can participate in the process of maintaining information flows. Our system has obvious decentralized characteristics, which significantly reduces the possibility of privately tampering with data within enterprises. Then through the thorough analysis of the major demands of system user, we designed a

decentralized system based on the blockchain and KYPC network. To alleviate the data explosion problem, we use collaborative management of on-chain and off-chain data to successfully reduce the amount of data of single node. To protect the sensitive business information, we use the enterprise-level smart contract instead of traditional transaction records to save and manage product data as well as verify the identity of enterprise. In this way, we can ensure the security of information and avoid spam attacks.

6.2 Recommendation for future project

To optimize the traceability system proposed in this paper is our future research work: Realize formatted upload of data by using IoT technology, reduce the possibility of manual input errors.

7. REFERENCES

[1] S. A. H. S. Amiri, A. Zahedi, M. Kazemi, J. Soroor, and M. HajiaghaeiKeshteli, ``Determination of the optimal sales level of perishable goods in a twoechelon supply chain network," Comput. Ind. Eng., vol. 139, Jan. 2020, Art. no. 106156, doi: 10.1016/j.cie.2019.106156.
[2] J. Sun, J. Tang, W. Fu, Z. Chen, and Y. Niu, ``Construction of a multiechelon supply chain complex network evolution model and robustness analysis of cascading failure," Comput. Ind. Eng., vol. 144, Jun. 2020, Art. no. 106457, doi: 10.1016/j.cie.2020.106457.
[3] A. Batwa and A. Norrman, ``A framework for exploring blockchain technology in supply chain management," Oper. Supply Chain Manage., Int. J., vol. 13, pp. 294-306, Apr. 2020, doi: 10.31387/OSCM0420271.
[4] M. Abdirad and K. Krishnan, ``Industry 4.0 in logistics and supply chain management: A systematic literature review," Eng. Manage. J., pp. 1-15, Jul. 2020, doi: 10.1080/10429247.2020.1783935.
[5] J. Yoon, S. Talluri, and C. Rosales, ``Procurement decisions and information sharing under multi-tier disruption risk in a supply chain,"Int. J. Prod. Res., vol. 58, no. 5, pp. 1362-1383, Mar. 2020, doi-10.1080/00207543.2019.1634296.
[6] D. Ivanov, ``Predicting the impacts of epidemic outbreaks on global supply chains: A simulation-based analysis on the coronavirus outbreak (COVID-19/SARSCoV-2) case," Transp. Res. E, Logistics Transp. Rev., vol. 136, Apr. 2020, Art. no. 101922, doi: 10.1016/j.tre.2020.101922.
[7] T. Sawik, ``Two-period vs. multi-period model for supply chain disruption management," Int. J. Prod. Res., vol. 57, no. 14, pp. 4502-4518, Jul. 2019, doi: 10.1080/00207543.2018.1504246.
[8] A. Alora and M. K. Barua, ``An integrated structural modelling and MICMAC analysis for supply chain disruption risk classification and prioritization in 32 India," Int. J. Value Chain Manage., vol. 10, no. 1, p. 1, 2019.
[9] V. Ahlqvist, A. Norrman, and M. Jahre, ``Supply chain risk governance: Towards a conceptual multi-level framework," Oper. Supply Chain Manage., Int. J., vol. 13, no. 4, pp. 382395, 2020, doi: 10.31387/oscm0430278.
[10] L. Luo, G. Q. Shen, G. Xu, Y. Liu, and Y. Wang, ``Stakeholder-associated supply chain risks and their interactions in a prefabricated building project in Hong Kong," J. Manage. Eng., vol. 35, no. 2, Mar. 2019, Art. no. 05018015, doi: 10.1061/(ASCE)ME.1943-5479.0000675.