

## IDENTIFYING COUNTERFEIT PRODUCTS USING BLOCKCHAIN TECHNOLOGY IN SUPPLY CHAIN SYSTEM

Pooja B. Fattepure\*<sup>1</sup>, Prof. Deepa Kulkarni\*<sup>2</sup>

\*<sup>1</sup>Department Of Computer Engineering, SPPU, Pune, India.

\*<sup>2</sup>Department Of Computer Engineering, SKNCOE, SPPU, Pune, India.

DOI : <https://www.doi.org/10.56726/IRJMETS53132>

### ABSTRACT

Abstract: These days, anything can be searched for and found out about thanks to technology. The greater the number of individuals within the community who utilize machine learning technology, the more data can be collected. There are currently many cases of cosmetic circulation violations in Indonesia. One example would be the distribution of products that have been fraudulently created by untrustworthy parties and lack a BPOM (Food and Drug Supervisory Agency) registration code. In addition to the many examples of cosmetic violations, there have also been changes in people's behaviors, such as changing patterns of consumption (users). The general public still lacks a great deal of knowledge regarding the safe selection and use of cosmetics. Applications for cosmetic safety checks are available to consumers, who can use them to independently verify whether the products they intend to use are genuine or fraudulent. The research methodology employed in this study is the waterfall approach combined with qualitative techniques. This programme aims to enable the public to quickly ascertain the authenticity of cosmetic products before making a purchase by simply scanning the barcode.

**Keywords:** Barcode, QR Code, BPOM, Fake Product Detection, Simply Scanning The Barcode Etc.

### I. INTRODUCTION

According to UN estimates, the global market for counterfeit goods is estimated to be worth US\$250 billion annually<sup>1</sup>. Counterfeiting poses a threat to almost every business, resulting in decreased revenue and damage to brand reputation.

Because of these losses, companies often are unable to recover their RD investments, which restricts their capacity to produce meaningful products going forward. Another school of thought holds that counterfeit goods help finance organized crime in some nations; any respectable business would not want to be connected to this. Counterfeit goods put consumers at risk, and some products can be deadly or seriously harmful to their health. When it comes to medical supplies or kid's toys, consumers may find it challenging or even dangerous to identify counterfeit goods. We'll talk about the topic of fake domains and concentrate on the areas where using IT technology can be beneficial. After introducing the relevant works, we will outline the solution concept and technical architecture and then concentrate on the challenges associated with implementing and evaluating such solutions.

In recent years, the global distribution of counterfeit goods has increased. There are a lot of fake products in the current supply chain. According to the survey, there has been a recent increase in the incidence of fake goods. Establishing a system that enables purchasers or users to confirm all product specifications is crucial in order for them to ascertain the authenticity of the item. India does not currently have a system in place to recognize counterfeit goods. As a result, the solution consists of a simple QR code-based identification that can help customers or end users scan and confirm the authenticity of the product using a smartphone. In this work, the supplier, user, and company modules of a blockchain-based supply chain management system were designed and developed. The blockchain stores every transaction, preventing network data attacks in the peer-to-peer (P2P) environment for systems that identify counterfeit goods.

#### Objectives:

The idea of this project came into existence because of the increase in the counterfeit products. The objectives of this project are:

The Complete solution to Counterfeit Products.

To Increase Awareness.

To Lower the rate of Fraud.

To Make customer happy and satisfied.

To design an approach for Identifying company product counterfeit where the system historical data in a QR Code manner detection

To create a distributed computing environment hierarchy for parallel data processing for efficient data extraction.

To build and develop one's blockchain to securely store all transaction data

To implement a verification algorithm which can validate each peer on every access request.

## II. RELATED WORK

1. Approvals significant and referenced are joined with an additional six ascribes from the manifest and the destroyed code in DREBIN [1]. Man-made intelligence computations are used to get a handle on the difference among dangerous and innocuous ventures normally. When arranged detached on a serious machine, the Assist Vector With machining is essentially conveyed the learnt model to the cell for perceiving risky applications.
2. In these[2] they investigate the reasonableness of distinguishing underhanded Android applications using consents and 20 features from application gatherings. According to their disclosures, a lone classifier can perceive around 81% of bogus undertakings. It may be a fast channel to recognize more suspect applications, according to them, by planning disclosures from a couple of classifiers.
3. Used the mentioned[3] and fundamental assents by an application similarly. Man-made intelligence computations and assents are used in this structure to group an application as innocuous or damaging.
4. As shown by [4] is a way for building computer based intelligence classifiers and recognizing malware by removing different properties from the Android manifest. These components are the specific per-missions searched for and the reasons feature; tag.
5. Presented [5] a construction for encouraging a simulated intelligence based malware de-tecton system for Android to perceive malware applications and further foster Cell clients' security and insurance. This structure accumulates different approval based properties and events from Android applications and assessments them using simulated intelligence classifiers to conclude whether the application is innocuous or vindictive.
6. Android[6] applications into two classes: utilities and games. Productive segment among games and gadgets, from their perspective, should offer a good characteristic of such structures' capacity to learn and show Android innocuous undertakings and maybe perceive mal-item reports using computer based intelligence (ML) strategies on static credits assembled from Android program records.
7. The writers of these books limit their assessment to the most often referenced assents (or a cer-tain selection of approvals) [7]. In any case, dependent upon the assault, assents like READ LOGS might be comparatively by and large around as dangerous as others (like Web). Each award should be care-totally assessed as having the ability to be unsafe when coordinated with another.
8. This technique for decision, as demonstrated by [8], makes broadly skewed results. Man-made intelligence based distinguishing proof strategies are seen to have two inconveniences: they have a high speed of fake issues, and picking which characteristics should be dominated during the planning stage is a problematic endeavor. The procedure of picking datasets for planning is thus a critical stage in these systems. The introduction of the classifier improves with time: for a particular month Mi, whose applications were used for the readiness datasets, the resultant classifier ends up being less and less fit for separating all malware.
9. To address the applications, the majority of these undertakings separate a rundown of capacities. The information passed on by such characteristics shifts depending upon the gig. There is no verification to show which credits give the best revelation results, however every assessment considers required per-missions. Moonsamy et al. [9] are enthused about including assents as the sole part to depict programs and perceiving explicit approval guides to perceive awesome and dangerous applications.

## III. METHODOLOGY

- The existing system has evolved into a centralized architecture similar to the single server base approach.
- System used inbuilt ethereum blockchain which is hard to update with custom logic.

Existing mining policy may generate additional difficulties to complete the entire transaction which generate overhead on the system.

Users:-In this System, Users is Customer which want to purchase the Products. The User can access the System and See the product. It can select the product and Scan the Product and see the product.

Admin:-The Admin can be the User/Manufacturer/Seller of the System, which can be add the product to the product list or it can be manage the product.

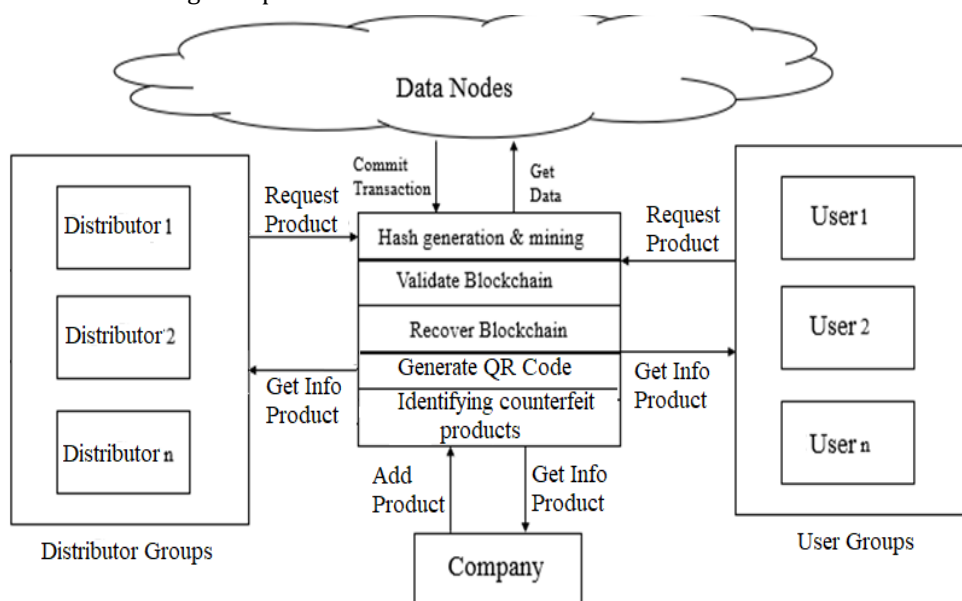


Figure 1: Architecture of System

The implementation of block chain data storage for product (medicine) supply chain distribution forms the core of the proposed algorithm. The system facilitates reliable communication between various stakeholders without requiring the use of an intermediary interface. The hash for the supplied string will be generated using the hash generation algorithm. Peer to peer verification is used to verify the data prior to carrying out any transaction. It will update or recover the current server blockchain if any chain is found to be invalid. This will continue to validate until the query is committed and all nodes are confirmed. Until a valid hash is generated, the mining algorithm is used to verify the hash generated.

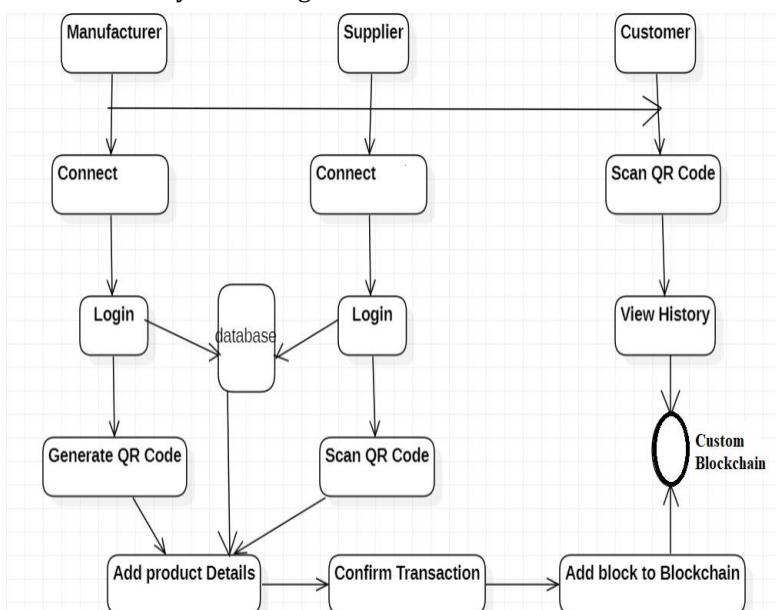


Figure 2: Activity Daigram

Activity diagram describes the flow of control in a system. So it consists of activities and links. The flow can be sequential, concurrent or branched. Activities are nothing but the functions of a system. Numbers of activity diagrams are prepared to capture the entire flow in a system. Activity diagrams are used to visualize the flow of controls in a system. This is prepared to have an idea of how the system will work when executed.

#### **IV. CONCLUSION**

There are multiple research avenues to apply Blockchain technology to the transaction industry due to the intricacies of this field and the demand for more reliable and effective information management frameworks. An interoperable architecture will be important in a number of transaction usage scenarios with comparable data exchange and communication issues. While there are many tools available for detecting counterfeit goods, most of them only take a picture of the barcode or logo. The purpose of this study is to provide recommendations for how to create a tool that can take a picture of a product logo, process it using artificial intelligence, and identify text and colors to tell if a product is real or fake. This application will show how portable and easy to use it is. It will be especially helpful for people who are not tech-savvy.

#### **V. REFERENCES**

- [1] G. Vidhya Lakshmi, Subbarao Gogulamudi, Bodapati Nagaeswari, Shaik Reehana, "Blockchain Based Inventory Management by QR Code Using Open CV", International Conference on Computer Communication and Informatics (ICCCI -2021) Coimbatore, INDIA, Jan. 27 – 29, 2021.
- [2] Abhinav Sanghi, Aayush, Ashutosh Katakwar, Anshul Arora, Aditya Kaushik, "Detecting Fake Drugs using Blockchain", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-10 Issue-1, May 2021.
- [3] Miguel A. Prada-Delgado, Gero Dittmann, Ilie Circiumaru, Jens Jelitto "A blockchain-based crypto-anchor platform for interoperable product authentication", IEEE International Symposium on Circuits and Systems (ISCAS),2021.
- [4] 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 Access,2020.
- [5] Veneta Aleksieva, Hristo Valchanov and Anton Huliyan, "Implementation of Smart-Contract, Based on Hyperledger Fabric Blockchain", International Symposium on Electrical Apparatus Technologies (SIELA) - Bourgas, Bulgaria,2020.
- [6] Ajay Kumar Shrestha, Julita Vassileva "Bitcoin Blockchain Transactions Visualization" University of Saskatchewan Saskatoon, Canada, 2020.
- [7] Vinayak Singla, Indra Kumar Malav, Jaspreet Kaur and Sumit Kalra, "Develop Leave Application using Blockchain Smart Contract", 11th international conference on Communication Systems and Networks,2019.
- [8] Jesus Maximo Montes, Cecilia E. Ramirez, Manuel Coronado Gutierrez, Victor M. Larios, "Smart Contracts for supply chain applicable to Smart Cities daily operations"5th IEEE International Smart Cities Conference (ISC2 2019), 2019.
- [9] Sanjay K. S, Dr. Ajit Danti "Detection of fake opinions on online products using Decision Tree and Information Gain" Third International Conference on Computing Methodologies and Communication (ICCMC 2019),2019.