

# Fake Product Detection Using Image Processing in Blockchain

Yash Bhalerao<sup>1</sup>, Tejas Sonawane<sup>2</sup>, Sawra Zirpe<sup>3</sup>, Sakshi Trimukhe<sup>4</sup>,

Prof. Shweta Baviskar,

Department of Computer Engineering,

Genba Sopanrao Moze College of Engineering, Balewadi, Pune, India

**Abstract:** There In recent times, the expansion of counterfeit products has become worldwide. There are many counterfeit goods in the latest supply chain. According to the record, counterfeit product affairs have increased in the last few years. It is essential to have a system for customers or clients to check the all details of the product so that client can decide that the product is counterfeit or not. In India actually, there is no such system to identify counterfeit products. So, the solution includes a simple QR code-based identification that can help the end-user or customers to scan and detect the genuineness of the product by using a smartphone. To design and developed a system for implementing system to detect fake products using blockchain technology, in this work system carried out three different modules like Manufacturer, Retailer and Consumers as well. Each transaction has stored into the blockchain which eliminate all network data attacks in P2P environment for product systems

**Index Terms** – Fake Product Detection, Image Processing, Java, Blockchain.

## I. INTRODUCTION

Blockchain technology or the distributed, secure ledger technology has gained much attention in recent years. This paper presents a detailed survey of blockchain technology literature and its applications. The sources of blockchain literature examined for this survey include research papers, books and book chapters, journal papers, specific cryptocurrency sites and wikis, conference papers, company 'Point of View's (PoVs), whitepapers published by various organizations implementing and experimenting in Blockchain. Blockchain being a much hyped and experimented technology a lot of literature is found in content hosted on proprietary forums such as company websites, web articles, etc. This survey is extensive and covers the various aspects of blockchain including consensus algorithms and their variations as well as currently implemented and possible future applications.

This survey will not cover the details of technical aspects of blockchain, however, references that coversheet aspects may be found in bibliography.

This survey is extensive and covers the various aspects of blockchain including consensus algorithms and their variations as well as currently implemented and possible future applications.

The Manufacturer generates the QR code using the user's order-entered transfer information, the user then uses a web application to read the QR code. Dynamic QR-code and unique ID generation for each product document in the

proposed system. The smart contract system also allows the updates in entire blockchain

## II. . LITERATURE SURVEY

1. Amofa, Sandro, et al. "A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data." 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom).IEEE, 2018  
Amofa, Sandro, et al. [1]. A block chain supported architectural framework for the secure control of personal data in health information exchange by combining user-generated acceptable use policies with smart contracts. We outline the features of our system, its user-centered focus, and also show experimental results, along with directions to enhance our work. The framework suggests minimal risk to the data by architecture mechanism for controlling the data after sharing.
2. Zheng, Xiaochen, et al. "Blockchain-based Personal Health Data Sharing System Using Cloud Storage." 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom).IEEE, 2018  
Zheng, Xiaochen, et al. [2] Propose conceptual design for sharing personal continuous dynamic health data using blockchain technology through cloud storage. The main purpose of the proposed system is to enable

users to securely communication, also share data in order to benefit from their personal dataset in accordance with the data protection. It also provides researchers and business data consumers an effective way to collect high quality personal health data for research and business purposes.

3. **Paharia, Bhumika, and Kriti Bhushan. "Fog Computing as a Defensive Approach against Distributed Denial of Service (DDoS): A Proposed Architecture." 2018. 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT).IEEE, 2018**

Paharia, Bhumika, and Kriti Bhushan. [3] Fog computing is increasingly being used as a defensive approach to DDoS attacks, especially in day-to-day security threats. Here the architecture proposes to stop malicious traffic generated by users by using the advantages of computing to cloud the cloud. Cloud has many existing security infrastructures;

4. **Saad Khan\*†, Simon Parkinson† and Yongrui Qin, "Fog computing security: are view of current applications and security solutions", 2017.**

Saad Khan Et.al [4] distributed and parallel computing recent approach in cloud environment model with the help of computing assets at the advantage of the network. This wide range of programs running functionality intensifies many security pitfalls regarding records, virtualization, segmentation, communities, malware and tracking.

5. **Gupta A, Patel J, Gupta M, Gupta H, "Issues and Effectiveness of Blockchain Technology on Digital Voting", International Journal of Engineering and Manufacturing Science, Vol. 7, No**

Gupta A, Patel J, et al [5] a block chain is a technology that enables digital coins or assets to be transferred from one person to another. The blockchain concept can be understood with the concept of linked lists in the data structure, as its next key address is stored in the previous key and they are interconnected. It was first conceptualized in first that, in the following year, implemented the digital currency as the main component of Bitcoin, which serves as the public account of all transactions. It is varying in size and grew up to 50 GB to 100 GB.

6. **Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, White Paper**

Miners, a collaborative consumer network, verify and check transactions and set up specialized computation equipment called "hashes." They vote with their CPU strength, demonstrating their

approval of legitimate blocks by working to expand them and by declining to operate on invalid blocks [6]. These record strings (hashes) that keep track of any Bitcoin transaction and are repeated on any device in the Bitcoin network

7. **Nirmala Singh and Sachchidanand Singh, "Blockchain: Future of financial and cyber security," in IEEE, Noida, 2016.**

Blockchain is a decentralized LEDGER used for safe trading of digital currencies, deals and Transactions [7] and peer-to-peer network management. All nodes adopt the same internode Contact protocol, and verify new objects. If the data is validated in every block no block will Change it. To modify individual block data, all corresponding block data will be modified, Resulting in network cooperation and denial of the transaction by all nodes.

8. **Henrique Rocha, Marcus Denker and Stephane Ducasse Santiago Bragagnolo, "Smart Inspect: solidity smart contract inspector," in IEEE, Italy, p. 2018.**

The power used to "farm" the cryptocurrency is a key aspect since its costs are rising. According to the Bitcoin statistics site Digiconomist, citizens worldwide use more than 30 terawatts-hours of electricity are mining the crypto-currency. This is greater than, at least, the human energy use 159 countries like Hungary, Oman, Ireland, and Lebanon [8].

9. **GWYN D'MELLO. (2018, Dec.) <https://www.indiatimes.com/technology/news>. [Online].**

**<https://www.indiatimes.com/technology/news/bitcoin-miners-are-using-more-electricity-than-irelandother-159-countries-no-kidding-335114.html>**  
Bitcoin mining is a Creation of new Bitcoin process by verifying Bitcoin Network transactions. That transaction is stored in a shared ledger, and all of the machines involved in the Bitcoin network check and manage the ledger. This "net" of transactions is known as the ledger, and. transaction is basically a timestamp for the database that may involve data [9].

10. **Narayanan A., Bonneau J., Felten E., Miller A. & Goldfeder S. (2018) Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton: Princeton University Press**

Narayanan et al. describe a block string as a data structure composed of a related array of hash pointers.

Every entity in the list is a block containing some previous block data and hash. This renders it a tamper-evident file, implying the data can only be applied to the list and the prior data cannot be changed without detection.

### III. METHODOLOGY

This Java project focuses on combating counterfeit products by integrating QR code processing with blockchain technology. The system generates and assigns unique QR codes to each product, containing essential information about its origin and manufacturing. Upon scanning, the QR code is processed using Java, triggering a verification process on the blockchain. The decentralized nature of blockchain ensures the integrity of the product's information, helping users differentiate between genuine and fake items. By utilizing Java for QR code processing and blockchain integration, this project offers a robust and efficient solution to address the challenges posed by counterfeit products, providing a secure and transparent method for product authentication.

- **Manufacturer:** The manufacturer logs into the manufacturer account generates a QR Code for the Product and adds the required details of the product the manufacturer adds a block to customs blockchain.
- **Retailer:** Retailer reads the product's QR code. Manufacturer-entered product data is made available to the retailer. In doing so, he transfers legal ownership of the product to the buyer.
- **Consumers:** Consumers may verify the product's purity by scanning a QR code, which displays a complete record of all purchases made by the product's owner. When a customer checks the product's Genuity, the status will be shown at that moment. If the goods are fraudulent, the buyer will realize that the QR code was likely forged.

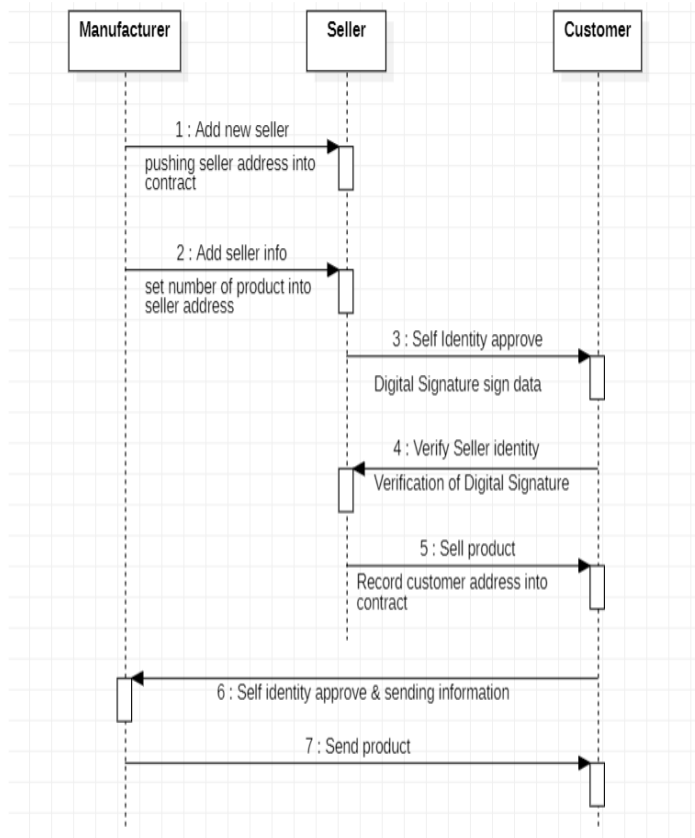


Fig. 1: Sequence Diagram

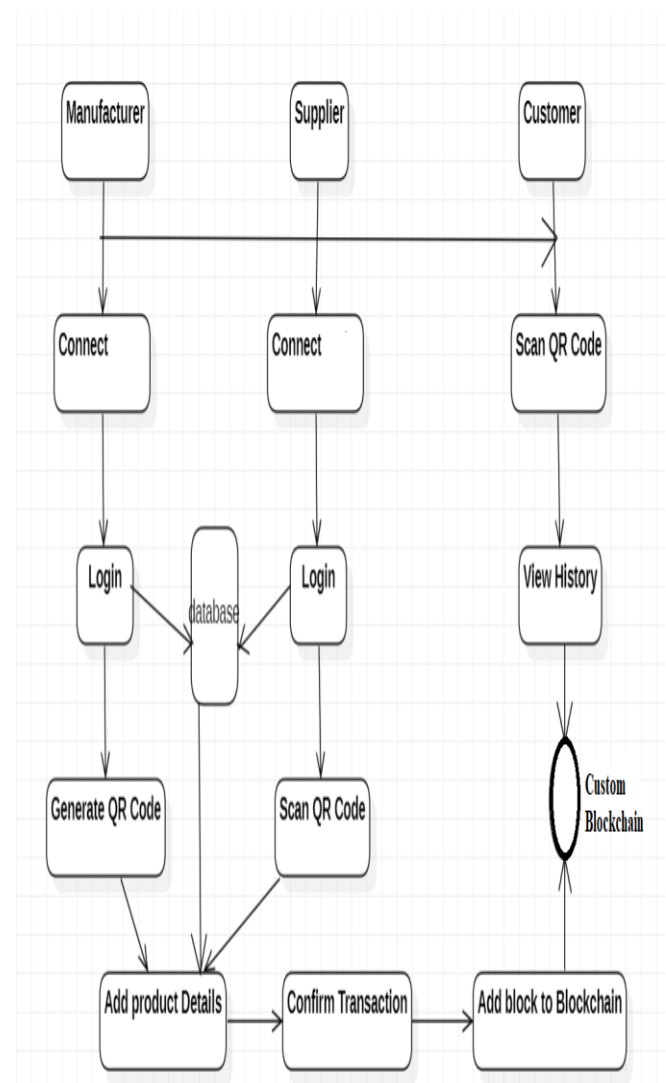


Fig. 2: Activity Diagram

This system highlights the implementation of e-transaction system using blockchain for such a proposal from a practical point view in both development/deployment and usage contexts. Concluding this work is a potential roadmap for blockchain technology to be able to support complex applications. Several techniques for implementing a blockchain-based supply chain management system have been presented by several groups of academics. One of them demonstrated a mechanism for identifying fake goods by searching for them in the Blockchain network, using a web application. A mechanism for identifying phony products using QR code and blockchain. All of the company's data, including the manufacturer's account address, is saved on the blockchain network, and the contract address is sent to the manufacturer. After a product is added to the blockchain, a QR code is generated and used to verify its authenticity. After registering, dealers will have access to the manufacturer's wholesale pricing. The QR code will allow you to monitor the product's ownership change.

- **Data Flow Diagram**

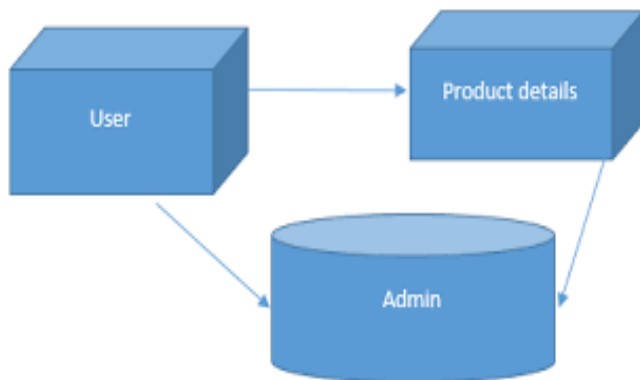


Fig. 3: Zero Level DFD

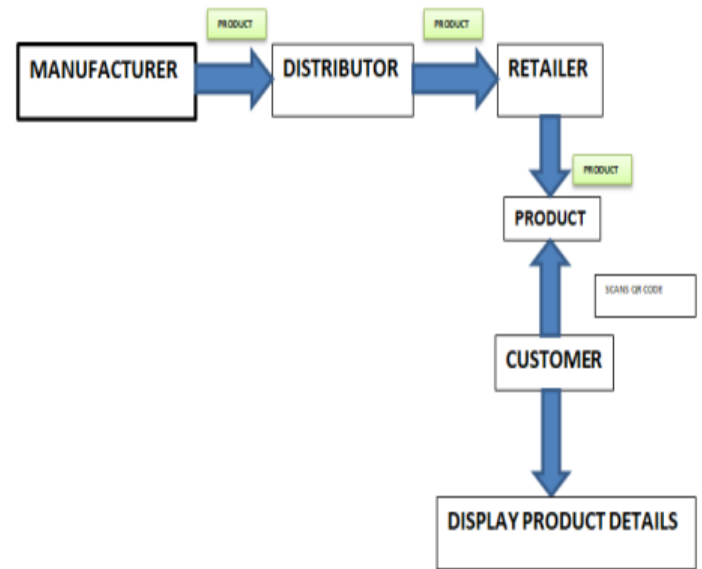


Fig. 4: Multi Level DFD

This Data Flow Diagram (DFD) illustrates the flow of information in a system designed to detect fake products by integrating QR code processing with blockchain technology. The diagram showcases the sequential steps involved in the process, starting with the generation of unique QR codes for products. These QR codes are then scanned by consumers or stakeholders, initiating the QR code processing component. The system subsequently interacts with the blockchain to validate the authenticity of the product, retrieving and verifying information such as manufacturing details and distribution history. The DFD highlights the efficient flow of data and the integral role of QR code processing and blockchain in creating a robust solution for fake product detection.

#### IV. SYSTEM DESIGN

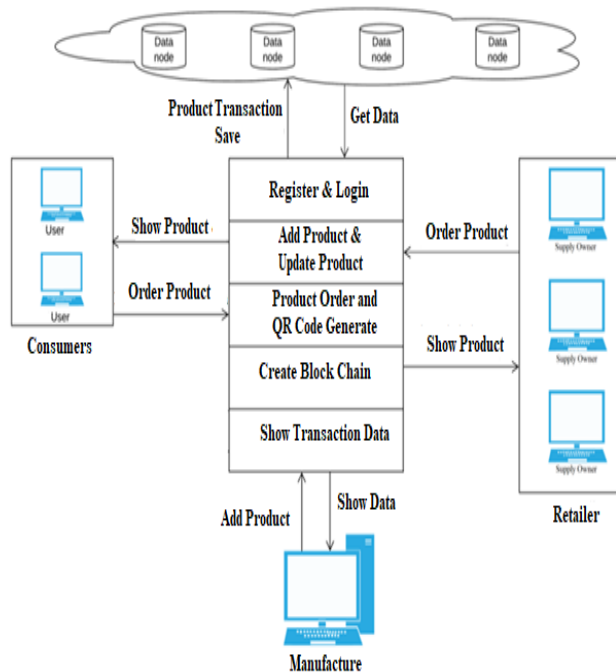


Fig. 5: System Architecture

#### V. CONCLUSION

This report presents survey on Blockchain as the decentralized system, hence it assures confidentiality and privacy of the data on the network. Manufacturer and Customers trust will build through this system it will helps in improving providence and reducing dishonesty. In proposed system, a Custom algorithm used in detection of counterfeit products system is proposed. Creating a system that could quickly and accurately spot counterfeit product was the aim of this endeavor

#### VI. REFERENCES

1. Amoral, Sandro, et al. "A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data." IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom).IEEE, 2018.
2. Zheng, Xiaochen, et al. "Blockchain-based Personal Health Data Sharing System Using Cloud Storage." 2018. IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom).IEEE, 2018.
3. Paharia, Bhumika, and Kriti Bhushan. "Fog Computing

as a Defensive Approach against Distributed Denial of Service (DDoS): A Proposed Architecture." 2018. 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT).IEEE, 2018.

4. Saad Khan\*†, Simon Parkinson† and Yongrui Qin," Fog computing security: are view of current applications and security solutions", 2017.
5. Gupta A, Patel J, Gupta M, Gupta H, "Issues and Effectiveness of Blockchain Technology on Digital Voting", International Journal of Engineering and Manufacturing Science, Vol. 7, No.
6. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, White Paper.
7. Nirmala Singh and Sachchidanand Singh, "Blockchain: Future of financial and cyber security," in IEEE, Noida, 2016.
8. Henrique Rocha, Marcus Denker and Stephane Ducasse Santiago Bragagnolo, "Smart Inspect: solidity smart contract inspector," in IEEE, Italy, p. 2018.
9. GWYN D'MELLO. (2018, Dec.) <https://www.indiatimes.com/technology/news.> [Online]. <https://www.indiatimes.com/technology/news/bitcoin-miners-are-using-more-electricity-than-irelandother-159-countries-no-kidding-335114.html>
10. Narayanan A., Bonneau J., Felten E., Miller A. & Goldfeder S. (2018) Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton: Princeton University Press