International Journal of Scientific Research and Engineering Development-– Volume 6 Issue 4, July- Aug 2023

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Fake Product Identification System

Avishkar Hongekar*, Anand Jaju**, Prajwal Bhargade***, Neel Acharya****, Prof. Atul Pawar*****

*(Dept. of Computer Engineering, Pimpri Chinchwad College of Engineering, and Pune
Email: avishkar.hongekar19@pccoepune.org)

** (Dept. of Computer Engineering, Pimpri Chinchwad College of Engineering, and Pune
Email: anand.jaju19@pccoepune.org

***(Dept. of Computer Engineering, Pimpri Chinchwad College of Engineering, and Pune
Email: prajwal.bhargade19@pccoepune.org

**** (Dept. of Computer Engineering, Pimpri Chinchwad College of Engineering, and Pune
Email: neel.acharya19@pccoepune.org)

*****(Dept. of Computer Engineering, Pimpri Chinchwad College of Engineering, and Pune
Email: atul.pawar@pccoepune.org)

----------**********----------

Abstract:

The worldwide improvement of a product or invention typically comes with risk considerations like forging and duplication. Forging might have an impact on both the client's well-being and the company's reputation. These days, spotting phony goods is the toughest challenge. A system that allows the end user to verify all information about the goods they are purchasing is essential so that the buyer can determine if the product is authentic or not. False goods have a detrimental impact on the organization and the well-being of the customer. As a result, manufacturers of goods are having a terrible time. Such fake and counterfeit items are something that India and other nations are battling against.

Blockchains may be used to identify real goods and prevent the sale of counterfeit goods. Blockchain technology is a decentralised, distributed ledger that stores transactional data in the form of blocks across a network of database nodes. Blockchain technology is secure because no block can be altered or compromised since data recorded once in the chain is immutable. Customers or users do not need to depend on other parties to vouch for the reliability and safety of the product.

In our project, a customised form of Blockchain technology is used to produce QR (Quick Response) codes. In this invention, trade records are stored in blocks. These squares' data storage is difficult to access or modify. Using a short code scanner, which connects a product's QR code to Blockchain, you may spot a fake product. Because of this, the system may be utilised for storing product information and specially generated unique codes as database blocks. The Blockchain database records are compared to the information contained in QR codes. If they match, the goods is legitimate and authentic, and we may present all the information associated to it; if not, the product is phoney or fraudulent, and the customer will be informed..

Keywords **—Blockchain, Bogus, Counterfeit, blocks, QR code, genuine.**

----------**********----------

I. INTRODUCTION

Risk elements like forgery and duplicates, which can impair the company's reputation, income, and customer health, are always present in the global growth of a technology or product. There are various indicators in the chain of supply that can tell if an item is real or fake. Due to fake or fraudulent goods, manufacturers are faced with serious problems and significant losses. The validity of a product may be confirmed using blockchain technology. The main idea behind our initiative is to establish whether the consumer has acquired authentic or counterfeit items. In contrast to blockchain, we still use traditional supply chains. Traditional supply chains offer a centralised structure in which the data is controlled by the company that provides the service or good to the market. Since thiscompany owns the data, it is vulnerable to change at any time. To profit from the cheaper price of the imitated products, counterfeit goods are produced. As was already said, traditional supply chains employ a centralised network structure, but Blockchain utilises a decentralised database and includes the data value for the items in every transaction[9].

This is achieved by creating a record whose legality can be verified by everyone in the community since blockchain is a network of peers. As a consequence, producers may use this technique to give buyers genuine goods. Client confidence will be maintained as a result, and the brand value of the product will increase. Each block in a blockchain is made up of data, a hash, and the hash of the block before it. Hash is the distinctive code, whereas data is the pertinent information. Since the individual altering the data must control the bulk of the network, it is challenging to alter the data of any block. The resultant hash will be altered if we try to change any block's contents.

A sale or purchase document, the legitimate owner of the commodities, anyone with access to the data, and the capability to edit the data are the system's four primary components. A hash for a good develops as its data is modified on the network, making it possible to track its recent transactions and ownership. Blocks are created as products flow from the producer to the distributor, then from the distributor to the client. When the product is created from the hash address, the QR code is appended to it. Details about the product and whether it is authentic or counterfeit are provided to the consumer when they scan the QR code. The properties of a single record in the system known as the Blockchain are shown in Figure 1[10].

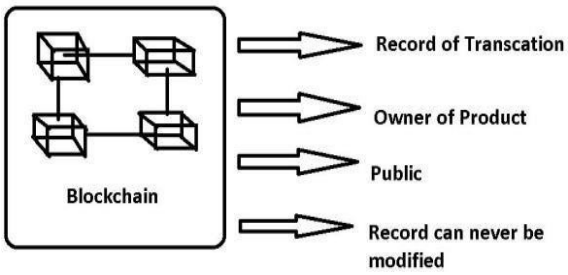

Fig. 1Block in blockchain

An easy way to comply with the conference paper formatting reThis design, which was modified in Word by Microsoft in 2007, may be used by authors to create electronic versions of their papers and published as a "word 97-2003 Format" for the PC. All traditional paper components were specified based on three criteria: (1) ease of access when editing individual research articles; (2) automatic acceptance of digital requirements that facilitate the development of online products simultaneously or later; and (3) uniformity of style all through conference proceedings. There are built-in margins, paragraph lengths, line spacing, and font styles; examples of the type kinds are provided throughout this text and are stated in italic form, inside brackets, following the illustration.

requirements is to use this document as a template and simply type your text into it.

II. MOTIVATION

In recent years, the global distribution of imitation products has increased. There are many fake products in the current supply chain. According to the poll, the prevalence of fake goods has grown recently. In order for customers or users to identify whether a product is genuine or not, it is critical that there be a procedure in place which allows them to confirm all the product's specs. India presently lacks a framework for identifying bogus goods. A simple QR code-based identification is thus required as part of the solution, which can help the consumer or end-user scan the code and confirm the product's legitimacy using a smartphone[3].

Product anti-counterfeiting is essential to Supply Chain management. Businesses that want to succeed in the e-commerce market should provide customers with product information and a place to ask questions about the products. The consumer must have confidence in the overall system architecture and be aware of how the good is given to the customer at the cycle's conclusion. Customers must have access to all of this via a website. Small and medium-sized businesses may be destroyed, while big corporations will likely be financially safe. Because consumers have little faith in the system, traditional methods of combating faking have not succeeded and may yet fail. Paying modest transaction fees and having faith in the system may completely eradicate imitations of goods. Man-in-the-middle attacks are a risk for both consumers and corporations. Contraband continued to occur despite the adoption using RFID along with other mobile technology. It will be necessary to develop encoded QR code techniques to thwart different assaults and product fraud. This can only be accessed by permitted users, who will be subject to the restrictions of the supply chain network. Successful Blockchain administration of systems will come from reliable operation in any company[10].

III. OBJECTIVE

- The project's goal is to develop an anti-counterfeit system.
- The surge in imitation products gave rise to the idea for this project, which aims to create an anti-counterfeit system
- To protect product information using a QR code. You might provide security to your clients by making data accessible to them.
- Manufacturers may use the system in order to record information about the items that will be sold and purchased on a public blockchain.

Iv. LITERATURE REVIEW

This report [1] provides a survey on the detection of counterfeit products. Customers frequently look for counterfeit products for a number of causes, such as a reduced price or as a replacement for the authentic, with the online market swiftly becoming as the primary location for obtaining counterfeit products. An exponential increase in fake goods is being seen both online and on the illicit market. Therefore, it is crucial to address the problem of recognising fake goods and provide the necessary technology to improve detection precision. This represents one of the study topics that is currently being looked at. the paper discusses a variety of methods for spotting fake goods, including holographic barcodes that use computer-generated holograms, watermarking algorithms, RFID methods, and QR code-based product authentication. Technology-based data analytics, such as immediate analysis, predictive analytics, security analytics, and trust analytics, are used to examine and compare these various approaches [1].

A framework for managing the quality of the supply chain based on blockchain has been developed in this study by [2] authors. It explains how the typical cloud storage method is centralised, which increases the risk of just one source of failure leading to a system failure. The technology integrates attribute-based encryption, the

blockchain of Ethereum, and the IPFS decentralised system of storage. The decentralised solution, which is built on the protocol known as Ethereum, provides a keyword search feature on the encoded text, which fixes the issue with standard data storage where cloud servers give false positives. In this study, a blockchain-based system was suggested. This framework, which is based on the concept of blockchain, will give a theoretical basis for knowledgeable chain of custody quality monitoring. It also acts as an initial basis for the creation of theories on the management of information resources in decentralised, virtual companies [2].

In this article, they use blockchain technology to develop a method for identifying bogus products based on QR codes. In the system's implementation, they employed the Android Studio tool and Firebase Cloud. The hashing process uses the SHA-256 algorithm. A 256-bit value is produced using the patented cryptographic hash algorithm SHA-256. The suggested system is made up of three primary components: an Android application for the consumer or user, an Android application for the manufacturer or business, and a database. The manufacturer creates a distinct QR code for each item and enters the product information into the database. All of the product-related data, including manufacturer information, the product id, the date of manufacturing, the price, etc., is saved in blocks. A product order has been saved on the internet once. The item involved in the transaction may be kept, and an encrypted code for that item is produced. For every item in the suggested system, a QR code is generated. Customers can use a custom programme that has a QR code scanner or the QR code reader app on their smartphone to access the QR barcode on the product or packaging. We can determine if the things are real or fake after scanning. Finally, we can monitor the product along the supply chain thanks to the Blockchain system, which maintains these product attributes together with a history of transactions. The block name, hash value, and all other product information are stored in the firebase database cloud database [3].

The use of smart identifiers for safeguarding brands and preventing counterfeiting in the beverage sector is the foundation of this study. Based on smart labels and cloud-enabled technologies, this paper suggests an intellectual property enforcement and to combat counterfeiting approach for the wine industry. Smart tags' primary tenet is the use of quick response codes, functional inks supported by a Cloud system, and a two-way connection between the winery and the end user [4].

The research's authors describe the idea of the digital ledger in terms of information security for the food supply chain and contrast it with the previous supply chain structure. The proposed approach emphasises the negative aspects while promoting blockchain for monitoring, tracking, and inspecting the agricultural supply chain and supporting producers in accurately recording transactions. They didn't actually put the recommended method into practise; they only offered a theoretical idea [5].

This article aids in the tracking of medications from the company to the consumer or patient is made easier by this article. The entire concept is mostly implemented using the Hyperledger fabric. In this setup, the manufacturer must submit the details of a medicine to a website, where they are subsequently submitted for government clearance. Pharmacists may utilise blockchain technology to order drugs once the government has approved them. Additionally, a request is made to the network's blockchain if a patient needs medicine or other pharmaceuticals. A doctor or medical authority will next decide whether to accept or reject the request. Because the whole approach is based on a distributed ledger called blockchain, we can stop medicine fraud and keep an eye on the flow of prescribed drugs from the manufacturer to the patient. In order to accept the product in this sector, this article primarily tells us about Hyperledger, as which may be included in our recommended system [7].

In this study, QR codes were created using Python and blockchain technology. They then used this technology to create a website or app that

allows users to manage their inventories. To create an accurate and open inventory management system, they are using blockchain and quick response code technology. They used Python to create quick response codes that are tailored to certain products. The P2P network then disseminates the information on the sold goods. By obtaining product details from the blockchain database—EVM is a Python-based version of the Ethereum protocol—a manufacturer may quickly calculate the holdings. It supports interoperability with the upcoming Ethereum 2.0 protocol as well as a small amount basic features for present-day Ethereum 1.0 chain. With Py-EVM, they created the Ethereum blockchain to record information about things that have sold out. They are using Python and Ethereum blockchain technology to create QR codes, which can be enhanced by using a blockchain algorithm. They employed such technology for keeping track of inventory at this location, and we used it to detect a fake product. We upgraded the information by creating a website.

Any industry has challenges with effective supply chain management, but the healthcare sector faces greater complexity and risk due to the direct impact that supply chain disruptions may have on the health of patients and their outcomes. One possible method for enhancing the safety, reliability, authenticity, and utility of the wellness supply chain is blockchain technology. In this study [11], with a focus on medical devices supply, hospital supplies and equipment, the World Wide Web (WWW) of Being well Things (IoHT), and the health of the community, we provide an overview of the potential and challenges associated with the adoption and deployment of blockchain in health care supply chain. A serious and well-known danger to the drugs supply chain is the intrusion of the mixed category of faulty and falsified (SF) medications, commonly referred to as counterfeit drugs but frequently having a distinct legal definition. These various types of tainted and fraudulent medications can appear as an outcome of importing inferior products without receiving local approval, using subpar manufacturing techniques or storing them improperly, stealing and diverting drugs, and penetrating grey markets (industry conducted outside of the law) with subpar or fake goods. By developing use cases, models for simulation, and blockchain prototypes, a number of organisations are now researching the potential of blockchain for medicinal products supply chain management. The basic thinking underpinning this development is being led by the Consortium for Supply Chain Studies[11].

V. METHODOLOGY

Stage 1: Stage 1: Product Registration Process: The maker will initially be the product's first owner. As a result, the vendor will add the items to the database and create a bar code each order the distributor places.

Stage 2: Dispatch Item to Distributor: The producer will ship the goods to the distributor in the next phase. When a distributor receives a product, they scan the QR code to ensure that it is valid. If it is, they may then update information like the product's price and quantity that is available. If the backend data and QR code data do not match, indicating that the product is false, the distributor will be properly notified, allowing for the identification and removal of the bogus goods from the chain of distribution.

Stage 3: conclusion the authentication process: At the conclusion of the chain, the end user will take the product and scan the QR code. If the scanned QR code data matches the original product data, the consumer will be able to obtain all information about the product from the manufacturer, including the product's Id, production date, and expiration date, among other details. After receiving information, the consumer may review it and decide whether or not to purchase the item.

Stage 4: Our customised blockchain will be running at the internal and the records of transactions will be saved in block form on different nodes once the distributor and the client have verified the product information and paid for their separate orders. If a node is somehow compromised, the info from the compromised node will still be retrieved using the other unhacked nodes depending on the recovery method.

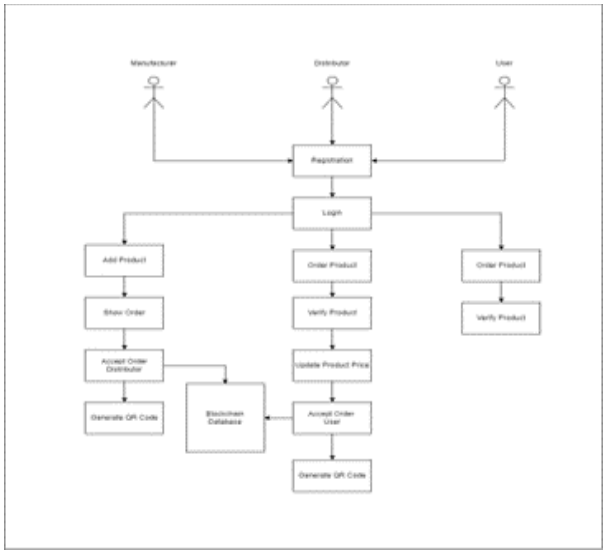

Fig. 2: Workflow of System

VI. ALGORITHM USED

A. SHA-256 (Secure Hashing Algorithm) :

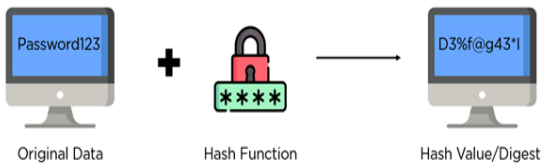

Fig. 3: Hash Function

How SHA works:

1. Initialization: Initialize the hash values (known as "initial hash state") with the first 32 bits of the fractional parts of the square roots of the first eight prime numbers (2, 3, 5, 7, 11, 13, 17, 19).
2. Padding: Append padding bits and length to the input message in order to make its length a multiple of 512 bits (the block size of SHA-256). The padding consists of a single "1" bit, followed by enough "0" bits to reach the desired length, and finally, the 64-bit representation of the original message length.
3. Message Digest Calculation: Divide the padded message into 512-bit blocks. Process each block sequentially.
4. Prepare the message schedule: Create a message schedule array (W[0..63]) of 32-bit words. For each block, divide it into 16 32-bit words, and extend the remaining 48 words using a specific formula based on the previously generated words.
5. Initialize working variables: Set up eight working variables (a, b, c, d, e, f, g, h) with the initial hash values.
6. Compression: Perform 64 rounds of compression using a combination of logical and arithmetic operations. Each round updates the working variables based on the message schedule and the values from the previous round.
7. Update hash values: After all rounds are completed for a block, update the hash values (initial hash state) by adding the working variables to them.
8. Continue: If there are more blocks, go back to step 4 and repeat the process.
9. Final hash value: Once all blocks are processed, the resulting hash value is obtained by concatenating the final hash values (a, b, c, d, e, f, g, h) in the specified order.

B. P2P Verification:

Between peers (P2P) authentication is a mechanism used in blockchain networks where each network node verifies the activities that are being recorded to the blockchain. This is important

for the security and reliability of the blockchain. There are multiple phases in the P2P verification algorithm. A transaction is first broadcast to all of the network's nodes. The transaction is then verified by each node to see if it complies with the blockchain protocol's standards for validity. The transaction is included in a block of entries if it is determined to be legitimate. Once a record of transactions has been established, the network's nodes compete to find the solution to a challenging mathematical conundrum so they may add the entire block to the blockchain. In order for other nodes to confirm that the outcome is accurate, the initial node to solve the challenge announces the answer to the network. The block of data is added to the technology and the actions it contains areand the actions that it contains are regarded as confirmed if the majority of the network's nodes concur that the result is accurate. This procedure assures that the blockchain is safe and impregnable by requiring a majority of the network's computer power to approve any effort to alter a block requiringrequiring more than half of the network's computer power to approve any effort to alter a block, this procedure assures that the blockchain is safe and impregnable.

C. Validity and majority:

Validity and majority algorithms are key features of blockchain technology that ensure the security and trustworthiness of the network. The validity algorithm is a set of rules that determine whether a transaction or block is valid according to the blockchain protocol. This algorithm ensures that transactions and blocks meet certain requirements, such as having a valid digital signature, not exceeding a certain size, and not being a duplicate of a previous transaction. The majority algorithm, also known as the consensus algorithm, is used to determine which blocks are added to the blockchain. In a decentralized blockchain network, there is no central authority that can decide which blocks are valid and which are not. Instead, the majority algorithm relies on the agreement of the majority of nodes in the network to determine which blocks are added to the blockchain.

Blockchain technology uses a variety of majority algorithms, including as Proof of Work, or PoW, Proof of Stakes (PoS), and delegation of proof of Stake (DPoS). A block can be added to the blockchain by the very first node to successfully solve a challenging mathematical challenge in a PoW system. Nodes are chosen to contribute blocks in a PoS or DPoS system based on their ownership in the overall system or their track record. In summary, the validity algorithm ensures that transactions and blocks meet certain requirements, while the majority algorithm ensures that the network agrees on which blocks are added to the blockchain. Together, these algorithms ensure the security, immutability, and trustworthiness of the blockchain network.

D. Recovery:

In a blockchain network with four nodes, if one node gets hacked and its data is compromised, the recovery algorithm can be used to recover the hacked data with the help of the remaining three unhacked nodes. The recovery algorithm typically involves a process called data reconstruction, where the unhacked nodes collaborate to reconstruct the hacked data. The process works as follows:

1. Identify the compromised node: The first step is to identify which node has been compromised. This can be done through various means, such as monitoring the network for unusual activity or running diagnostic tests on the nodes.
2. Isolate the compromised node: Once the compromised node is identified, it is isolated from the network to prevent further damage or data loss.
3. Recover the data: The remaining three nodes can then collaborate to recover the data from the compromised node. This is done by comparing the data stored on the compromised node with the data stored on the remaining nodes. If any discrepancies are found, the correct data can be determined through a voting mechanism, where the majority of nodes determine the correct data.

4. Rebuild the network: Once the data is recovered, the compromised node can be rebuilt or replaced with a new node to restore the network to its original state.

The recovery algorithm is designed to ensure that even if one node is compromised, the network can still function and recover from the attack. However, it is important to note that the recovery algorithm is not fool proof, and there is always a risk of data loss or compromise in a blockchain network. Therefore, it is crucial to implement strong security measures and protocols to prevent attacks and minimize the risk of data loss.

VI. TOOLS & LANGUAGE USED

A. *Java:*

Widely employed in web development, Java is a high-level, object-focused programming language. Because Java is platform-independent, it may be used to run programmes on any system that supports a Java Virtual Machine (JVM). Java is widely used in web design because it has a wide range of features and tools that make it simple to create online applications that are reliable, scalable, and secure. Java libraries like Java Servlet Apis and Java Server Pages (JSP) allow programmers to construct dynamic and interactive web pages, while Java frameworks like Spring, Struts, and Java Server Faces (JSF) give a framework for developing online applications Java's security features make it an effective platform for developing enterprise-level online applications. It offers built-in security tools including a Security Manager and a Sandbox environment that assist defend against malicious programmes and unauthorised access. All things considered, Java is a robust programming language with a wealth of features and tools that make it ideal for web development. Particularly in enterprise-level situations, its platform autonomy, flexibility, and security capabilities have rendered it a popular option for designing online applications.

B. *Java Server Pages (JSP):*

Java Server Pages (JSP) is a technology used in web development that allows developers to create dynamic, server-side web pages. JSP is based on the Java programming language and is often used in conjunction with Java Servlets to create web applications. JSP pages are essentially HTML pages that include special tags, called JSP tags, that are used to insert dynamic content. JSP tags can be used to access JavaBeans, which are reusable components that can be used to store and manipulate data, and to create conditional statements and loops. JSP pages are compiled into Java Servlets by the web server, which can then be executed on the server-side. This allows JSP pages to generate dynamic content in response to user requests, such as displaying database records or processing user input.

JSP is commonly used in web development because it allows for the separation of presentation logic and business logic. The presentation logic, which defines how the web page looks and behaves, is contained within the JSP page, while the business logic, which defines how the application processes data and interacts with databases, is contained within Java classes. Overall, JSP is a powerful technology for creating dynamic, server-side web pages that can be used to create sophisticated web applications. Its integration with Java and its ability to separate presentation and business logic make it a popular choice for web developers.

C. *Eclipse IDE:*

Eclipse is a popular IDE (Integrated Development Environment) for creating software programmes. It is free to use and works with many other programming languages, including Python, C++, and Java. Eclipse is well-liked among developers since it provides a variety of capabilities. With tools like syntax pointing out, code completion, and refactoring, it offers a strong code editor. It also offers tools for debugging, testing, and profiling code. One of the key features of Eclipse is its extensibility. It has a plugin architecture that allows developers to add

functionality to the IDE and customize it to their specific needs. There are many plugins available for Eclipse, including plugins for version control systems, build tools, and code analysis.

Eclipse also offers support for collaborative development through its integration with various team collaboration tools, such as Git, Subversion, and Team Foundation Server. Overall, Eclipse is a powerful IDE that offers many features and tools for developing software applications. Its extensibility and support for collaboration make it a popular choice among developers.

D. *HeidiSQL:*

HeidiSQL is a free and open-source application that is used for managing and administering MySQL and Microsoft SQL Server databases. It is available for Windows operating systems and provides a range of features that make it a popular choice among database administrators and developers. HeidiSQL provides a user-friendly interface for managing databases. It allows users to easily create, modify, and delete database objects such as tables, views, and indexes. It also provides a range of tools for managing data, including the ability to import and export data, run queries, and perform backups.

In addition, HeidiSQL offers advanced features such as SSH tunneling, which allows users to connect to remote databases securely, and support for multiple simultaneous connections, which makes it easy to manage multiple databases at once. HeidiSQL is also highly customizable, with a range of options for configuring the interface and behavior of the application. It also provides a range of plugins and add-ons that allow users to extend its functionality. Overall, HeidiSQL is a powerful and versatile application for managing and administering MySQL and Microsoft SQL Server databases. Its user-friendly interface, advanced features, and customization options make it a popular choice among database administrators and developers.

E. *Apache tomcat*:

Apache Tomcat is an open-source web server and Servlet container that is used to run Java-based web applications. It is widely used in the development and deployment of Java-based web applications and is a popular choice among developers and organizations. Tomcat provides a range of features that make it a powerful and flexible platform for web application development. It supports the Java Servlet API, which allows developers to write server-side code in Java and run it on the server-side. It also supports JavaServer Pages (JSP), which allows for dynamic content generation. Tomcat is designed to be lightweight and easy to use. It can be easily installed and configured on a variety of platforms, including Windows, Linux, and macOS.

It also provides a user-friendly administration interface for managing web applications and server configurations. One of the key features of Tomcat is its extensibility. It provides a range of plugins and modules that can be used to extend its functionality, such as support for additional programming languages and frameworks. Overall, Apache Tomcat is a powerful and flexible platform for web application development and deployment. Its support for Java-based web applications, lightweight design, and extensibility makes it a popular choice among developers and organizations.

VII. RESULTS

The project's findings demonstrate how the system functions and how it might be applied to finding fake goods. When a QR code is scanned, the system displays information about the product, including its name, description, manufacturer, unique product identifier, date of manufacture, and expiration, among other details. If this information is displayed, we can conclude that the product is genuine. After scanning the QR code, the system will notify you that a fake product has been spotted and won't provide any information that would allow you to conclude that the product has been counterfeited if the product or its QR code has been tampered with

along the supply chain. So, we can say that the product is fake.

Once distributor and customer verify the product details and pay the bill for their respective order, our custom blockchain will run at the backend and the transaction history will be stored in the blocks on multiple nodes. If anyhow any node gets hacked, still based on recovery algorithm the data from the hacked node will be recovered with the help of remaining untampered nodes. In this way blockchain and its features or algorithm can be very useful in our system to identify the counterfeit products.

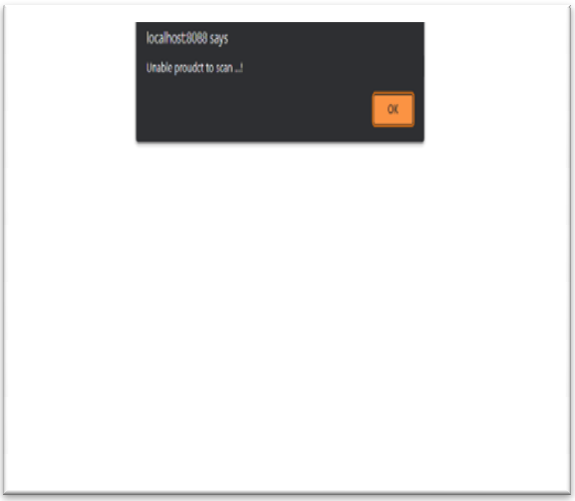

Fig. 4: Alternate/Wrong QR Code Scan Error

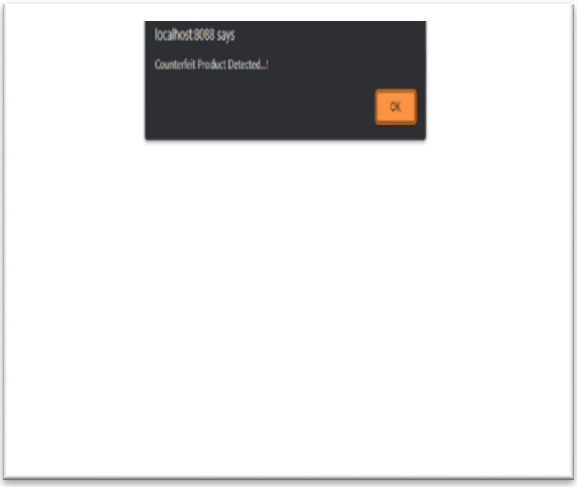

Fig. 5: Scanning Tampered QR Code for Original Product detects product as Counterfeit

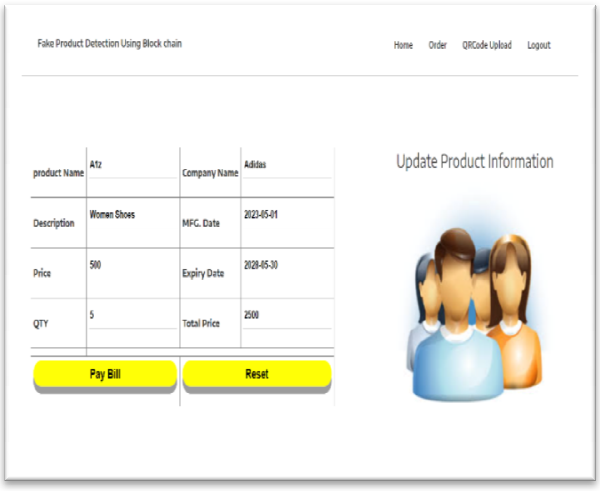

Fig. 6: Successful QR Code Scan gives Product Details

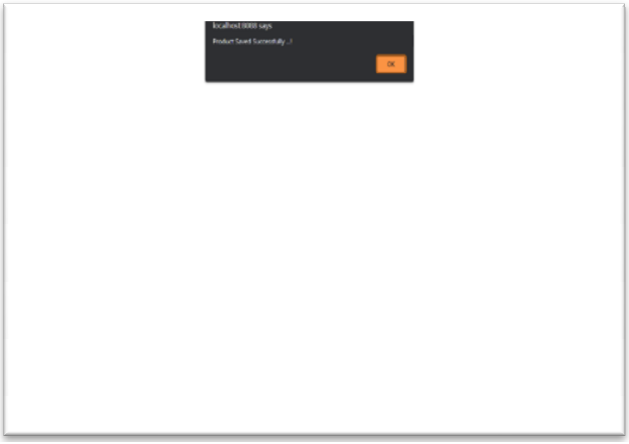

Fig. 7: After Bill payment transaction data saved in Blockchain

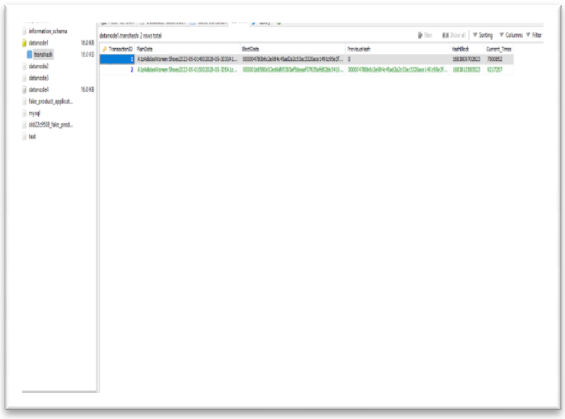

Fig. 8: Transaction Data in Custom Blockchain

ACKNOWLEDGMENT

We want to express our sincere appreciation to Prof. Atul Pawar, who served as our mentor, for his constant advice and comments during the project's progress and the writing of the research paper. Additionally, we appreciate the help and advice provided by the PCCOE Department of Computer Engineering.

REFERENCES

[1] B.Prabhu Shankar, Dr.R.Jayavadivel, "A Survey Of Counterfeit Product Detection", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 8, ISSUE 12, DECEMBER 2019.
[2] Si Chen, Rui Shi, Ren, Jiaqi Yan, Yani Shi, "A Blockchain-based Supply Chain Quality Management Framework", 14th, IEEE International Conference on e-Business Engineering, 2017.
[3] Tejaswini Tambe, Sonali Chitalkar, Manali Khurud, Madhavi Varpe, S. Y. Raut," Fake Product Detection Using Blockchain Technology", International Journal of Advance Research and Innovation ideas in Education(IJARIIE), 2021.
[4] Steven Sandi, Sanja Radonjic, Jovana Drobnjak, Marko Simeunovic, Biljana Stamatovic and Tomo Popovic "Smart Tags for Brand Protection and Anti-counterfeiting in wine Industry" 23rd International Scientific-Professional Conference on Information Technology (IT), 2018.
[5] Daniel Tse, Bowen Zhang, Yuchen Yang, Chenli Cheng, Haoran Mu, "Blockchain Application in Food Supply Information Security", 2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM).
[6] Feng Tian, "A supply chain traceability system for food safety based on HACCP, blockchain &Internet of things", 2017 International Conference on Service Systems and Service Management.
[7] 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 Issue1, May 2021.
[8] 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.
[9] Swaroop Jambhulkar, Harsh Bhoyar, Shantanu Dhore, Arpita Bidkar, Prema Desai, " Blockchain based Fake Product Identification System",International Research Journal of Modernization in Engineering Technology and Science, 2022.
[10] Srikrishna Shastri, Vishal, Sushmitha, Lahari, Ashwal R Shetty, " ISSN (O) 2278-1021, ISSN (P) 2319-5940 Fake Product Detection Using Blockchain Technology", International Journal of Advanced Research in Computer and Communication Engineering, 2022.
[11] K. A. Clauson, E. A. Breeden, C. Davidson, and T. K. Mackey, "Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare:: An exploration of challenges and opportunities in the health supply chain"' BHTY, vol. 1, Mar, 2018.
[12] Feng Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," 2016 13th International Conference on Service Systems and Service Management (ICSSSM), 2016, pp. 1-6, doi: 10.1109/ICSSSM.2016.7538424.
[13] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash,2008
[14] Dhiren Patel, Jay Bothra, Vasudev Patel," Blockchain exhumed", IEEE 2017.
[15] Johansen, Stefan K. "A Comprehensive Literature Review on the Blockchain Technology as a Technological Enabler for Innovation.", Mannheim University, Department of Information Systems, Version: 2.
[16] Blockchain: what is in a block? URL: https://dev.to/damcosset/blockchain-what-is-in-a-block-48jo
[17] "Types of Cryptocurrencies Hashing Algorithms - Bitcoinlion.Com". Bitcoin Lion - Your Gate to Cryptocurrency, 2018, http://www.bitcoinlion.com/cryptocurrency-mining-hash-algorithms/. Accessed 5 Aug 2018.
[18] Janvi Dattani, Harsh Sheth, "Overview of Blockchain Technology", Asian Journal of Convergence in Technology.
[19] Xiaoyan Gong, Sheping Zha, "Research on the Application of Cryptography on the Blockchain", Journal of physics, California.
[20] Tsz Yiu Lam & Brijesh Dongol (2020): A blockchain-enabled e-learning platform, Interactive Learning Environments, DOI: 10.1080/10494820.2020.1716022
[21] https://blokchainnetwork.com/how-does-blockchain-work/
[22] Li, H. Li, H. Hou, K. Li, and Y. Chen, "Proof of vote: A high performance consensus protocol based on vote mechanism & consortium blockchain," in High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/Smart City/DSS), 2017 IEEE 19th International Conference on. IEEE, 2017, pp. 466– 473.