Counterfeit Product Detection System Using Blockchain Technology

Prof. Sunil Yadav[1], Swayamprabha[2], Samruddhi[3], Payal[4], Anil[5]

[1]Asst. Professor of Department of Computer Engineering DYPCOEL, Varale, Pune (SPPU), Maharashtra, India.
[2,3,4,5]BE Student of Department of Computer Engineering DYPCOEL, Varale, Pune (SPPU), Maharashtra, India.

Abstract

To overcome and stop the crucial effects of counterfeiting, a blockchain based system is used in identification of original products and also detects duplicate products to ensure theidentification of original goods. In this project, with massive emerging trends in wireless technology, QR (Quick Response) codes provides a technique to cut down the practice of counterfeiting the products. The fake products are identified using QR of the product or goods is linked to a blockchain to store product details and guaranteed unique code of each product stored as blocks in the database. If the code in product matches, the notification will be sent to the customer indicating the authenticity of the product and else if it does not match the code in database, a notification will besent to customer indicating that product is fake or counterfeited and notification is also sent to manufacturer about the place of purchase if customer accepts the request made by the application.

Keywords: Ethereum Blockchain, Smart Contracts, QR - code, SHA-256,Meta mask wallet, AES etc.

1. Introduction:

The process of identifying counterfeit products by utilizing blockchain generation is known as "fake product detection" in blockchain. Blockchain is an immutable, decentralized virtual ledger which offers transaction security and transparency. Businesses are able to use blockchain technology to ensure that their items are authentic, and customers can trust that the products they purchase are authentic. It operates by creating a digital record of the product's origin and tracking its journey through the supply chain. An irreversible and transparent report of the product's records is created at the blockchain every time the arms are adjusted .This files helps you avoid fraud by verifying product authenticity[1].

The research suggests an innovative approach for identifying counterfeit products that uses blockchain technology to authenticate products while keeping an accurate record of all transactions related to the product. Manufacturers can ensure the authenticity of their products by registering each one on the blockchain and giving it a unique digital identity. This ensures that customers are buying the right item by allowing them to confirm the product's authenticity before making a purchase[2].

By simplifying the verification process, blockchain may ensure that products are authentic and lower the possibility of fakes entering into the supply chain. The potential benefits of this approach, such as increased transparency, supply chain traceability, and consumer protection, will also be covered in the paper. For every cosmetic product, for example, the platform produces a digital record that includes information about the product's origin, creation date, and supply chain. A tamper-proof record of a cosmetic product's journey from farm to table is created when it is scanned at every step of the supply chain and its information is updated on the blockchain. Users can also obtain this information by scanning a QR code present on the cosmetic item's label or package. Businesses can quickly detect any inconsistencies or irregularities in the supply chain that would point to the existence of fake or counterfeit products thanks to the blockchain record, which offers an immutable and transparent account of the cosmetic item's trip. For instance, a product will be deemed to be phony or counterfeit if its record reveals that it was produced in a different location from the one listed on the packaging[3].

Additionally, this work aims to provide a critical evaluation of the proposed device, including its challenges and challenging situations. It will look into how the suggested gadget measures up against current anti-counterfeiting technology and identify potential future features. This paper will conclude with recommendations for additional research on this area and its possible effect on businesses and customers. All things considered, blockchain-based fake product identification has the potential to completely transform how businesses authenticate products and stop fraud, benefiting consumers and businesses[4].

2. Literature Review:

In This paper, the paper focuses on the integration of blockchain generation and QR codes to fight counterfeiting. Developing an anti-counterfeit system dedicated to product authentication is its pertinent goal. The project aims to establish robust systems for confirming product authenticity at some point in the supply chain through using the features of blockchain and QR codes. This new strategy aims at solving the major issue of counterfeiting by offering an accurate method to differentiate real products from fakes. In order to improve consumer acceptance and confidence in the validity of the product, this research aims to develop anti-counterfeit efforts through the proposed integration of blockchain and QR codes[1].

The author of the paper, one appealing solution is a blockchain device designed to combat counterfeit goods while reducing transaction costs. This innovative method ensures transparency across the supply chain and prevents product frauds through the use of Ethereum. Businesses may effectively address the challenge of counterfeit goods in a cost-effective way through the use of blockchain technology, improving safety and protecting their brand. Organizations of all sizes may implement robust anti-counterfeiting measures without incurring significant costs thanks to the blockchain machine's capacity to maintain low transaction fees. In the continuous fight against counterfeit products, implementing the blockchain age is a great step forward that will increase customer acceptance and trust in the authenticity of the product[2].

Finding the causes of counterfeit goods and their effects on society has been one of the survey's main goals. There are a number of methods for detecting counterfeit products that include artificial intelligence, blockchain, QR codes, and machine learning. Diverse scholars have proposed various methods for developing a blockchain-based supply chain management system[3].

A Study on the Detection of Fake Products by Prabhu Shankar and R. Jayavadivel. The amount of counterfeit products on the internet and in the underground market is growing tremendously. Therefore, it is essential to address the challenges in identifying fake products and develop appropriate technologies to improve detection precision. This is one of the current research topics being studied in the modern world. Several methods for detecting fake goods are addressed in this essay[4].

3. Methodologies:

3.1. Blockchain:

The blockchain takes on a series shape in blocks to achieve information immutability. A block consists of the block header and the block frame. The block header contained a lot of information, including the time stamp, issue value (nBits), random wide variety (Nonce), current block version, Merkle Root, and distinguishable block signature price (Parent Block Hash) (refer to Table 1 for details). The transaction is not only a way to change the blockchain facts, but it also serves as a database for the blockchain. All of the transaction statistics in the cutting-edge block are kept inside the block frame.

The Merkle tree prepares transactions inside the block. For instance, when a transaction occurs on the Bitcoin device, the nodes queue the transactions according to the transaction time order, obtain the hash fee for each transaction using a hash operation, and splice unique hash values to compute the new hash value again, continuously from the bottom to the backside. The Merkle Root is then obtained by splicing the hash operation. For a particular period of time, Merkle Root serves as a representation of every transaction fact and could be regarded as the tree's signature. In the event of a transactional change, the Merkle Root obtained by repeating the procedure mentioned earlier should be different from the previous value. It is possible to check if every transaction has been altered with as long as Merkle Root is kept. The node first confirms that the transaction was lawful before receiving the transaction statistics via the device. The verification can only be exceeded if the transaction satisfies specific requirements. The illegal transaction is immediately denied, while the legitimate transaction is broadcast to the nearby node and stored locally. The following block statistics the Parent Block Hash and joins the chain after achieving the required Nonce and passing the verification in order to establish contact with the leading block. A records structure chain is formed from the ordered hyperlinks as the block continues to develop. The information in the chain is locked and constantly verified. To tamper with a transaction, the tamper must possess more than 51 percent of the device's computational capacity in order to compute all blocks following the transaction and standardize the chain after recalculation via other nodes. As a result, all nodes' historical data is stored on a complete blockchain. It is possible to show whether or not each transaction has been altered for as long as the closing block's version variety is kept.

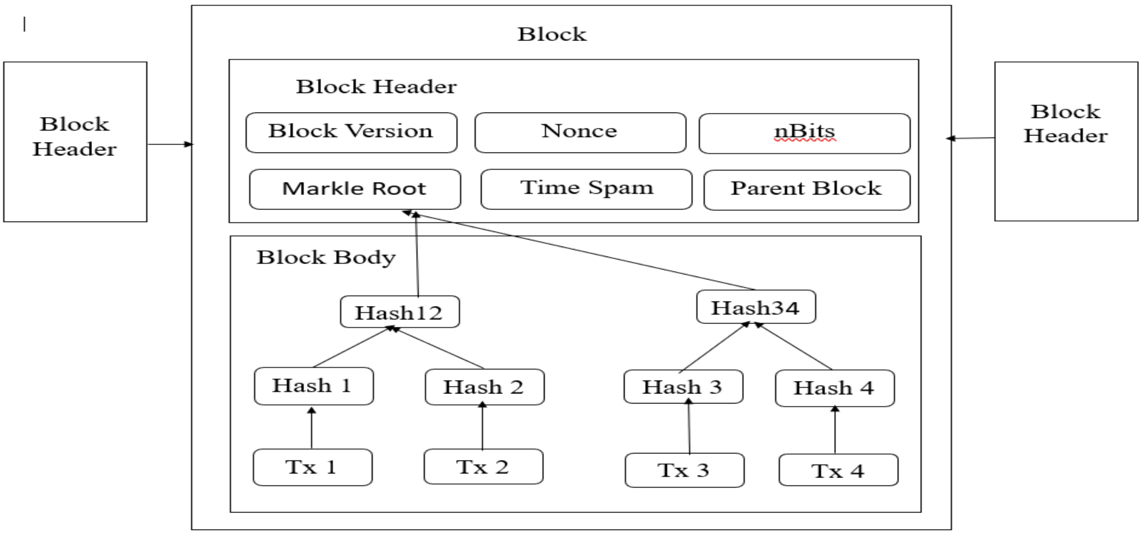

Fig 3.1: Blockchain Structure

3.2. Ethereum:

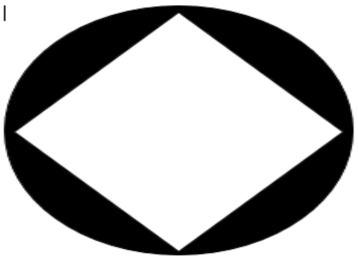

Fig 3.2: Ethereum

(ETH) Ethereum is a non-hierarchical, permissionless network of computers (nodes) that constructs and agrees on a constantly changing set of "blocks," or batches of transactions, known as the blockchain. Every block includes an identifier of the chain that must come before it in order for the block to be considered to be valid. The ETH balances and other storage values of Ethereum money due are changed whenever a node adds a block to its chain. This is because the node performs the transactions in the block in the order that they are indexed. In a Merkle tree, these values and balances—collectively referred to as the "kingdom"—are kept up to date on each node progressively from the blockchain.

The "peers" that each node communicates with are a very limited subset of the network. A node transmits a copy of a transaction to each of its peers whenever it wants to add a new transaction to the blockchain. These peers then send copies to all of their peers, and so on. In this way, it spreads across the community. A list of all these new transactions is kept by certain nodes, called miners, who utilize it to generate new blocks that are then sent throughout the network. Every time a node receives a block, it checks to see if it and all of the transactions within it are authentic. If it finds that they are, it adds the block to its blockchain and completes all of the transactions. A node may also receive numerous blocks vying to be the successor of a specific block because block advent and broadcasting are permissionless. The node records every valid chain that emerges from this and frequently discards the shortest one: The Ethereum protocol states that the canonical chain is the one that is the longest at any given moment.

Ether (ETH) is the cryptocurrency generated by means of the Ethereum protocol as a praise to miners in a evidence-of-paintings gadget for including blocks to the blockchain. It is the most effective foreign money familiar to pay for transaction costs, which also go to miners. The block-addition praise collectively with the transaction fees offer the motivation to miners to preserve the blockchain developing (i.E. To keep processing new transactions).

3.3. Smart Contracts:

Initially, smart contracts were defined as a collection of digitally defined promises and agreements made by settlement participants to implement these obligations. Clever contracts have been rewritten and implemented with the advent of blockchain generation. In order to create software-defined systems and assets that can automatically process data and shop deliverable values, smart contracts—a key component of the settlement layer inside the blockchain infrastructure—may be integrated into any transaction involving tangible or intangible assets. A clever contract consists of a collection of logic and occasion-driven programmatic policies.

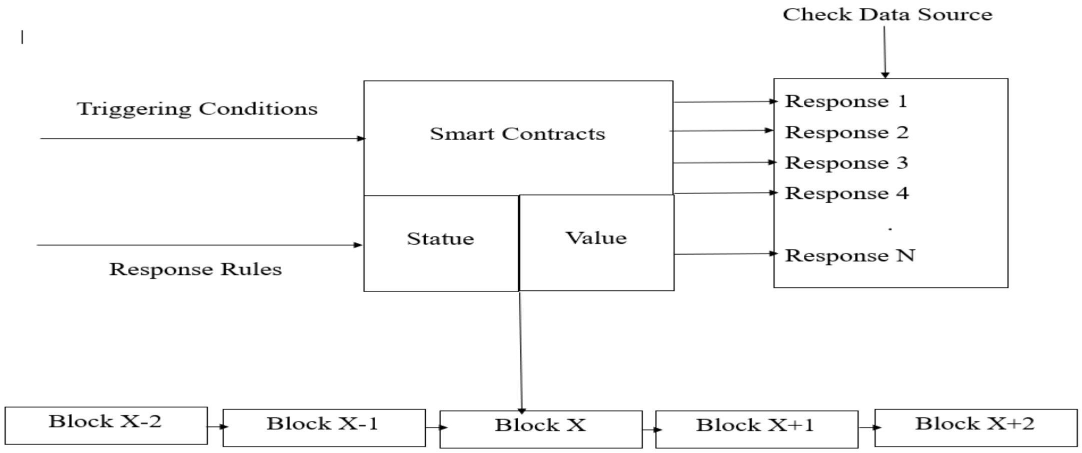

Fig 3.3: Smart Contracts

Smart contracts specify rules for gaining access to statistics as well as buying and selling logic. After being signed by the events involved, certain programmatic policies and logics are typically created for specific scenarios that are linked to the transaction information in the form of software code. The program code is compiled into an opcode that is stored inside the blockchain and assigned a storage address once it has been distributed around the network and verified by the system. In compliance with the settlement specifications, the external utility must name the clever agreement, carry out the transaction, and obtain entry to the facts.

3.4. Solidity:

Solidity is an item-oriented programming language for imposing clever contracts on numerous blockchain structures, maximum substantially, Ethereum. It was advanced by using Christian Reitwiessner, Alex Beregszaszi, and several former Ethereum middle contributors. Programs in Solidity run on Ethereum Virtual Machine. Solidity is a statically typed programming language designed for growing clever contracts that run at the Ethereum Virtual Machine (EVM). Solidity uses ECMAScript-like syntax which makes it acquainted for existing web developers; however in contrast to ECMAScript it has static typing and variadic go back kinds. Solidity is different from other EVM-targeting languages which include Serpent and Mutan in a few vital methods.

3.5. Metamask:

The Ethereum wallet, MetaMask, is a browser plugin that functions similarly to other browser plugins. Customers can shop for Ether and other ERC-20 tokens once it's connected, enabling them to transact with any Ethereum trade. Users can swap tokens on decentralized exchanges (DEXs), stake tokens in gambling apps, and spend their money in games by linking MetaMask to Ethereum-based dapps. Additionally, it gives users access to the growing world of decentralized finance, or DeFi, by providing a way to use DeFi apps like PoolTogether and Compound. Additionally, MetaMask's open platform is crucial in marketing Ethereum-based dApp enhancements for programmers and technologists.

Metamask comes pre-configured with quick connections to Ethereum and many check networks via Infura for developers building a dApp. Because of these integrated links, developers can start creating a new dApp on Ethereum without having to install and maintain a complete network node. In order to support a brand-new decentralized marketplace, bootstrapped entrepreneurs may find this useful whether they are developing a simple, browser-friendly user interface (UI) or a fully functional, mainnet-ready dApp. Furthermore, because MetaMask extensions work well with well-known browsers like Chrome, Firefox, and Safari, the tool makes it easier for developers to construct new applications that are intended to run in conventional browsers.Thus, MetaMask's role in allowing dApp adoption is two-fold: It offers a portal for quit users to get admission to dApps, whilst additionally enabling builders to streamline their direction to getting those packages to market.

4.Algorithms:

4.1.SHA-256 Algorithm:

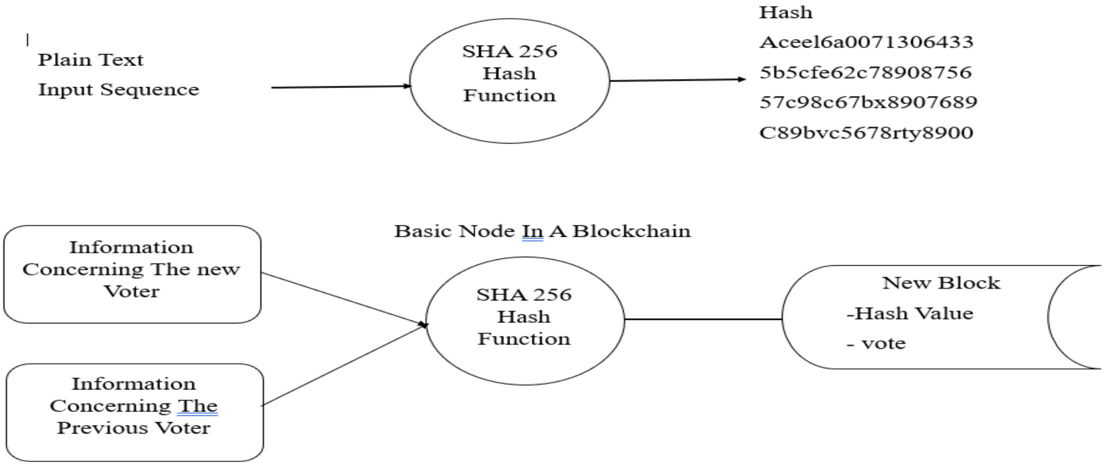

Fig 4.1 : SHA256

Secure Hashing Algorithm (SHA) - 256 is the hash potential and mining calculation of the Bitcoin conference, alluding to the cryptographic hash work that yields a 256 pieces in duration esteem. It directs the creation and the executives of addresses, and is also utilized for trade test. Bitcoin makes use of twofold SHA-256, implying that it applies the hash capacities two instances. The calculation is a variation of the SHA-2 (Secure Hash Algorithm 2), created by means of the National Security Agency (NSA). SHA-256 is also applied in well known encryption conventions.

4.2. Encryption Algorithm:

In order to save you the records transmission method from being attacked, the blockchain makes use of an encryption device to make sure records protection. A common encryption system gen erally includes encryption and decryption keys, encryption and decryption algorithms, ciphertext, plaintext and other elements. A simple encryption and decryption process is proven in Fig

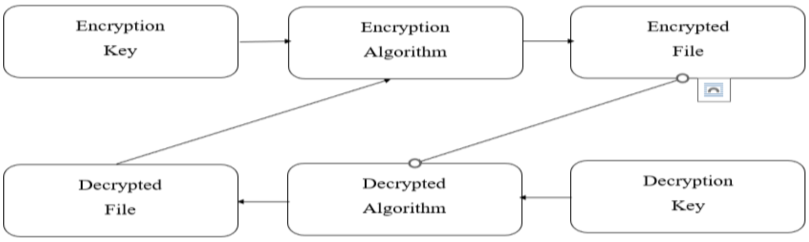

Fig 4.2:Encryption Technique

During the encryption process, the ciphertext is obtained by encrypting the plaintext using the encryption key and algorithm; during the decryption process, the ciphertext is decoded using the decryption key and method to recover the plaintext. The encryption method can be separated into two categories: symmetric cryptography and asymmetric cryptography, depending on whether the keys are the same. Blockchain systems mostly employ the asymmetric encryption algorithm, while symmetric encryption uses identical keys and asymmetric encryption uses unique keys. Public key and non-public key are the two keys used in the asymmetric encryption set of rules. The general public key is generated using a personal key, whereas the non-public secret is typically obtained using a random procedure. Every node in the device has an entirely different key, the private key is stored with the help of the node, and the public key is shared with the entire community.

In order to confirm the legitimacy of the statistics source, other nodes in the transaction wish to use the general public key to decrypt the records if the node uses the private key to sign and encrypt the data. In the same way, the private key wants to be used for decryption if the public secret is used for encryption.The safety of uneven cryptographic algorithms is based on complicated mathematical troubles inclusive of large-scale factorization, discrete logarithms, and elliptic curves to make sure, the representative algorithms encompass RSA, Diffie-Hellman, ElGamal, Elliptic Curve Cryptography (ECC), ShangMi 2, and so on. On the idea of uneven encryption, virtual signature technology is also derived to verify the integrity of records content and verify the facts supply . The virtual signature algorithms utilized in common scenes consist of Digital Signature Algorithm (DSA), Elliptic Curve Digital Signature Algorithm (ECDSA), and so on. The virtual signature algorithms for special scenes consist of Blind Sig nature (BS), Multiple Signature (MS), Group Signature (GS), Ring Signature (RS) and so on.

4.3.Proof of Work (PoW) :

In a blockchain network, it's the real consensus algorithm. A new block is added to the chain and the transaction is validated using the set of rules. Under these regulations, children (a group of people) vie with one another to finish the community transaction. Mining is the method by which they compete against one another. He is compensated as soon as miners successfully produce a valid block. Bitcoin is the most well-known application of Proof of Work (PoW). Creating proof of work could be a random process with little chance of success. Before a legitimate proof of labor is produced, a great deal of trial and error is required. The most important running precept of proof of labor is a mathematical puzzle that can effortlessly prove the answer. Proof of work may be implemented in a blockchain by using the Hashcash evidence of work gadget

5. System Architecture:

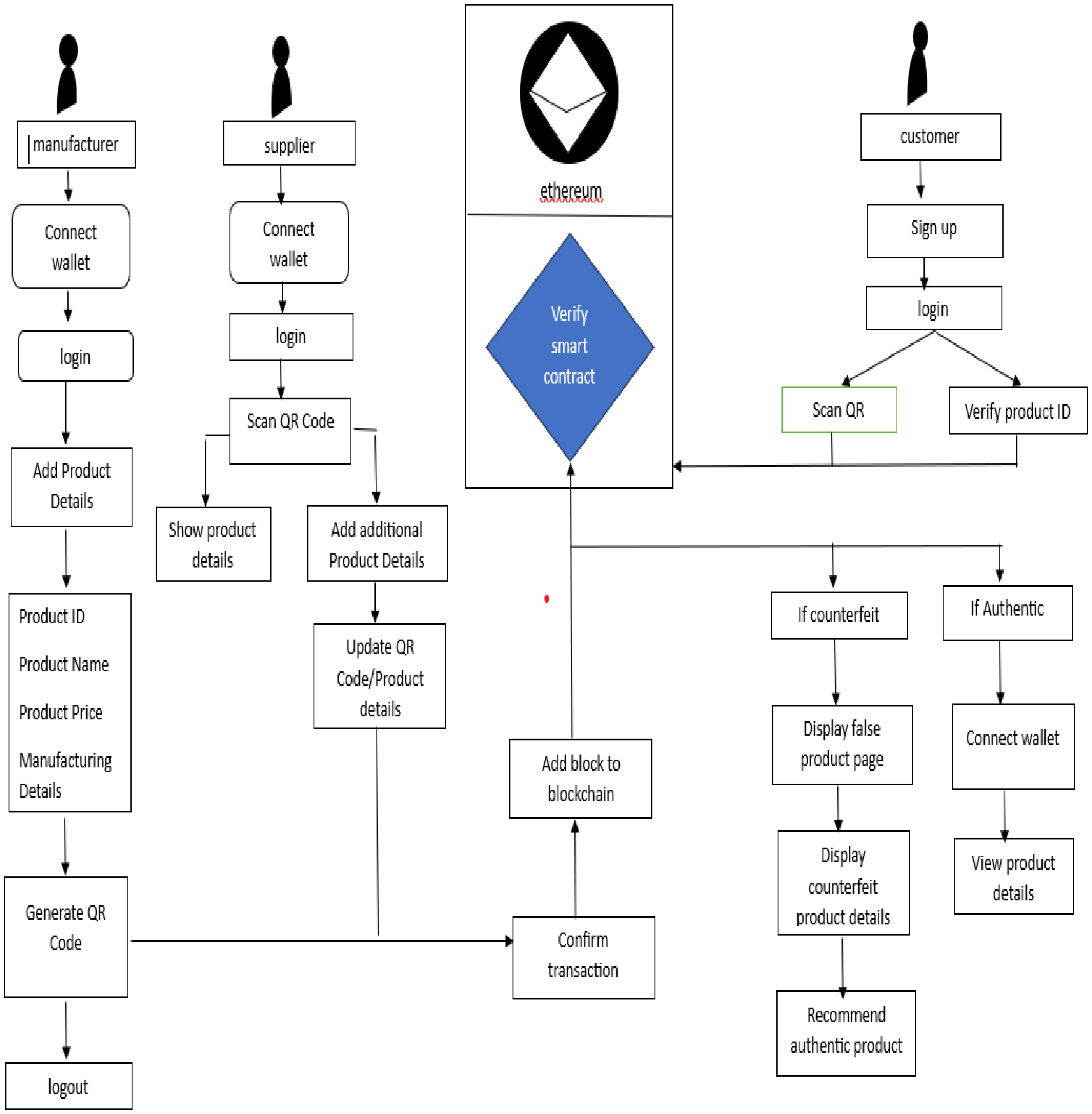

Fig 5.1: System Architecture

6. Challenges And Future Scope:

It's crucial to confirm that the data added to the blockchain is accurate and authentic. The immutability of the blockchain will preserve inaccurate information if fake data is entered. All supply chain participants—manufacturers, distributors, retailers, and many others—should embrace the blockchain technology for it to function properly. It could be challenging to persuade people to abandon conventional systems. Scalability issues plague the blockchain era, particularly with public blockchains. The network's ability to manage a vast number of products and transactions may be limited as the diversity of transactions grows, making it slower and more expensive.

The use of blockchain technology in a variety of industries, including pharmaceuticals, luxury products, electronics, and food merchandise, will increase as more businesses see its potential to combat counterfeiting. Combining blockchain technology with Internet of Things (IoT) devices can provide real-time product monitoring, simplifying the process of displaying a product's whole lifecycle. Without requiring human involvement, smart contracts may automate the validation and verification process, ensuring the validity of items. By forecasting counterfeit characteristics, examining supply chain data, and seeing trends that can point to counterfeiting, artificial intelligence (AI) and device learning might improve blockchain responses.

Conclusion:

In essence, the undertaking concludes with a comprehensive machine designed to fight counterfeit products with the aid of integrating revolutionary technology inclusive of blockchain, Solidity clever contracts, React, and QR code scanning features. Through the usage of these superior equipment, the system establishes an immutable ledger that allows transparent tracking of product origins and moves throughout the deliver chain. This answer enables manufacturers to safely input product information, lets in providers to authenticate and replace facts upon receipt, and gives consumers with easy verification of product authenticity. Leveraging the Ethereum blockchain ensures decentralized records garage and transaction validation, thereby improving security and reliability. With its consumer-friendly interface and robust security features, the task gives a seamless and truthful solution that fosters transparency, integrity, and confidence in deliver chain control practices.

References:

1. M.C. Jayaprasanna, V.A. Soundharya, M. Suhana, S. Sujatha, A block chain based management system for detecting counterfeit product in supply chain, in: 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 2021, pp. 253–257
2. J. Davies, Y. Wang, Physically unclonable functions (PUFs): a new frontier in supply chain product and asset tracking, IEEE Eng. Manag. Rev. 49 (2) (june 2021) 116–125
3. N. Agrawal, H. Kushwaha, S. Shetty, V.B. Lobo, A system to detect fake products using blockchain technology, in: 2022 7th International Conference on Communication and Electronics Systems (ICCES), 2022, pp. 874–878
4. G.V. Lakshmi, S. Gogulamudi, B. Nagaeswari, S. Reehana, BlockChain based inventory management by QR code using open CV, in: 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1–6
5. Yongge Wang, Khaled M. Khan, Matrix Barcode Based Secure Authentication without Trusting Third Party, Published by the IEEE Computer Society, 2019
6. Yan Zhang, Haitao Pu, Jian Lian, Quick response barcode deblurring via L0 regularisation based sparse optimization, IET Image Process. 13 (8) (2019) 1254–1258
7. T.R. Lekhaa, S. Rajeshwari, J.A. Sequeira, S. Akshayaa, Intelligent shopping cart using bolt Esp8266 based on internet of things, in: 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), 2019, pp. 758–761
8. M.A. Habib, M.B. Sardar, S. Jabbar, C.N. Faisal, N. Mahmood, M. Ahmad, Blockchain-based supply chain for the automation of transaction process:8 ITM Web of Conferences 44, 03015 (2022 International Conference on Engineering and Emerging Technologies (ICEET) (IEEE, 2020), pp. 1–7
9. S. Chen, R. Shi, Z. Ren, J. Yan, Y. Shi, J. Zhang, blockchain-based supply chain quality management framework, in 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE) (IEEE

2017), pp. 172–176

10. M. C. Jayaprasanna, V. A. Soundharya, M. Suhana and S. Sujatha, "A Block Chain based Management System for Detecting Counterfeit Product in Supply Chain," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 2021, pp. 253-257
11. Nruthya Ganapathy B*, 2Keerthan Kumar, 3Poojary Shreya Jaya, 4Rajath D Shetty, 5Dr. Shreekumar T 1Student, 2Student, 3Student, 4Student, 5Assosciate Professor, FAKE PRODUCT DETECTION USING BLOCKCHAIN TECHNOLOGY, 2022 IJCRT | Volume 10, Issue 7 July 2022
12. 1Sayyina sharo shaiju, 2Ms.Sumi M 1MCA Scholar, 2Assistant Professor, 1Department of MCA, SUPPLY CHAIN COUNTERFEIT PRODUCT DETECTION SYSTEM USING BLOCKCHAIN TECHNOLOGY, 2024 IJCRT | Volume 12, Issue 3 March 2024
13. Kshitija Karande 1, Yashasvii Sawal 2 , Utkarsha Shelar 3 , Sujata Kullur 4 1Student, 2Student, 3Student 1 Information Technology, Counterfeit Product Detection Using Blockchain, 2024 JETIR May 2024, Volume 11, Issue 5
14. T. Tambe, S. Chitalkar, M. Khurud, M. Varpe, S. Y. Raut, "Fake Product Detection Using Blockchain Technology," in International Journal of Advance Research, Ideas and INNOVATIONS in Technology, vol. 7, pp. 314-319, 2021
15. J. Ma, S. Lin, X. Chen, H. Sun, Y. Chen and H. Wang, "A Blockchain-Based Application System for Product Anti-Counterfeiting." in IEEE Access, vol. 8, pp. 77642-77652, 2020