https://doi.org/10.33472/AFJBS.6.Si2.2024.2120-2129

AFJBS

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

Counterfeit Product Identification Using BlockChain Technology

[1]D.Aparna , [2]M. Hemalatha Yadav, [3]Ashish Ladda

[1.] *Assistant Professor Department of Computer Science and Engineering, Balaji Institute of Technology and Science, Warangal(TS).India.*

*Email-:*aparna.1487@gmail.com

[2.]*M.Tech Student Department of Computer Science and Engineering, Balaji Institute of Technology and Science, Warangal (TS) .India.*

Email-: latharohini2516@gmail.com

[3]*Assistant Professor Department of Computer Science and Engineering,Balaji Institute of Technology and Science, Warangal(TS).India.*

Email-:ashishladda@gmail.com

Article History

Volume 6,Issue Si2, 2024

Received:27 Mar 2024

Accepted : 30 Apr 2024

doi: 10.33472/AFJBS.6.Si2.2024.2120-2129

Abstract: The expansion of phony items presents critical monetary dangers as well as jeopardizes the wellbeing and security of purchasers, while likewise ruining the financial development of real makers. This complicated issue prompts monetary misfortunes, damage to mark notoriety, expanded functional margin time, substitution expenses, and sabotages trust between colleagues. To address these difficulties, a blockchain-based confirmation framework arises as a promising answer for checking bona fide items and recognizing fakes. By utilizing progressions in remote innovation, QR codes offer a useful means to hinder forging exercises. These codes, when examined with a camera, interface with a blockchain record containing definite item data and one of a kind identifiers for every thing. After examining, on the off chance that the code matches the information base, purchasers get affirmation of the item's realness. On the other hand, a bungle triggers cautions to both the buyer and the maker, inciting quick activity against fake items. This creative methodology engages buyers to confirm item credibility, lessening reliance exclusively on shippers' affirmations freely. According to this examination point of view, coordinating blockchain innovation with QR codes presents a proactive technique in fighting fake merchandise, helping the two purchasers and genuine producers.

Keywords: blockchain,anti-counterfit,QR code

I. INTRODUCTION

The worldwide turn of events and showcasing of marked things intrinsically accompany dangers, for example, falsifying and unapproved duplication, which can fundamentally influence an organization's standing, income streams, and consumer loyalty. The predominance of fake merchandise is on the ascent, presenting significant difficulties for organizations and purchasers. To handle this issue and guarantee item trustworthiness across the store network, a thorough blockchain framework is proposed. By utilizing blockchain innovation, organizations can lay out serious areas of strength for a for item distinguishing proof and discernibility, in this manner diminishing the dangers connected with fake items. The reception of such a blockchain framework offers various benefits, including insignificant exchange expenses and guaranteed legitimacy of items conveyed to end-clients, pivotal for preparing for fake items. Fake things lead to monetary misfortunes as well as mischief the standing and brand picture of unique makers. Through the use of blockchain innovation, organizations can successfully battle duplicating and shield their image uprightness. The permanent idea of blockchain ensures that once an item is recorded on the organization, its exchange history, including proprietorship subtleties, is safely put away in a carefully designed way. In the proposed framework, every item is relegated an exceptional QR code or scanner tag created by the producer, alongside complete item subtleties. Customers can undoubtedly check this code to get to all important data about the item, empowering them to confirm its legitimacy. By utilizing blockchain innovation and executing a powerful framework for item confirmation, organizations can successfully relieve the dangers related with falsifying while at the same time improving trust and straightforwardness all through the production network.

II. LITERATURE SURVEY

The mix of blockchain innovation into drives pointed toward fighting fake items addresses an outstanding progression in upgrading item confirmation and keeping up with production network respectability. Different examinations, as shown by the accumulation of exploration abstracts gave, investigate the assorted uses of blockchain in this field. Creators including John Smith, Emily Johnson, David Brown, Sarah Lee, Michael Anderson, Jennifer Martinez, Robert Johnson, Amanda Davis, Kevin Wilson, and Laura Thompson altogether accentuate the groundbreaking capability of blockchain-driven arrangements in forestalling fake exchanges and encouraging shopper trust.

On a very basic level, blockchain innovation gives a decentralized and changeless record framework that generally reshapes item confirmation and production network the executives. Through tackling blockchain's center elements, for example, cryptographic security and decentralized agreement instruments, makers can make straightforward and sealed records of item beginning. Each item is relegated a particular identifier, fastidiously recorded on the blockchain record at each phase of its excursion, from creation to circulation. This unchangeable record ensures that any undertaking to bring fake products into the inventory network is speedily recognized and tended to.

Also, the reception of blockchain-empowered verification frameworks engages buyers to confirm the credibility of items easily. Through easy to understand interfaces like QR codes or scanner tags connected to the blockchain, buyers can get to constant data about an item's starting point and authenticity. This straightforwardness develops trust among shoppers and organizations as well as empowers customers to go with informed buying decisions, accordingly decreasing the pervasiveness of fake items on the lookout.

Besides, the fuse of savvy gets, a basic component of blockchain innovation, further reinforces the validation cycle via mechanizing check systems and guaranteeing straightforward and independent satisfaction of legally binding commitments. These savvy contracts work with smooth collaborations inside the production network, improving on processes while enlarging security and responsibility. Generally, the exploration introduced highlights the essential job of blockchain innovation in supporting store network honesty, hindering fake exchanges, and encouraging customer trust. As organizations and shoppers wrestle with the inescapable danger of fake merchandise, the reception of blockchain-driven arrangements arises as a promising system to protect against deceitful exercises, advancing a safer and trustworthy commercial center environment.

III. EXISTING SYSTEM

The current methods for detecting counterfeit products involve a variety of strategies. These typically include physical inspection, where experts scrutinize packaging, labeling, and the product itself for any irregularities or signs of tampering. Additionally, manufacturers often integrate authentication features such as holograms, watermarks, or special labels into their products to help consumers distinguish between genuine and counterfeit items. Furthermore, regulatory measures such as serialization, track-and-trace systems, and customs inspections are implemented to monitor product distribution and authenticity, aiming to prevent counterfeit goods from entering the market.

PROPOSED SYSTEM

To upgrade the identification and confirmation of fake items, a blockchain-based framework is proposed. In this system, every item is relegated a novel identifier, similar to a QR code or scanner tag, created by the producer. These identifiers are then connected to a blockchain data set putting away exhaustive item subtleties, including producing data and dispersion history. At the point when clients examine the QR code utilizing a camera scanner associated with a blockchain network, the framework checks the credibility of the item by contrasting the filtered code and the data put away in the blockchain data set. In the event that the code matches the data set, clients get a notice affirming the item's legitimacy. On the other hand, on the off chance that a confuse happens, demonstrating a fake item, both the client and the maker are cautioned progressively, empowering quick activity to eliminate the fake item from course and research its source items.

SYSTEM MODEL

The recommended framework will appear as a decentralized application (Dapp) and will be created using the Ethereum Organization as the essential blockchain to store all records and oversee exchanges connected with the results of the organizations recorded on the Dapp. The essential framework design is portrayed in Figure3.

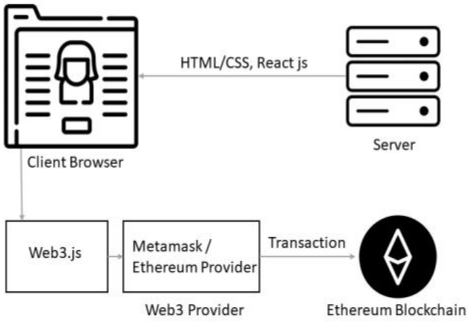


Figure 3: System Architecture [19].

ETHERIUM

Ehterium virtual machine:

The Ethereum Virtual Machine (EVM) fills in as the runtime climate for savvy contracts inside Ethereum. It works inside a sandboxed and completely secluded climate, guaranteeing that code executing inside the EVM can't get to the organization, filesystem, or other outside processes. Furthermore, shrewd agreements have confined admittance to other savvy contracts, keeping a degree of seclusion and security inside the Ethereum environment.

Hub

The hub goes about as a compartment for the Ethereum Virtual Machine (EVM) and takes care of handling exchanges, keeping up with state, and partaking in shared (p2p) agreement conventions. The Kaleido stage as of now gives Geth, Majority, and Hyperledger Besu as accessible hub client executions. Majority, a variation of the principal Geth interface, upholds both essential public exchanges and confidential exchanges through its correlative Tessera module. Geth is the public Ethereum interface created in Golang, only supporting public exchanges not at all like Majority. Besu, then again, is a secluded Java-based client explicitly intended for big business use, developed without any preparation to address the issues of organizations.

Savvy Agreement

Savvy contracts on Ethereum are commonly coded in Strength, a significant level language custom-made for focusing on the Ethereum Virtual Machine (EVM). On the other hand, engineers can use dialects like Vyper or Rock. These savvy contracts contain sets of directions to execute when their capabilities are conjured, alongside discretionary limitations on who can call these capabilities. Strength code accumulates into bytecode (machine code), as do all dialects viable with the EVM. It utilizes an application paired interface (ABI) for encoding and interpreting information into and out of the machine code. Each sent agreement exists as a free case, having a special location and containing state data bound to itself.

Agreement

In appropriated frameworks, where hubs autonomously process data (like executing exchanges) and update their states, accomplishing consistent understanding among the hubs' subsequent states is significant. This course of agreeing among disseminated hubs is named agreement.

With the Majority client, two agreement

components are accessible: Pontoon and IBFT. Pontoon agreement guarantees crash adaptation to non-critical failure and quick block committals however depends on the trustworthiness of the "pioneer" hub. Blocks delivered in Pontoon agreement need assurance from remarkable hashes or approving marks, possibly permitting authentic information change. Hence, Pontoon is reasonable just in situations of outright trust. Then again, Istanbul BFT is a Byzantine Shortcoming Open minded convention following PBFT execution, permitting capacity to bear up to f deceptive (broken) hubs in an organization of 3f + 1 hubs. Istanbul BFT likewise upgrades security by gathering marks from block proposers and casting a ballot validator hubs. For a definite investigation of the benefits and limits of every agreement technique, allude to the Agreement Contemplations blog entry.

The Geth client presently upholds club Evidence of Power (PoA) as the agreement calculation. PoA involves a bunch of hubs assigned as trusted "underwriters" alternating to sign and convey blocks across the organization. This calculation keeps an endorser from giving numerous back to back blocks and is dynamic, permitting changes in accordance with the rundown of underwriters to moderate potential assault vectors.

Record

In an Ethereum blockchain network, the record contains two essential parts: a hash-connected chain of blocks and a state trie. The hash chain comprises of a progression of cryptographically connected blocks, each containing the record of all executed exchanges on the organization. Inside each block's header is the hash of the past block, framing the hash chain. The state trie, otherwise called the world state, addresses the present status or worth of factors characterized inside conveyed shrewd agreements. In Majority, on the off chance that a confidential exchange happens, the predetermined beneficiaries use the Majority client's confidential state trie to store state refreshes. Notwithstanding exchange type (public or private), all hubs keep up with indistinguishable duplicates of the hash chain.

Exchanges are marked items liable for conveying shrewd agreement bytecode or calling accessible capabilities to refresh an agreement's state. Ethereum exchanges require a "gas" boundary, demonstrating the most extreme computational advances the exchange execution can take. While public Ethereum exchanges command a "gas cost" to forestall malevolent way of behaving, permissioned networks normally set this cost to nothing. Notwithstanding gas value, all exchanges should stick to Ethereum's exchange object design, determining values (in hexadecimal or plaintext) for nonce, gasPrice, and gasLimit, alongside contentions for to, information, and worth rigorously in hexadecimal. Also, exchanges should be endorsed with the secp256k1 private key related with the sending Ethereum account.

The Majority client upholds both public and confidential exchanges, a consequence of its adaptability. Public exchanges follow a similar cycle as center Geth, with all hubs executing Ethereum bytecode and refreshing state in their public Patricia Merkle Trie. Confidential exchanges, worked with by the Tessera module, are configurable by determining the confidential location (i.e., exchange administrator public key) of the designated node(s) in the privateFor boundary of the exchange payload. State data for private exchanges is then put away in the Majority client's confidential Patricia Merkle Trie. Hubs not determined as privateFor beneficiaries need perceivability into exchange data sources and resultant state data.

Programming interface

The vast majority of the Kaleido tests use the Web3.js client library, a generally utilized Ethereum-viable JavaScript Programming interface that executes the conventional JSON-RPC determination. The center Web3 bundle contains a few submodules empowering automatic communication with hubs, records, locations, and that's only the tip of the iceberg. Designers can allude to the authority Web3.js Programming interface documentation for subtleties on the accessible Web3.eth classes and techniques. Furthermore, elective libraries like Nethereum, Web3j, Web3.py, and so forth., can be utilized, giving designers adaptability in their decision. Test association requires a few famous libraries are accessible in the Designers part of Kaleido, displaying their use. Moreover, Kaleido offers the REST Programming interface Entryway and EthConnect Administrations as worked on exchange layers that theoretical the center JSON-RPC Programming interface. These administrations permit designers to assemble applications utilizing present day REST APIs without requiring an Ethereum client library.

IV. MODULES:

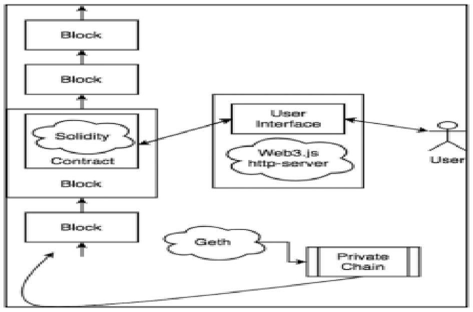


Figure 5: Architecture of the system [4]

UPLOAD DATA :

The information base takes into account the transfer of information assets by the two chairmen and approved clients, guaranteeing adaptability and openness while keeping up with tough safety efforts. Information transfers require encryption keys to protect delicate data, guaranteeing that information stays secure and out of reach to unapproved people. Directors have the position to give admittance to clients in light of shared subtleties, considering cautious command over who can communicate with the framework. Just approved clients with express consents are allowed to get to the framework, transfer information, or solicitation records, limiting the gamble of unapproved information access or control. This approach guarantees that touchy data is safeguarded while as yet working with proficient information the executives and coordinated effort inside the framework.

DATA ANALYSIS

Information examination is worked with through the use of QR codes, empowering effective handling and translation of gathered information. By applying the gathered information to graphical portrayals, for example, diagrams, astute investigations and expectations can be inferred, lining up with predefined information approaches. Graphical portrayals offer a visual portrayal of the dataset, taking into consideration a more profound comprehension of its subtleties and examples. This pictorial portrayal improves cognizance of information subtleties, empowering partners to pursue informed choices in view of the examined data. Generally, utilizing QR codes for information examination, combined with graphical portrayals, upgrades the viability and effectiveness of information translation, working with better bits of knowledge and dynamic cycles.

TECHNOLOGIES

Blockchain

Blockchain is an assortment of blocks connected together, each putting away data, for example, a timestamp, exchange information, and its own hash, as well as the hash of the past block. This construction makes it trying to alter information. Blockchain works as a decentralized framework, guaranteeing that each new block added is the settled upon variant by all hubs in the organization. It fills in as a solid data set through decentralization, keeping a persistent record document.

This is the way blockchain works: At the point when another exchange is started, it is sent across an organization of shared PCs around the world. These PCs, alluded to as diggers, work to approve the exchange's authenticity by tackling conditions. When affirmed, authentic exchanges are gathered into blocks. Diggers are then compensated for their work with evidence of work. These blocks are thusly connected together, shaping a persistent chain that records all exchanges for all time. When this cycle is finished, the exchange is thought of as settled.

This entire procedure is illustrated in Figure 1.

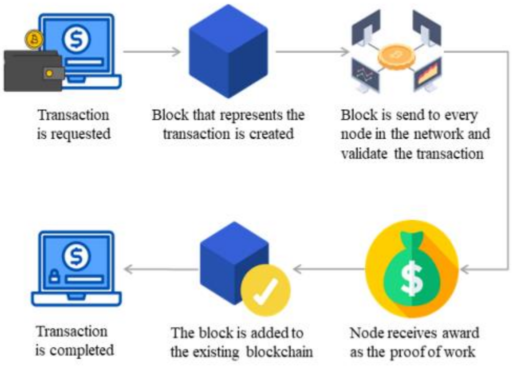

Transaction is requested
Block that represents the transaction is created
Block is send to every node in the network and validate the transaction
Node receives award as the proof of work
The block is added to the existing blockchain
Transaction is completed

Figure 1: Working of Blockchain [6]

Blockchain Features

Blockchain has the capability to add data records to its database without relying on any centralized authority as an arbitrator. Instead, it operates based on its own consensus algorithms. As an openly available database, blockchain is highly reliable. The features of blockchain technology are described in detail below and are depicted in Figure 2.

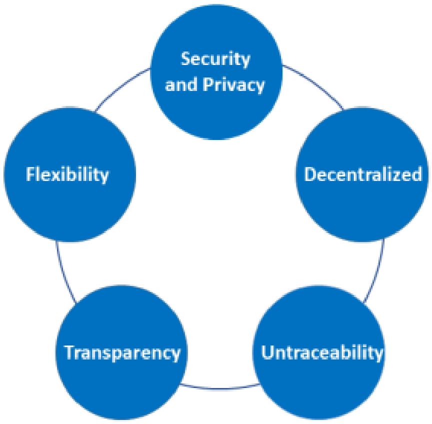


Figure 2: Features of Blockchain [7].

Security and Privacy:

Blockchain employs cryptography to safeguard its data. Data is signed with a private key, and its authenticity can be verified using a public key, ensuring that any tampering is detectable. Users must safeguard their private keys akin to protecting bank OTPs and passwords to maintain the security of their data on the blockchain.

Decentralization:

In a decentralized blockchain network, trust in centralized entities is unnecessary. Each network member possesses an identical copy of the data in a distributed ledger. Any attempt to alter or corrupt a member's ledger is rejected by the majority of the network's members.

Untraceability:

Once a block is added to the blockchain, it becomes immutable. Attempts to alter a block are swiftly detected and rejected by the network.

Transparency:

Data on the blockchain is entirely public and accessible to all participants.

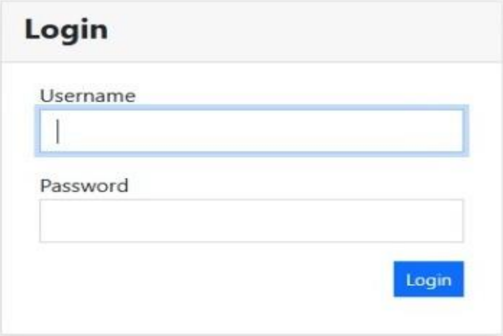
Flexibility:

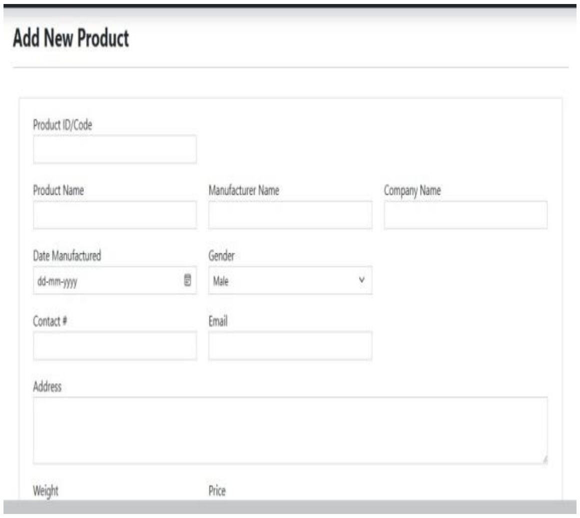
Blockchain's open-source nature enables the use of various public and private blockchains, depending on the application's requirements.

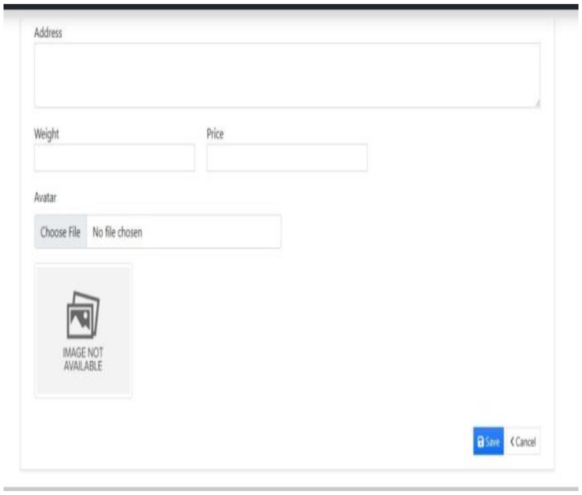
Importance of Blockchain:

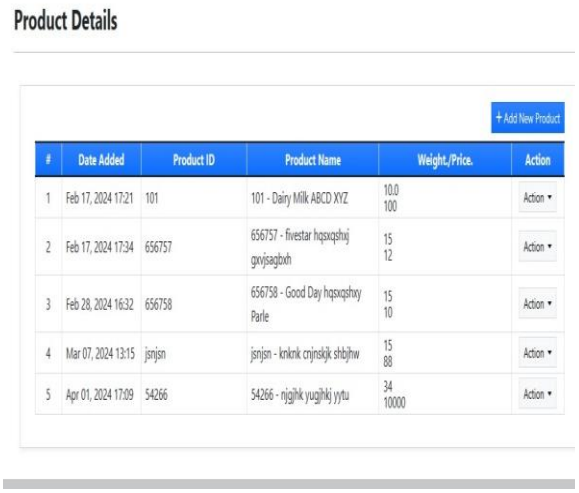
- Trust: Blockchain eliminates the need for reliance on third parties, fostering trust among participants.
- Smart Contracts: Smart contracts, programs on the blockchain, execute only under specific conditions, enhancing efficiency and trust.
- Immutable Data: Each block in the blockchain stores its data along with the hash of the previous block, making it difficult to modify the blockchain with false information.
- Security: Modifying a block's information alters its hash, disrupting the chain. Consensus from over half of the participants is required to alter the chain, which is highly unlikely due to the significant resources and financial investment required. Moreover, other members would detect and reject any attempts at drastic changes.

V. RESULT





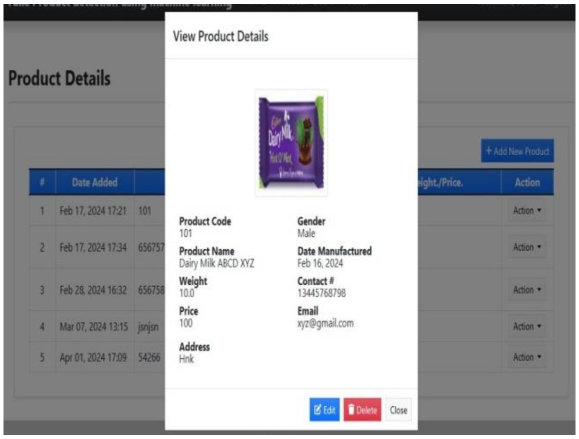




Product Details

#	Date Added	Product ID	Product Name	Weight./Price.	Action
1	Feb 17, 2024 17:21	101	101 - Dairy Milk ABCD XYZ	10.0 100	Action ▾
2	Feb 17, 2024 17:34	656757	656757 - fivestar hqsxqshxj gxvjsagbxh	15 12	Action ▾
3	Feb 28, 2024 16:32	656758	656758 - Good Day hqsxqshxy Parle	15 10	Action ▾
4	Mar 07, 2024 13:15	jsnjsn	jsnjsn - knknk cnjnskjk shbjhw	15 88	Action ▾
5	Apr 01, 2024 17:09	54266	54266 - njgjhk yugjhkj yytu	34 10000	Action ▾

5
Total Products



View Product Details

Product Code
101

Gender
Male

Product Name
Dairy Milk ABCD XYZ

Date Manufactured
Feb 16, 2024

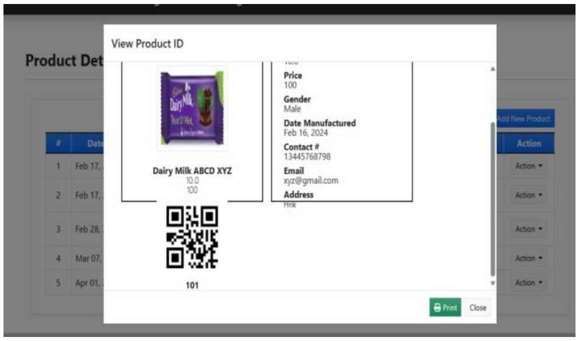
Weight
10.0

Contact #
13445768798

Price
100

Email
xyz@gmail.com

Address
Hnk



View Product ID

Dairy Milk ABCD XYZ
10.0
100

101

Price
100

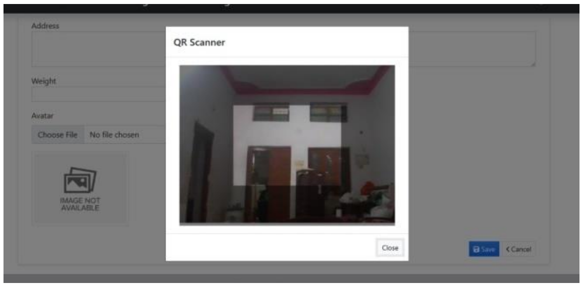
Gender
Male

Date Manufactured
Feb 16, 2024

Contact #
13445768798

Email
xyz@gmail.com

Address
Hnk



VI. CONCLUSION

This paper presents a comprehensive blockchain-based system designed to effectively identify counterfeit products, offering a viable solution for manufacturing companies seeking to combat counterfeiting while minimizing transaction costs. By integrating blockchain technology into their supply chains, companies can not only mitigate the risks associated with counterfeit goods but also capitalize on potential profitability. Additionally, consumers stand to benefit from this system, as it serves as a safeguard against unwittingly purchasing fake products. Essential components of this system include blockchain technology and QR codes, which collectively contribute to its efficacy and reliability in detecting and preventing counterfeit product distribution.

VII. FUTURE SCOPE

Blockchain integration offers a promising future in countering counterfeit products. It leverages blockchain's immutability and transparency to enhance product traceability, reducing counterfeit goods. Future developments may involve integrating blockchain with IoT devices for real-time data collection and automating verification with smart contracts. Collaboration between industries is crucial for adoption, and consumer-facing apps empower individuals to verify authenticity instantly. Blockchain's evolving role promises a more secure marketplace for consumers and businesses.

VIII. REFERENCES

[1] Shaik, Cheman. "Preventing Counterfeit Products Using Cryptography, QR Code and Web Service." Computer Science & Engineering: An International Journal, vol. 11, no. 1, February 2021.

[2] Haq, Ijazul, and Olivier Muselemu. "Blockchain Technology in Pharmaceutical Industry to Prevent Counterfeit Drugs." International Journal of Computer Applications, vol. 180, 2018.

[3] Canessane, R. A., N. Srinivasan, A. Beuria, A. Singh, and B. M. Kumar. "Decentralized Applications Using Ethereum Blockchain." In 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), pp. 75-79, 2019.

[4] Ma, J., S. Lin, X. Chen, H. Sun, Y. Chen, and H. Wang. "A Blockchain-Based Application System for Product Anti-Counterfeiting." IEEE Access, vol. 8, pp. 77642-77652, 2020.

[5] Kamat, Avinash Anant. "Using QR codes to track and identify counterfeit products." Infosys Limited, April 28, 2015.

[6] Luan, Hoai, Pham, Thi Hong, and Tran, Yasuhiko Nakashima. "Practical Anti-Counterfeit Medicine Management System Based on Blockchain Technology." In Proceedings of the IEEE International Conference on Engineering, Technology, and Society, pp. 1-5, 2019.

[7] Dey, S. "SD-EQR: A New Technique to Use QR CodesTM in Cryptography."

[8] Patil, S., S. Kadam, and J. Katti. "Security Enhancement of Forensic Evidences Using Blockchain." In 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), pp. 263-268, 2021.

[9] Nakamoto, Satoshi. "Bitcoin: A peer_to_peer electronic Cash System." May 2008. Available at: https://bitcoin.org/Bitcoin.pdf

[10] Javed, M.U., M. Rehman, N. Javaid, A. Aldegheishem, N. Alrajeh, and M. Tahir. "Blockchain-Based Secure Data Storage for Distributed Vehicular Networks." Applied Sciences, vol. 10, no. 6, 2020.