Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 6- Issue 2, August 2023
Paper : 08

Fake Product Identification Using Blockchain

Aryan Jain[1], Arya Vats[2], Kuhu Bhatnagar[3], Meghna Tyagi [4], Dr Pooja Tripathi[5]
Department of Information and Technology, Inderprastha Engineering College, Ghaziabad

***ABSTRACT* — The global development of products and technologies is always accompanied by threats such as counterfeiting and counterfeiting, which can damage the company's name, the company's revenue and the health of its customers. There are so many products in the circuit. To verify whether a product is genuine or counterfeit. Because counterfeit or counterfeit manufacturers face the biggest problems and huge losses. Blockchain technology can be used to check if a product is counterfeit. Blockchain technology can help solve the problem of product counterfeiting. Blockchain technology is more secure. When a product is stored online, a hash code is created for that product, allowing us to record the sale and current owner of the entire product. This is because chains are created for these commercial transactions. All sales records are stored as blocks on the blockchain. The proposed system uses a supply chain to track the product . The customer can track and get all the information about that product and find out if the item is genuine or counterfeit.**

I. INTRODUCTION

Nowadays, with the growth of technology and applications, the problem of distinguishing between original and duplicate has also caused a lot of damage to consumers, merchants, retailers and also manufacturers. There are many fake products in the current power chain. According to the report, the cases of fake products have increased manifold in recent times. For foreigners or drugs, there must be a system that checks all the information about the product so that the drugs can decide whether the product is genuine or fake. India currently does not have a similar system to describe fake products. The end result is therefore a simple identification with the help of a supply chain, which helps the headstone or guests to notice and identify the fictitiousness of the product with the help of blockchain . Therefore, to combat this, a blockchain based operation against counterfeit products is proposed. This design includes the system design, including a complete description of how the system works and the stone interface. The issue prevents counterfeiting of an accessible, accurate and affordable product using blockchain features. The system is ablockchain-backed feature used to catch counterfeit products throughout the day.The figure below indicates some of the common counterfeited products in 2020.

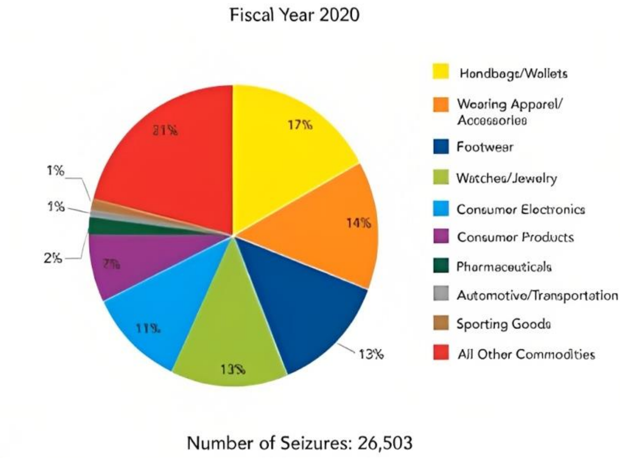


Fig I : Number of counterfeited products as of year 2020.

II. PROBLEM DEFINITION

Risk factors like forging and duplication frequently accompany the global enhancement of a product or innovation. The reputation of the company and the well-being of the customer can both be affected by forging. Nowadays, finding fake items is the biggest test. False goods have a serious negative effect on the organization and the clients' welfare. Blockchain technology aids in addressing the issue of product counterfeiting. In comparison to previous technologies, blockchain technology is more secure. A chain will be constructed for the product's transactions once it is stored on the network, making it possible to keep all transaction records for both the product and its present owner. In the blockchain, it will keep every transaction record as a block. As a result, product makers are facing severe hardship. India and other countries are fighting against such phony and counterfeit goods. The suggested framework tracks the product by employing Blockchain technology. Blocks are used to hold exchange records in this innovation since data stored in these squares cannot easily be accessed or changed.

III. RESEARCH OBJECTIVE

The objective is to create a blockchain-based system to combat the distribution of counterfeit products. This system involves using the supply chain to secure and provide customers with necessary product information. By utilizing this technology, customers can be assured of the authenticity and integrity of the products they purchase. Additionally, the use of blockchain technology ensures transparency and security in all transactions. The ultimate aim is to raise customer awareness of counterfeit goods and prevent their production, which can be achieved by providing transparent and reliable information about the products. Furthermore, the use of the supply chain enables the inclusion of all relevant information about the product and manufacturer. By implementing these measures, the performance of existing anti-counterfeit initiatives can be improved, leading to a reduction in imitations of the main product sold in the market.

IV. Technologies and Algorithm used

1) SHA-256

SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hashing algorithm that yields a 256-bit fixed-size output from an input message of any length. To make the input message a multiple of 512 bits, extra bits are inserted as padding. The algorithm is given a set of starting hash values, also known as initialization vectors, which are a collection of constant values.A set of mathematical operations are performed on each 512-bit block of the padded message during processing. A new hash value is generated by combining the results of each block with the existing hash value and then applying a compression function. The concatenation of the hash values generated for each block is the final hash value. The SHA-256 algorithm converts the input message into a fixed-size output by combining bitwise operations, modular arithmetic, and logical operations. Since it is intended to be a one-way function, it is computationally impossible to identify two distinct inputs that result in the same hash value. Digital signatures, authentication, and verification are just a few of the uses for which SHA-256 is frequently employed. Although it is thought to be a secure and reliable hash function, it is not impervious to some assaults, such as collision attacks, in which an attacker can discover two different inputs that result in the same hash value.

2) METAMASK

MetaMask is a browser extension and mobile application that allows users to control their cryptocurrency wallets and access Ethereum-based decentralized applications (dApps) using MetaMask, a browser extension and mobile app. It serves as a link between a user's web browser and the Ethereum blockchain, offering an intuitive and safe way to engage with decentralized apps. Users are able to send and receive Ethereum and other ERC-20 tokens, examine account balances, manage multiple Ethereum wallets, interact with smart contracts, and establish and manage multiple Ethereum wallets using MetaMask. Additionally, it offers a function for securely managing and saving private keys, which are necessary for accessing and controlling cryptocurrency wallets. Decentralized exchanges (DEXs), gaming platforms, and apps for decentralized finance (DeFi) are just a few of the web3-enabled dApps and platforms that are supported by MetaMask. Users can easily link their web3-enabled dApp accounts across different platforms, offering a convenient and consistent experience. For Chrome, Firefox, and Brave browsers as well as mobile devices running iOS and Android, MetaMask is accessible as a browser plugin. With millions of users all over the globe, it is among the most widely used Ethereum wallet solutions.

3) *SOLIDITY*

The Ethereum network uses the programming language Solidity to create smart contracts. It is a high-level computer language that focuses on contracts and objects and is intended to be used to build smart contracts that execute on the Ethereum Virtual Machine. (EVM).

The norms and regulations specified in the contract code are automatically enforced by smart contracts, which are self-executing contracts stored on the blockchain. They can be used to automate a variety of operations and deals, including the transfer of tokens, the trading of assets, and the execution of sophisticated financial instruments. A variety of features are supported by the statically typed language Solidity, including inheritance, modules, and sophisticated user-defined types. Because of its resemblance to JavaScript and C++, developers with prior expertise in these languages will find it simple to pick up and begin using Solidity programming right away. The Ethereum Virtual Machine executes the bytecode that Solidity code has been converted into. Deployed on the Ethereum blockchain, Solidity-written smart contracts can be accessed and used by other smart contracts, decentralized apps (dApps), and users. For creating smart contracts on the Ethereum network, Solidity has emerged as one of the most used programming languages. Developers use it frequently to create new digital assets and construct decentralized applications.

4) GANACHE

With the help of Ganache, a private blockchain for Ethereum development, programmers may build and test Ethereum-based apps in a local environment. It offers a portable, customisable blockchain that runs locally on a developer's computer, enabling quick prototyping and testing without the need for a real network connection.

There are two varieties of Ganache: Ganache CLI (Command Line Interface) and Ganache GUI (Graphical User Interface). For administering the blockchain and engaging with smart contracts, Ganache CLI is a command-line tool that may be combined with other development tools and scripts. Ganache GUI is a standalone desktop programme. With Ganache, programmers can set up numerous accounts, each of which has a unique Ethereum address and private key that can be used to communicate with the local blockchain. Additionally, it enables a number of testing and debugging functions, such as setting the gas price and limit, manipulating blocks, and inspecting transactions. One of the key benefits of utilizing Ganache is that it lets programmers test their smart contracts and applications in a safe setting without taking on the costs and hazards of putting them into production on the main Ethereum network. This enables developers to rapidly test for potential vulnerabilities and edge cases, revise and improve their code, and guarantee that their applications are operating as intended before releasing them to a live network.

V. IMPLEMENTATION

Exploration paper is the only smart contract-based blockchain system that proposes a fully functional anti-counterfeiting operation. Businesses rent it quickly because of its useful features. Blockchain has set itself up as an excellent tool for identifying and eliminating counterfeit goods in force chain operations. The proposed system allows stoners to fluently identify and collect information about the products they want to review or review by paying a really low turnover. Drug addicts in this operation no longer have to worry about the possibility of stealing's immortality counterfeit. Manufacturers can use this operation to store relevant product details on the blockchain, which can be accessed by anyone on the factory network. With the help of the supply chain, the total number of offers sold by distributors, retailers and manufacturers and the number of products currently remaining in warehouses is transparent to production managers. Consumers can continue to perform manufacturer-side verification with all the functionality provided by the operation. The system uses supply chain to provide identity verification. This helps drug addicts make better choices when enquiring, and also allows them to trust retailers and manufacturers. A smooth and safe experience. Unless the key owner accidentally loses the key, there is no other way to decrypt the key owner's private key.

A fully functioning operation effectively lowers the anti-counterfeiting threshold of deep-rooted goods, gives diligence to limited tax resources, and makes it easier for consumers to prey on counterfeit products that are less susceptible. You can give them confidence and assurance that they will not. Overall, this blockchain technology-based operation will act as a lifesaver for businesses, offering a new system for more secure and stoner-friendly transactions.

VI. SYSTEM ARCHITECTURE

In this proposed system, we do Fake product Identification Using Blockchain Technology. The first step is to bring all the manufacturers to the blockchain network and collect their major product information. Product verification is done by registering the manufacturer on the metamask wallet.. The manufacturer will be the main owner of the item. The manufacturer will ask the seller to add the product to the network while the unique address will be assigned to that product. The regulator will register the product and the manufacturer on the network if the applicant is the actual manufacturer. Once the product is recorded on the network it will create a smart contract with the unique hash code of the product where the product details are stated in the encrypted text form. In the next step the manufacturer will send the product to the distributor and the status is set as shipping; it will not change the ownership of the product until a request from both parties for the purchase and sale of the product is approved. As soon as both parties agree to a joint venture, its ownership in the blockchain network will be transferred in the form of a smart contract automatically after payment has been made. At this stage clients will be provided with the right to the track the product by using the hash code. The consumer tracks the product and removes the encrypted text in the algorithm provided and receives information about the current manufacturer and owner of the product and can decide whether to purchase the item or not.

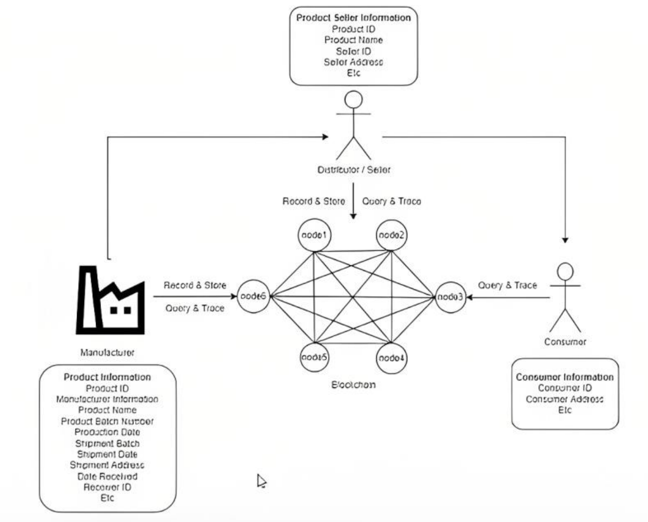


Fig II: Architecture of the proposed system .

VII. PROJECT WORKFLOW

Define the project's scope

Establish the specific industries and product categories to concentrate on as well as the main characteristics of the upcoming blockchain-based system.

Gather data

Gather information on the relevant products, such as any current techniques for product identification, cases of known counterfeiting, and pertinent supply chain data.

Identify the blockchain infrastructure

Consider the project's needs while choosing a blockchain platform, keeping security, scalability, and user-friendliness in mind.

Develop the smart contracts

To store and validate product information on the blockchain, create smart contracts. These agreements should be created to guard against manipulation and guarantee the accuracy of the product data.

Create the front-end user interface

Create a user-friendly user interface so that users can communicate with the blockchain-based system. Users should be able to readily input and access product information using this interface, as well as view any alerts regarding fake goods.

System evaluation

Test the system thoroughly to make sure everything is working as it should and that all security precautions are in place.

Activate the system

Launch the system for usage by relevant parties, such as producers, distributors, retailers, and customers, after it has undergone extensive testing.

System maintenance and monitoring

Keep an eye on the system to make sure it is still operating as intended and that all product data is correct and current. As required, update or modify the system as appropriate.

Assist continuously

Provide users of the system with ongoing assistance, including any necessary training and troubleshooting.

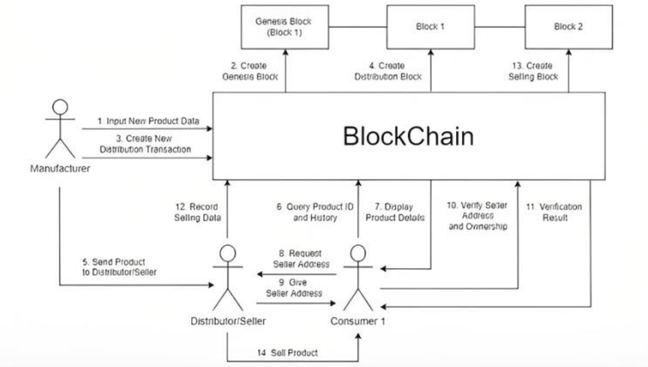

Genesis Block (Block 1)
Block 1
Block 2
2. Create Genesis Block
4. Create Distribution Block
13. Create Selling Block
Manufacturer
1. Input New Product Data
3. Create New Distribution Transaction
BlockChain
12. Record Selling Data
6. Query Product ID and History
7. Display Product Details
10. Verify Seller Address and Ownership
11. Verification Result
5. Send Product to Distributor/Seller
8. Request Seller Address
9. Give Seller Address
Distributor/Seller
Consumer 1
14. Sell Product

Fig III : Flowchart demonstrating project workflow

VIII. BLOCKCHAIN

Blockchain is a distributed ledger technology that makes it possible to transport and store data securely and openly among a network of computers. Although it was primarily intended to support Bitcoin, its uses have now spread to a wide range of industries, including finance, supply chain management, healthcare, and more. A blockchain is essentially a database that keeps blocks, which are collections of records that are added to over time. An immutable and impenetrable record of the data is produced by each block, which consists of a set of transactions and a hash of the block before it in the chain. Blockchain is a very safe and reliable technology because of this design, which makes any modifications to the data detectable and simple to trace. As blockchains are decentralized, there is no single entity in charge of the network. In its place, a network of computers known as nodes collaborates to verify and archive transactions. Before data is added to the blockchain, transactions are verified using a consensus method in which nodes agree on the accuracy of the information. Increased security, transparency, efficiency, and cost reductions are just a few of the potential advantages of blockchain technology. It has the potential to completely transform industries by opening up new business models and eliminating the need for middlemen. Scalability, interoperability, and regulation are a few of the issues that need to be resolved.

IX. LITERATURE REVIEW

“ARMOR: An anti-counterfeit security Mechanism for low cost Radio frequency identification systems, Yildiran Yilmaz, Viet-Hoa Do and Basel Halak, Published in:IEEE Transactions on Emerging Topics in Computing,Volume: 9,Issue: 4, Oct.-Dec. 1 2021”.

A huge amount of money is lost by the global economy each year as a result of fake technology. Through the use of simple, difficult-to-forge tags attached to each product, radio frequency identity (RFID) generation provides a viable answer to this issue. Nonetheless, there are serious safety issues associated with RFID technology. For instance, a cunning adversary might be able to access the sensitive information stored on the device if the communication link between the reader and the tag is exploited. The ability of the RFID era to prevent counterfeiting has been severely undercut by the demonstration that tag cloning assaults are also technically possible. The use of an authentication protocol is one way to solve the issue, but the current options lack mutual authentication [1].

“Comparative Analysis of Bitcoin, Ethereum, and Libra, Wenzheng Li and Mingsheng He , year2020, IEEE 11th International Conference on Software Engineering and Service Science (ICSESS), INSPEC Accession Number:20131326”.

Because of cryptocurrencies' rising repute, the blockchain technology that underpins them, including Bitcoin and others, has gradually risen to prominence in recent years. After the official release of Facebook's cryptocurrency [2] assignment Libra and the release of the Libra white paper, Libra sparked a significant amount of international discussion. The use of Libra, which has increased peoples' belief in open financing, has had a significant impact on the traditional banking system. In this essay, we carefully examine and clarify the blockchain era and highlight Libra's advancements in terms of overall performance and application situation. We look into Ethereum, Bitcoin, and Libra. We conclude by discussing the difficulties that Libra [2] may encounter in the future.

“Block-Supply Chain: a New Anti-Counterfeiting Supply Chain Using NFC and Blockchain, Naif Alzahrani, Nirupama Bulusu, year-2019, MobiSys '18: The 16th Annual International Conference on Mobile Systems, Applications, and Services.”

A centralized authority is necessary for the current supply networks that combat fake goods. Single factor processing, failure, and garage are problems for this structure. A potential solution to these problems is the emerging blockchain era. In this paper, we support the block supply chain, a new decentralized supply chain that uses blockchain to track attempts at counterfeiting and modern near-field communication technology. Block supply chain is a current consensus protocol that substitutes the centralized supply chain in terms of design. It is completely decentralized, in contrast to other protocols, and it demonstrates stability between efficiency and security. Our simulations demonstrate that, in comparison to the most advanced consensus protocol[3], soft mint, the suggested protocol offers great performance with first-rate levels of current safety.

An ADS-B Anti-counterfeiting System Based on TDOA, Hao Shen1, Keren Liu1, Yuxuan Yao, Jun Wang, IEEE International Conference on Signal, Information and Data Processing in 2019”.

Aviation safety could be at danger because the ADS-B signal is not secured in any way and cannot be authenticated by conventional receivers. This study suggests a four-station passive multilateration ADS-B anti-counterfeiting system based on TDOA in light of the insecurity of ADS-B. The Chan Algorithm is used to solve TDOA equations, and a reference station is used to synchronize each station's clock. We developed the technology and put it to the test on multiple flights that passed close to Beijing Capital International Airport. To achieve the goals of ADS-B anti-counterfeiting and pseudo signals localisation, the system may follow the flight path of the aircraft in real-time and compare it to the places claimed by ADS-B messages[4].

X. RESULT

The main aim of this proposed system is to maintain the genuineness of the product by helping the customer track the supply chain history of the product. System give customers the power to track the history of an entire product from manufacturer to customer using blockchain. This product anti-counterfeiting system based on Blockchain is composed of four roles, the Manufacturer role, the Retailer, the Distributor role, and the suppliers role.

Supplier

The supplier can access the information that the manufacturer has entered.It can add his shop destination and push it in the blockchain.Now the product will be at supplier stage.

Manufacturer

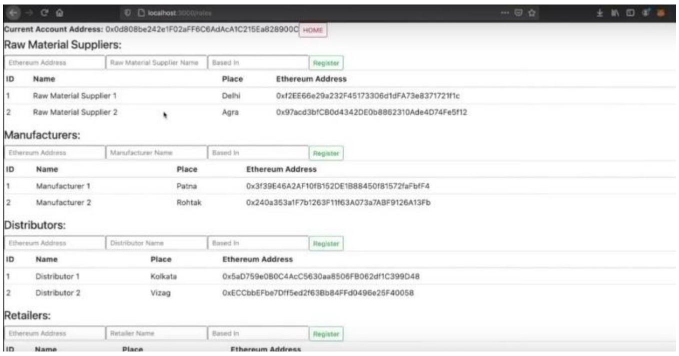
The manufacturer can only register and add the id of the product which adds a block on the ethereum blockchain. Now this user id and wallet address will be mapped together.

Distributor

The distributor can add his user id and wallet address and after mapping of both , it will get added to the blockchain. Now the product is at distributor stage.

Retailer

Similar to the above , the distributor can add his user id and wallet address and after mapping of both , it will get added to the blockchain. Now the product is at retailer stage.



Current Account Address: 0x0d808be242e1F02aFF6C6AdAcA1C215Ea828900C

Raw Material Suppliers:

ID	Name	Place	Ethereum Address
1	Raw Material Supplier 1	Delhi	0xf2EE66e29a232F45173306d1dFA73e8371721f1c
2	Raw Material Supplier 2	Agra	0x97acd3bfCB0d4342DE0b8862310Ade4D74Fe5f12

Manufacturers:

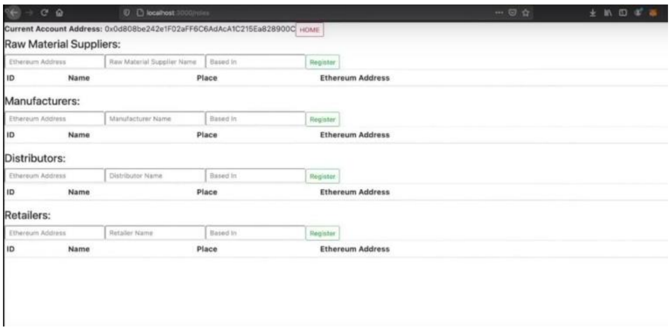
ID	Name	Place	Ethereum Address
1	Manufacturer 1	Patna	0x3f39E46A2AF10fB152DE1B88450f81572faFbfF4
2	Manufacturer 2	Rohtak	0x240a353a1F7b1263F11f63A073a7ABF9126A13Fb

Distributors:

ID	Name	Place	Ethereum Address
1	Distributor 1	Kolkata	0x5aD759e0B0C4AcC5630aa8506FB062df1C399D48
2	Distributor 2	Vizag	0xECCbbEFbe7Dff5ed2f63Bb84FFd0496e25F40058

Retailers:

ID	Name	Place	Ethereum Address



Current Account Address: 0x0d808be242e1F02aFF6C6AdAcA1C215Ea828900C

Raw Material Suppliers:

ID	Name	Place	Ethereum Address

Manufacturers:

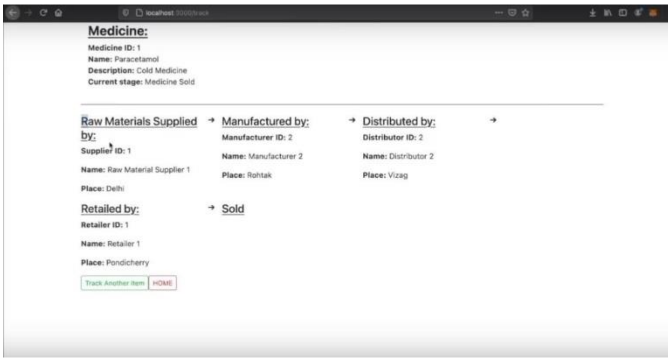
ID	Name	Place	Ethereum Address

Distributors:

ID	Name	Place	Ethereum Address

Retailers:

ID	Name	Place	Ethereum Address



Medicine:

Medicine ID: 1
Name: Paracetamol
Description: Cold Medicine
Current stage: Medicine Sold

Raw Materials Supplied by: → Manufactured by: → Distributed by: →

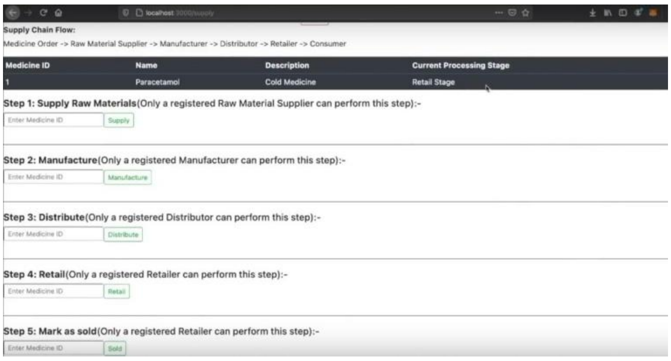
Supplier ID: 1
Name: Raw Material Supplier 1
Place: Delhi

Manufacturer ID: 2
Name: Manufacturer 2
Place: Rohtak

Distributor ID: 2
Name: Distributor 2
Place: Vizag

Retailed by: → Sold

Retailer ID: 1
Name: Retailer 1
Place: Pondicherry



Supply Chain Flow:
Medicine Order -> Raw Material Supplier -> Manufacturer -> Distributor -> Retailer -> Consumer

Medicine ID	Name	Description	Current Processing Stage
1	Paracetamol	Cold Medicine	Retail Stage

Step 1: Supply Raw Materials(Only a registered Raw Material Supplier can perform this step):-
Enter Medicine ID

Step 2: Manufacture(Only a registered Manufacturer can perform this step):-
Enter Medicine ID

Step 3: Distribute(Only a registered Distributor can perform this step):-
Enter Medicine ID

Step 4: Retail(Only a registered Retailer can perform this step):-
Enter Medicine ID

Step 5: Mark as sold(Only a registered Retailer can perform this step):-
Enter Medicine ID

XI. Conclusion

The research paper is the only smart contract based blockchain system that offers fully functional anti-counterfeiting. Businesses start borrowing it very quickly because of its useful features. Blockchain is designed to be an excellent tool to identify and eliminate counterfeit products in power chain operations. The proposed system allows stone sellers to identify and collect information about the product they want to review or approve, paying a very small sales fee. Medicines in this operation no longer have to worry about the delicately forged chances of survival. Product Manufacturers can use this feature to store valid product information on a blockchain that is accessible to all members of the operating network. The total number of offers sold by distributors, retailers and manufacturers and the number of products currently in stock are transparent to the product manager. Consumers can use all the features offered by the feature to perform a manufacturer-directed continuity test. The system enables identity verification by tracking using the supply chain. This helps addicts make better choices in their investigation and trust the retailer and manufacturer. They don't have to rely on third parties to verify the authenticity of the product, which helps them have a smooth and risk-free user experience. There is no other way to know the key's private key unless the key accidentally leaks the key. A fully operational operation can effectively lower the anti-counterfeiting threshold for fortified goods and provide due diligence with a limited treasury and a simpler approach to give consumers the confidence and peace of mind that they do not survive the risk of counterfeiting. Overall, this activity based on blockchain technology can be a savior for businesses and provide a new system for trading, tokenization and tapping that is more secure and stone-friendly.

References

[1] Yildiran Yilmaz, Viet Hoa Do and Basel Halak , “ARMOR: An anti counterfeit security Mechanism for low cost Radio frequency identification systems”, 2021.

[2] Wenzheng Li and Mingsheng He, “Comparative Analysis of Bitcoin, Ethereum, and Libra,” 2020.

[3] N. Alzahrani, “Block supply chain: A new anti counterfeiting supply chain using NFC and blockchain,” 2018.

[4] Hao Shen1, Keren Liu1, Yuxuan Yao, Jun Wang, An ADS B Anti counterfeiting System Based on TDOA, IEEE International Conference on Signal, Inf ormation and data Processing in 2019”.

[5] 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.

[6] Blockchain Based Fake Product Identification in Supply Chain Ajay Funde, Pranjal Nahar, Ashwini Khilari.

[7] Fake News Detection In Social Media using Blockchain: - Shovon Paul, Jubair Joy, Shaila Sarkar.

[8] A Blockchain-Based Application System for Product Anti-Counterfeiting Jinhua Ma, Xin Chen, hung-Min Sun.

[9] Y. Dabbagh, R. Khoja, L. AlZahrani, G. AlShowaier and N. Nasser, "A Blockchain-Based Fake Product Identification System," 2022 5th Conference on Cloud and Internet of Things (CIoT), 2022, pp. 48-52, doi: 10.1109/CioT53061.2022.9766493.

[10] Daoud, E. & Gaedke, M., 2019. Decentralizing Products Certificates Using Blockchain. Cagliari, Italy, 18th International Conference on WWW/Internet, p. 8.

[11] Directorate-General for Justice and Consumers (European Commission), 2018. Results of the EU rapid alert system for dangerous non-food products, Brussels: European Commission.

[12] Li, L., 2013. Technology designed to combat fakes in the global supply chain. Business Horizons, 56(2), pp.

167-177. Liu, W. et al., 2016. SSD: Single Shot MultiBox Detector. s.l., arXiv preprint, arXiv:1512.02325.

[13] OECD/EUIPO, 2016. Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact. Paris: OECD Publishing. React, 2020.

[14] Redmon, J. & Farhadi, A., 2019. Yolov3: An incremental improvement. s.l., arXiv preprint arXiv:1804.02767.

[15] Ren, S., He, K., Girshick, R. & Sun, J., 2016. Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks. s.l., In Advances in neural information processing systems (pp. 91-99)..

[16] RESEARCH AND MARKETS, 2018. Global Brand Counterfeiting Report, s.l.: RESEARCH AND MARKERTS.

[17] Shields, D. & Deshmukh, R., 2020. Anti-Counterfeit Packaging Market - Food And Pharmaceuticals by Authentication Packaging Technology., 97220 United States:

[18] Global Opportunity Analysis and Industry Forecast. Statista, 2019. Number of smartphone users worldwide from 2016 to 2021, s.l.: Statista.

[19] Vahab, A., Naik, M. S., Raikar, P. G. & R, P. S., 2019. Applications of Object Detection System. International Research Journal of Engineering and Technology , 06(04), pp. 4186-4192.

[20] Zhao, Z., Zheng, P., Xu, S. & Wu, X., 2019. Object detection with deep learning: A review.. IEEE transactions on neural networks and learning systems, 30(11), pp. 3212-3232.

[21] M. R. Ullah, M. A. R. Bhuiyan and A. K. Das, "IHEMHA: Interactive healthcare system design with emotion computing and medical history analysis," 2017 6th International Conference on Informatics, Electronics and Vision & 2017 7th International Symposium in Computational Medical and Health Technology (ICIEV-ISCMHT), Himeji, 2017, pp.1-8.

[22] T. Adhikary, A. K. Das, M. A. Razzaque, M. O. Rahman and C. S. Hong, "A distributed wake-up scheduling algorithm for base stations in green cellular networks," ICUIMC '12 Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication, Kuala Lumpur, Malaysia, 2012,

[23] A. Tashnim, S. Nowshin, F. Akter and A. K. Das, "Interactive interface design for learning numeracy and calculation for children with autism," 2017 9th International Conference on Information Technology and Electrical Engineering (ICITEE), Phuket, 2017, pp.

[24] A. K. Das, T. Adhikary, M. A. Razzaque, M. Alrubaian, M. M. Hassan, Z. Uddin, and B. Song, "Big media healthcare data processing in cloud: a collaborative resource management perspective," Cluster Computing. Volume 20, Issue 2, pp 1599-1614. June 2017.

[25] S. Yu, K. Lv, and Z. Shao, "A High-Performance Blockchain Platform for Intelligent Devices IEEE Conference Publication" ieeexplore.ieee.org.2019

[26] T. Adhikary, A. K. Das, M. A. Razzaque, M. Alrubaian, M. M. Hassan, and A. Alamri, "Quality of service aware cloud resource provisioning for social multimedia services and applications," Multimedia Tools and Applications, Volume 76, Issue 12, pp 1-4485- 14509, June 2017.

[27] M. Akter, F. T. Zohra and A. K. Das, "Q-MAC: QoS and mobility Taware optimal resource allocation for dynamic application offloading in mobile cloud computing," 2017 International Conference on Electrical, Computer and Communication Engineering (ECCE). Cox's Bazar, 2017, pp. 803-808.

[28] S. Gilda, "Evaluating machine learning algorithms for fake news detection - IEEE Conference Publication," ieeexplore.ieee.org, 2019.

[29] M. Granik and V. Mesyura, "Fake news detection using naive Bayes classifier - IEEE Conference Publication," ieeexplore.ieee.org. 2019.

[30] A. Dey, R. Rafi, S. Hasan, and S. Kundu, "Fake news pattern recognition using linguistic analysis," Dspace.bracu.ac.bd, 2019.

[31] A. K. Das, A. Ashrafi and M. Ahmmad, "Joint Cognition of Both Human and Machine for Predicting Criminal Punishment in Judicial System." 2019 4th International Conference on Computer and Communication Systems (ICCCS), Singapore, 2019.

[32] FaNDeR: Fake News Detection Model Using Media Reliability -IEEE Conference Publication. [Accessed 22 Mar. 2019].

[33] A. K. Das, T. Adhikary, M. A. Razzaque, E. J. Cho and C. S. Hong, “A QoS and profit aware cloud confederation model for IaaS service providers,” ICUIMC ’14 Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication, Siem Ream, Cambodia, 2014.

[34] F. T. Zohora, M. R. R. Khan, M. F. R. Bhuiyan and A. K. Das, “Enhancing the capabilities of IoT based fog and cloud infrastructures for time sensitive events,” 2017 International Conference on Electrical Engineering and Computer Science (ICECOS), Palembang, 2017, pp.224-230.