International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Authentication of Product & Counterfeits Elimination Using Blockchain

Mr. D. Koteswarao, Associate Professor & HOD of Data Science Department, NRI institute of technology, Andhra Pradesh, India, dkr.itds9@gmail.com.

Mrs. P. Nalini, Assistant Professor, department of Data Science, NRI institute of technology, Andhra Pradesh, India, Nalini.polu@gmail.com.

K. Harika, department of Data Science, NRI institute of technology, Andhra Pradesh, India, harikakotte55@gmail.com.

N. Jyothi Swaroop, Department of Data Science, NRI institute of technology, Andhra Pradesh, India.

K. Rakesh, Department of Data Science, NRI institute of technology, Andhra Pradesh, India.

M. Naveen, Department of Data Science, NRI institute of technology, Andhra Pradesh, India.

Abstract:

Blockchain technology has garnered significant interest due to its potential to disrupt various industries beyond finance. This paper investigates the application of blockchain in combating counterfeiting. By eliminating the need for trusted intermediaries, enabling faster transactions, and enhancing transparency, blockchain offers promising solutions to address counterfeit issues. The paper presents an overview of anti-counterfeit solutions, different blockchain technologies, and highlights the unique characteristics of blockchain that make it suitable for this use case. Three novel concepts and the expansion of an existing system are explored, emphasizing that technological solutions alone cannot effectively reduce counterfeiting. A multifaceted approach involving increased awareness, legal measures against counterfeiters, robust alert systems, and tamper-proof packaging is essential. By integrating blockchain technology with these strategies, a comprehensive and efficient approach to combat counterfeiting can be achieved.

Keywords – Authentication, Blockchain, Encryption

1. INTRODUCTION

Counterfeiting is a pervasive issue that permeates various industries, posing significant economic and health risks on a global scale. From fashion and retail products to pharmaceuticals and digital media, counterfeit goods infiltrate markets worldwide, undermining consumer trust and safety [1]. The impact of counterfeiting extends far beyond mere economic losses, threatening public health, intellectual property rights, and legitimate businesses [2].

The scale of counterfeiting is staggering, with reports estimating its cost at approximately $600 billion annually in the United States alone [3]. Moreover, projections by the International Chamber of Commerce indicate that counterfeiting and piracy could drain a staggering $4.2 trillion from the global economy by 2022, endangering millions of legitimate jobs [4]. In the pharmaceutical sector, the counterfeit medicine market is particularly alarming, accounting for around 1 million deaths per year and posing grave dangers to public health [5]. With an estimated worth of $75 billion annually, the counterfeit medicine industry is growing at an alarming rate, far surpassing the growth of legitimate pharmaceuticals and rivaling the global narcotics trade in profitability [6].

Trust forms the cornerstone of all transactions, whether it involves financial transactions, exchange of goods, or provision of services. However, establishing trust becomes increasingly challenging in transactions where multiple parties and intermediaries are involved, such as international money transfers facilitated by banks and clearinghouses [7]. These third-party intermediaries not only add complexity to transactions but also increase costs and introduce vulnerabilities to fraud and counterfeiting [8].

The emergence of blockchain technology presents a revolutionary solution to address the challenges posed by counterfeiting and the need for trust in transactions. Initially introduced as the underlying technology for cryptocurrencies like Bitcoin, blockchain technology has demonstrated its potential to eliminate the need for trusted intermediaries and ensure secure, transparent, and immutable transactions [9]. Bitcoin's success in facilitating direct peer-to-peer transactions without intermediaries has showcased the transformative power of blockchain in revolutionizing traditional financial systems [10].

Blockchain technology operates on the principles of decentralization, cryptographic security, and consensus mechanisms, enabling the creation of tamper-proof and transparent transaction records [11]. By leveraging blockchain, transactions can be securely recorded and verified in a decentralized manner, eliminating the risk of tampering or manipulation [12]. The distributed nature of blockchain ensures that transaction data is accessible to all participants in the network, fostering trust and transparency [13].

Beyond financial transactions, blockchain holds immense potential to redefine various aspects of the digital economy, including supply chain management, intellectual property rights, and anti-counterfeiting efforts [14]. By enabling the tracking and authentication of products throughout their lifecycle, blockchain technology offers a robust solution to combat counterfeiting and ensure the integrity of goods [15].

Authentication plays a pivotal role in combating counterfeiting, allowing consumers and authorities to verify the authenticity of products and safeguard against the harmful effects of counterfeit goods [16]. Traditional authentication methods rely on overt or covert features embedded within products to confirm their genuineness [17]. However, these methods are often susceptible to replication or manipulation by counterfeiters, underscoring the need for more robust and tamper-proof authentication solutions [18].

This paper aims to explore the potential of blockchain technology in reducing counterfeiting by providing a comprehensive overview of existing anti-counterfeit solutions, different blockchain technologies, and their applicability to the

authentication of products [19]. By examining the strengths and limitations of blockchain in addressing counterfeit issues, this paper seeks to propose innovative strategies and concepts for leveraging blockchain technology to enhance authentication and combat counterfeiting effectively [20].

2. LITERATURE SURVEY

Counterfeiting poses a significant threat to various industries, ranging from fashion and retail to pharmaceuticals and digital media. As the scale of counterfeiting continues to escalate, there is a growing need for innovative solutions to combat this pervasive problem. In recent years, blockchain technology has emerged as a promising tool for addressing counterfeiting by providing secure, transparent, and tamper-proof transaction records [1].

Satoshi Nakamoto's seminal paper, "Bitcoin: A Peer-to-Peer Electronic Cash System," laid the foundation for blockchain technology [2]. Nakamoto's vision of a decentralized digital currency system, powered by a distributed ledger, demonstrated the potential of blockchain to revolutionize traditional financial systems and eliminate the need for trusted intermediaries [3]. Since then, blockchain has evolved beyond cryptocurrencies like Bitcoin, finding applications in various industries, including anti-counterfeiting efforts [4].

Hyperledger, an open-source collaborative effort hosted by the Linux Foundation, has contributed significantly to advancing blockchain technology. In their document "HyperledgerBlockchain Performance Metrics," Hyperledger provides insights into the performance metrics of blockchain networks, including throughput, latency, and scalability [5]. Understanding the performance characteristics of blockchain is crucial for assessing its suitability for anti-counterfeiting applications and ensuring efficient transaction processing [6].

R.C. Merkle's work on public key cryptosystems laid the groundwork for cryptographic techniques used in blockchain technology [7]. Merkle's protocols for public key cryptosystems form the basis for ensuring the security and integrity of transactions recorded on the blockchain. By employing cryptographic hashing and digital signatures, blockchain achieves immutability and authenticity, making it a robust solution for combating counterfeiting [8].

Armin Ronacher's documentation on Flask, a lightweight web application framework, highlights the practical implementation of blockchain technology in real-world applications [9]. Flask's versatility and ease of use make it a valuable tool for developers seeking to integrate blockchain into anti-counterfeiting solutions. By leveraging Flask's capabilities, developers can create secure and user-friendly interfaces for authenticating products and tracking their provenance on the blockchain [10].

Gavin Wood's paper on Ethereum, titled "Ethereum: A secure decentralized generalized transaction ledger," introduced the concept of smart contracts, enabling programmable and self-executing transactions on the blockchain [11]. Ethereum's innovative approach to blockchain technology expands its applicability beyond financial transactions, offering a platform for implementing complex business logic and authentication mechanisms [12]. Smart contracts hold immense potential for enhancing anti-counterfeiting efforts by automating authentication processes and ensuring compliance with predefined rules and regulations [13].

The Organization for Economic Co-operation and Development (OECD) has extensively researched illicit trade and its impact on the global economy. In their publication "Illicit Trade: Converging Criminal Networks," the OECD examines the convergence of criminal networks involved in counterfeiting, smuggling, and other illicit activities [14]. The OECD's insights into the intricate networks behind illicit trade underscore the need for coordinated international efforts to combat counterfeiting and protect legitimate businesses [15].

In the field of distributed systems, Miguel Castro and Barbara Liskov's work on practical Byzantine fault tolerance (PBFT) has significant implications for blockchain technology [16]. PBFT protocols enable decentralized systems to maintain consensus and tolerate Byzantine faults, ensuring the integrity and reliability of transaction processing [17]. By implementing PBFT mechanisms, blockchain networks can withstand malicious attacks and maintain trust among network participants, critical factors in combating counterfeiting [18].

Additionally, Elaine Clement et al.'s research on making Byzantine fault-tolerant systems tolerate Byzantine faults addresses the challenges of designing resilient distributed systems [19]. Their work provides valuable insights into mitigating the impact of Byzantine faults on blockchain networks, enhancing their robustness and fault tolerance [20].

Overall, the literature survey highlights the diverse contributions to blockchain technology and its potential applications in combating counterfeiting. From foundational works on cryptography and distributed systems to practical implementations and case studies, the body of literature provides a comprehensive understanding of blockchain's role in authentication and anti-counterfeiting efforts [21]. As blockchain technology continues to evolve, interdisciplinary collaboration and research efforts will be crucial for unlocking its full potential in addressing the challenges posed by counterfeiting.

3. METHODOLOGY

a) Proposed Work:

Our proposed system integrates blockchain technology to revolutionize the authentication process, addressing the shortcomings of traditional methods. Blockchain's decentralized ledger ensures that each product is assigned a unique digital identifier or "token," which is securely recorded and immutable.

The decentralized nature of blockchain ensures that no single entity has control over the system, reducing the risk of data manipulation or tampering. This enhances transparency and trust, as stakeholders can verify the authenticity of products independently without relying on centralized authorities.

To further bolster security, tamper-evident packaging is employed to deter counterfeiters and safeguard products from unauthorized access or alteration. Any attempt to tamper with the packaging would be immediately detectable, triggering alerts and investigation procedures.

Moreover, smart contracts can be utilized to automate legal agreements and penalties, ensuring swift and effective action against perpetrators.

Overall, our proposed system offers a comprehensive approach to combating counterfeiting by leveraging blockchain technology's transparency, immutability, and decentralization.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

b) System Architecture:

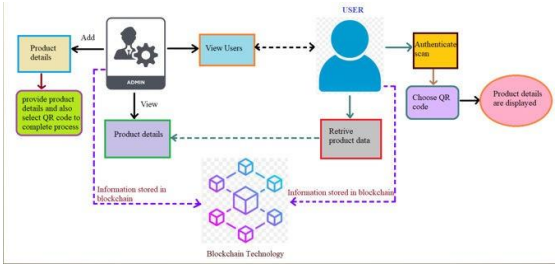


Fig1 Proposed Architecture

The system architecture for integrating blockchain technology into product authentication processes involves several key components. Firstly, a decentralized blockchain network is utilized to securely store and manage product details. Each product is assigned a unique identifier, and relevant information such as manufacturing details, supply chain history, and authenticity verification records are stored on the blockchain.

When a user scans the product's QR code, the system retrieves the corresponding information from the blockchain, ensuring transparency and integrity. Authentication is facilitated through cryptographic verification mechanisms, leveraging the immutability and tamper-proof nature of blockchain transactions.

An administrative interface allows authorized users to view and manage product details, while the blockchain network ensures data integrity and accessibility across multiple nodes. This architecture ensures a secure and transparent product authentication process, enhancing consumer trust and combating counterfeiting effectively.

c) Save Product with Blockchain Entry

This module acts as the primary interface for authenticating products within the supply chain. Users input product details and link them with barcode images. A unique digital signature is generated for each barcode. Upon validating previous transactions on the blockchain, the product details, digital signatures, and associated information are securely recorded as a new transaction block. This process ensures the integrity and authenticity of product data throughout the supply chain.

d) Retrieve Product Data

This module facilitates user access to product information stored in the blockchain. By inputting a product ID, users can efficiently retrieve corresponding details. This functionality enhances transparency and traceability within the supply chain, enabling users to access reliable and accurate data about products. With seamless access to blockchain-stored information, users can make informed decisions and ensure the integrity of the supply chain ecosystem.

e) Authenticate Scan

The Authenticate Scan module is pivotal in product verification, where users upload scanned barcode images. The system cross-references their digital signatures with blockchain records. Upon a match, product authenticity is confirmed, and details are displayed. In cases of no match, authentication fails, signaling potential counterfeit products. This process ensures transaction safety and fosters trust by promptly identifying and alerting users to possible counterfeit goods.

f) Blockchain Integration

blockchain technology is utilized to verify the authenticity of products as they move through the supply chain. Each product is associated with a unique identifier or digital record on the blockchain, making it possible to track the product's journey from its source to the end

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

consumer. This transparency ensures that products are legitimate and not counterfeit.

By leveraging blockchain for online transactions, the system reduces reliance on third-party intermediaries like banks or payment processors. Blockchain's inherent security features, including encryption and decentralized verification, enhance the overall security of transactions. This means that participants can engage in transactions with greater confidence, knowing that the blockchain network verifies and secures each transaction.

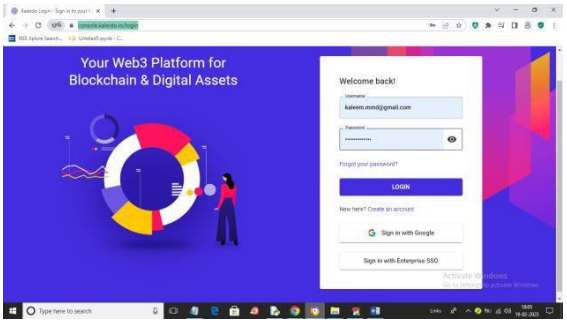
Product information and barcodes are converted into digital signatures, which are unique representations of the data. These digital signatures are then securely stored on the blockchain. The tamper-proof nature of the blockchain ensures that once the data is recorded, it cannot be altered or tampered with, maintaining the integrity and authenticity of the product details.

4. EXPERIMENTAL RESULTS

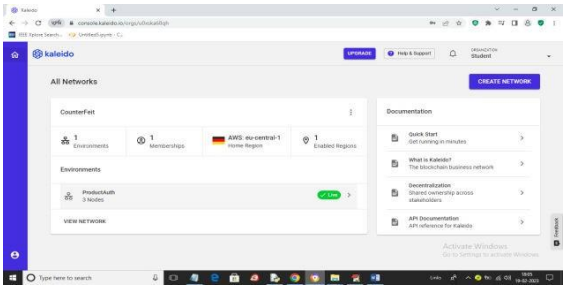
Authentication of Product & Counterfeits Elimination Using Blockchain

To connect to hyperledger running node and peers we need to follow bellows steps

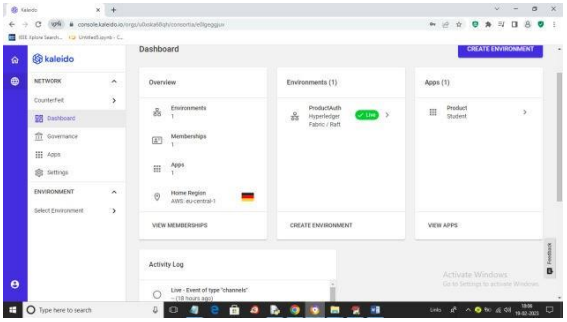
1) Open browser and enter URL as https://console.kaleido.io/login
2) Enter username as 'kaleem.mmd@gmail.com' and password as 'Offenburg965#' and then press button to login to Blockchain cloud application like below screen



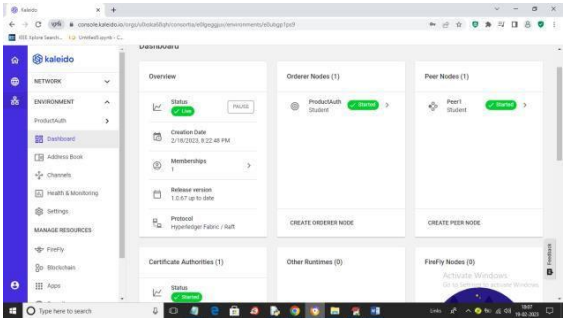
3) After login will get below page



In above screen in bottom line you can see link like 'VIEW NETWORK' and then click on that link to get below page

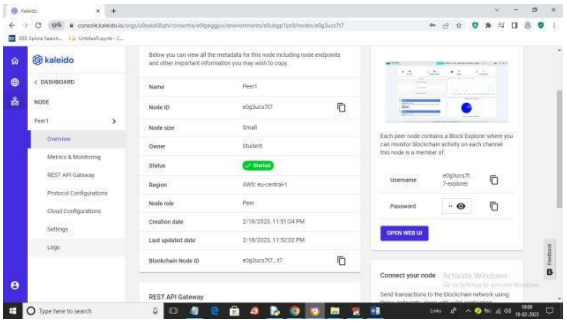


In above screen in middle panel you can see 'ProductAuthHyerledger Fabric' and just click on that to get below page

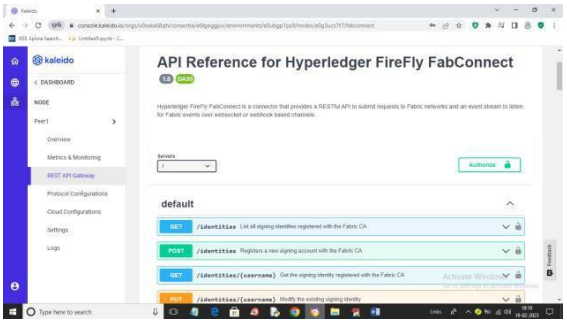


In above screen in last panel you can see one peer is running called "Peer1" and just click on that 'Peer1' link to get below page

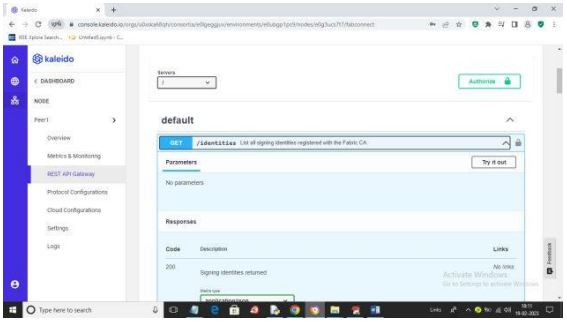
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362



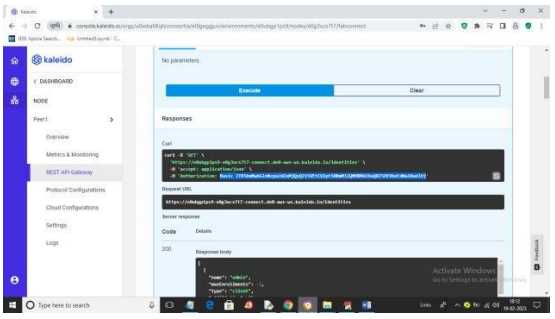
In above screen we can see hyper ledge peer started and now from left side of panel you can see ‘REST API Gateway’ and just click on that to get below page



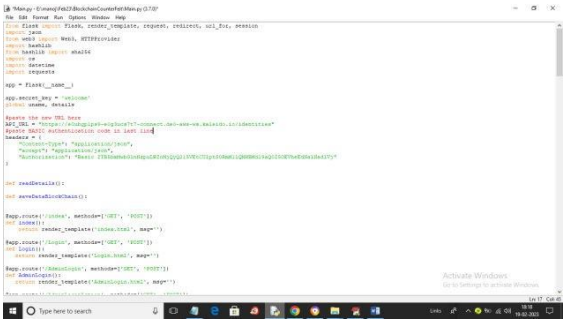
In above screen Hyperledger started and running and now click on first ‘GET’ button to get Hyperledger URL and we need to specify that URL in python program to save data inserted in our Counter Feit application



In above screen from left side click on ‘Try it Out’ button and then click on ‘Execute’ button to get below page



From above screen just copy which I am showing blue colour selected text and then paste that code inside python ‘Main.py’ application which I am showing in below screen and you need to copy and paste Request URL also showing in above screen



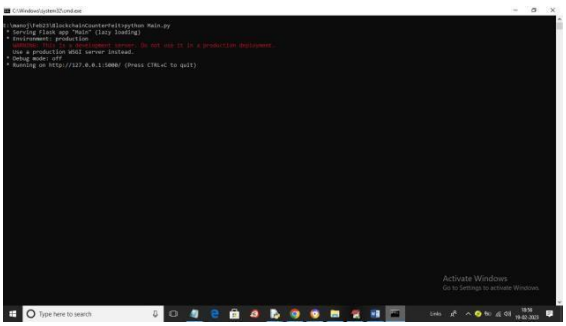
In above screen you can see in API_URL I pasted copied Requested URL (https://e0ubgp1ps9-e0g3ucs7t7-connect.de0-aws-ws.kaleido.io/identities) and then in headers last 3rd green line I pasted (Basic ZTB5bmMwbGlnNzpuLWZoMjQyQ215VEtCUlptS0RmM1lQMHBMdl9aQ0Z5OEVheEdNalNadlVj)

So whenever you are running application you need to login and then copy both request URL and authentication code and paste in PYTHON Main.py so python can connect to Hyperledger and save data.

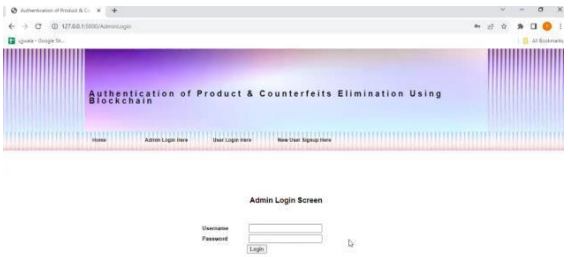
So with above instructions your Hyperledger and python code is sync up and now you can run code as similar t previous application.

Now double click on ‘run.bat’ file to start FLASK server and get below page

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362



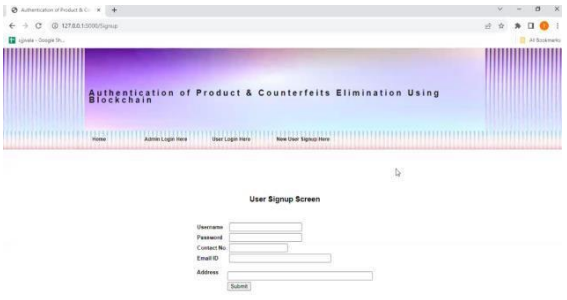
In above screen FLASK server started and now open browser and enter URL as 'http://127.0.0.1:5000/index' and press enter key to get below page

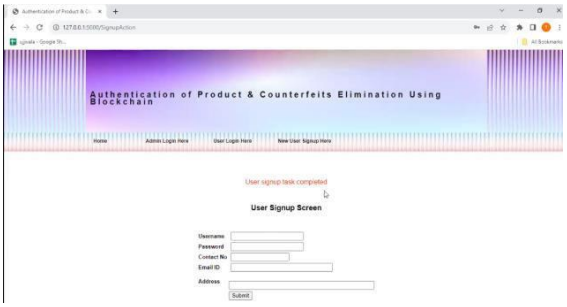


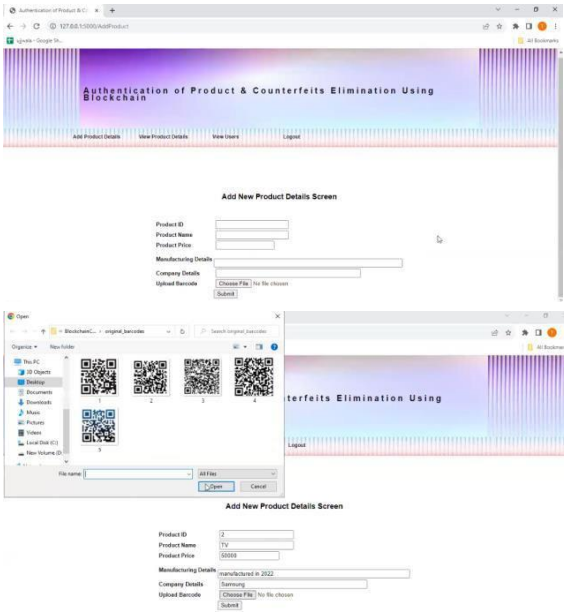
In above screen admin is login and after login will get below page

In above screen click on 'Admin Login Here' link to login as admin and get below page

In above screen click on 'Add Product Details' link to get below page

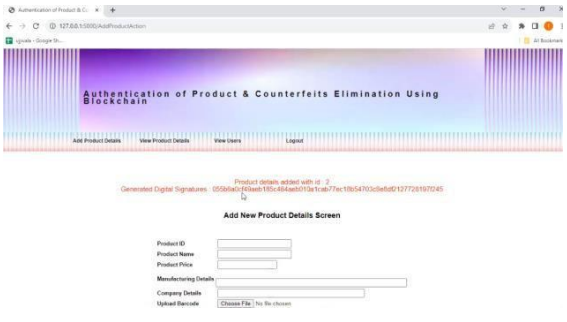




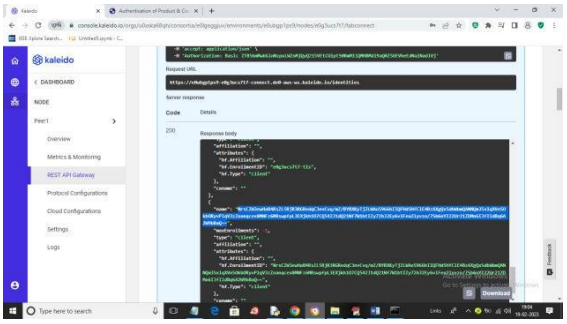


In above screen entering product details and then uploading bar code image and then press button to get below page

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362



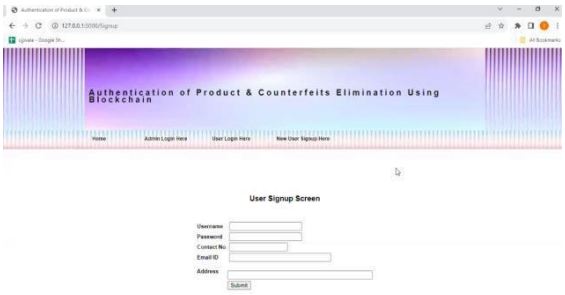
In above screen product details added and we can see generated digital signatures and this encrypted will be saved inside Hyperledger below screen and just you need to click on 'GET' button and click 'Try it out' and then click 'Execute' button to get below output in Hyperledger cloud page like below screen

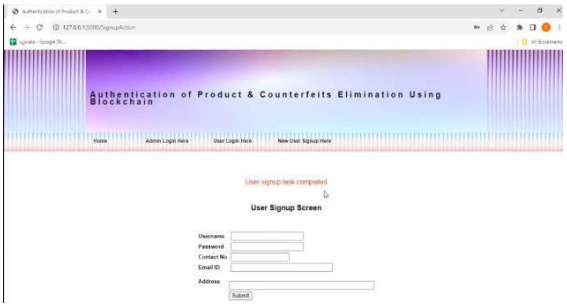


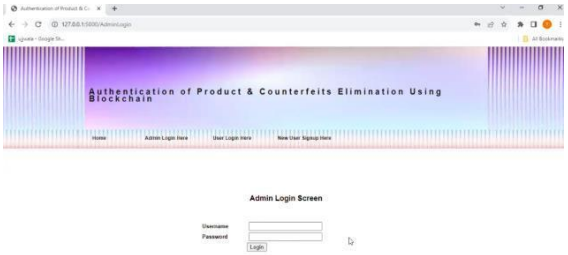
In above screen in blue colour text we can see AES encrypted data saved at Hyperledger and similarly each inserted record will saved at this HyperledgerBlockchain

Now in below screen I am registering new user and after pressing button then this user also will get saved inside Hyperledger in encrypted format

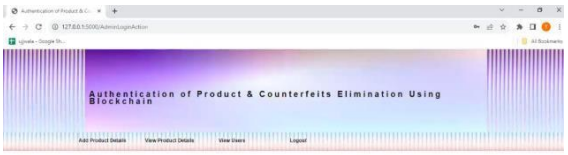
In above screen click on 'Admin Login Here' link to login as admin and get below page





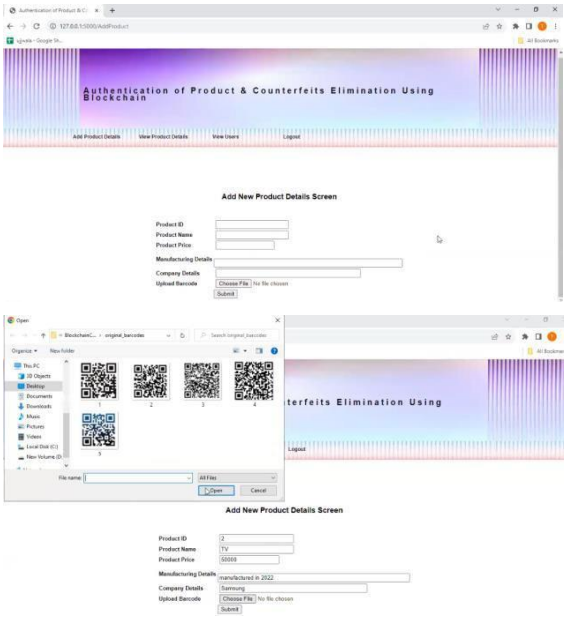


In above screen admin is login and after login will get below page



In above screen click on 'Add Product Details' link to get below page

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362



In above admin screen click on 'View Product Details' link to get all details from Hyperledger in decrypted format like below screen

In above screen we can see all product details in decrypted format and now click on 'View Users' link to view all registered user details

In above screen we can see all user details and now logout and login as user

In above screen user is login and after login will get below page

In above screen user can click on 'Retrieve Product Data' link button to get below output

In above screen enter product ID and press button to retrieve details from Blockchain like below screen

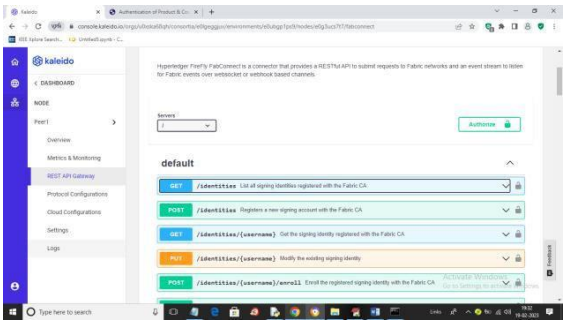
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

In above screen user can view product details by ID and now click on 'Authentication Scan' link to authenticate product using bar code image

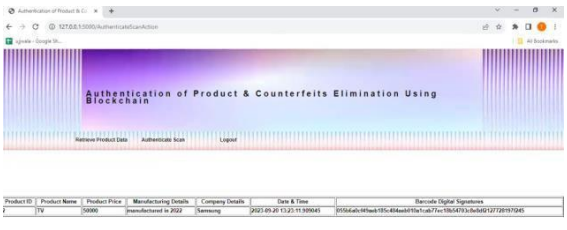
In above screen uploading fake code and press button to get below page

In above screen we can see authenticated failed and now in below screen we can see each transaction proof of work by clicking on 'LOG' link

In above screen uploading 'QR code' image and then click on 'Submit' button to get product details if CODE authenticated like below screen

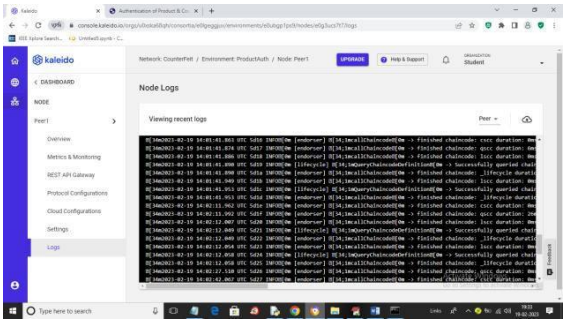


In above screen in left side panel bottom you can see link like 'LOGS' just click on that link to view mining of all transactions



In above screen code is authenticated and we got product details and now will upload fake product code and test it

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362



In above log we can see each chain code is successfully mined and queried to retrieve details. All transaction details you can see in above logs file

5. CONCLUSION

In conclusion, the development of a blockchain-based system dedicated to authenticating products within the supply chain marks a significant step forward in combating counterfeiting. The project's emphasis on user-friendliness through an intuitive interface streamlines product verification processes. By leveraging blockchain technology, the project reduces reliance on third-party intermediaries, enhancing transaction security. The implementation of digital signatures and secure blockchain storage ensures data integrity, maintaining the accuracy and reliability of product information. Ultimately, the project's impact extends to public safety and financial security by thwarting the entry of counterfeit products into the market, thereby protecting consumers from harm and businesses from economic losses. Through its comprehensive approach to product authentication, the project contributes to fostering trust and integrity within the supply chain ecosystem, underscoring the transformative potential of blockchain technology in combating counterfeiting and ensuring the authenticity of goods.

6. FUTURE SCOPE

Future iterations of the system hold immense potential for further advancement and enhancement. Integration of Internet of Things (IoT) devices presents a promising avenue to bolster product tracking and authentication capabilities. By embedding IoT sensors into products or packaging, real-time data on product location, environmental conditions, and other pertinent parameters can be collected, thereby enhancing traceability and security within the supply chain.

Moreover, the incorporation of artificial intelligence (AI) and machine learning (ML) algorithms stands to revolutionize counterfeit detection and prevention efforts. These advanced technologies can analyze vast datasets derived from blockchain transactions and IoT devices to discern counterfeit patterns and anomalies. By leveraging AI and ML, the system can proactively identify suspicious activities, mitigate risks, and fortify defenses against counterfeit infiltration, thereby further safeguarding consumers and businesses alike.

Overall, the future scope of the system lies in leveraging cutting-edge technologies to continuously innovate and enhance its capabilities, ultimately fostering greater transparency, security, and trust within the supply chain ecosystem.

REFERENCES

[1] Satoshi Nakamoto, ―Bitcoin: A Peer-to-Peer Electronic Cash System‖, 2008

[2] Hyperledger, ―HyperledgerBlockchain Performance Metrics‖, V1.01, October 2018

[3] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on

Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[4] Armin Ronacher, ―Flask Docs‖, http://flask.pocoo.org/docs/‖

[5] G. Wood, __Ethereum: A secure decentralised generalized transaction ledger,‘‘ Tech. Rep., 2014.

[6] OECD (2016), Illicit Trade: Converging Criminal Networks, OECD Reviews of Risk Management Policies, OECD Publishing, Paris, https://doi.org/10.1787/9789264251847-en.

[7] M. Castro and B. Liskov, __Practical byzantine fault tolerance and proactive recovery,‘‘ ACM Trans. Comput. Syst., vol. 20, no. 4, pp. 398 461, Nov. 2002.

[8] Clement, E. Wong, L. Alvisi, M. Dahlin, and M. Marchetti, __Making byzantine fault tolerant systems tolerate byzantine faults,‘‘ in Proc. 6th USENIX Symp. Netw. Syst. Design Implement., 2009, pp. 153–168.

[9] Cachin, __Architecture of the hyperledgerblockchain fabric,‘‘ Tech. Rep., Jul. 2016..

[10] S. Underwood, ―Blockchain Beyond Bitcoin‖, in Communications of the ACM, vol. 59, no. 11, p. 15-17, 2016.

[11] Deloitte, Israel: A Hotspot for Blockchain Innovation, 2016. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/il/Documents/financial-services/israel_a_hotspot_for_blockchain_innovation_ feb2016_1.1.pdf. [Accessed: 2.11.2016].

[12] G. Greenspan and M. Zehavi, Will Provenance Be the Blockchain‘s Break Out Use Case in 2016?, 7.1.2016. [Online]. Available: http://www.coindesk.com/ provenance-blockchain-tech-app/. [Accessed: 12.12.2016].

[13] Counterfeit medicines. QA counterfeit.World Health Organization (WHO) 2009. Available from: http://www.who.int/medicines/services/counterfeit/faqs/QACounterfeit-october2009.pdf [last cited on 2010 Jun 12].

[14] An ICC initiative Business Action to Stop Counterfeiting and Piracy (BASCAP). Brand protection directory.The World Business Organization. Available from: http://www.iccwbo.org/bascap [last cited on 2010 Jun 10].

[15] L. Li, ―Technology designed to combat fakes in the global supply chain‖, in Business Horizons, vol. 56, no. 2, p. 167-177, 2013.

[16] White paper. Dhar R. Anti counterfeit packaging technologies.A strategic need for the Indian industry. Confederation of Indian Industry 2009:1-47. Available from: http://www.bilcare.com/pdf/CII_anti_counterfeit_pkg_technologies_report.pdf [last cited on 2010 Oct 29].

[17] Berman, ―Strategies to detect and reduce counterfeiting activity‖, in Business Horizons, vol. 51, no. 3, p. 191-199, 2008.

[18] K. D´egardin, Y. Roggo and P. Margot. ―Understanding and fighting the medicine counterfeit market‖, in Journal of Pharmaceutical and Biomedical Analysis, vol. 87, p. 167-175, 2013

[19]R. C. Merkle, __A digital signature based on a conventional encryption function,‘‘ in Proc. Conf. Theory Appl. Cryptogr. Techn., 1987, pp. 369–378

[20] J. Leng, P. Jiang, K. Xu, Q. Liu, J. L. Zhao, Y. Bian, and R. Shi, ‘‘Makerchain: A blockchain with chemical signature for selforganizing process in

social manufacturing,''J. CleanerProd., vol. 234, pp. 767–778, Oct. 2019.

[21] N. Alzahrani and N. Bulusu, ''Block-supply chain: A new anticounterfeiting supply chain using NFC and blockchain,'' in Proc. 1st Workshop CryptocurrenciesBlockchainsDistrib. Syst. (CryBlock), 2018, pp. 30–35.

[22] (2018). Litecoin.[Online]. Available: https://litecoin.info/index.php/Main Page

[23] (2019). Github.[Online]. Available: https://github.com/ethereum/wiki/ wiki/White-Paper

[24] G. Wood, ''Ethereum: A secure decentralised generalised transaction ledger,'' Ethereum Project YellowPaper, vol. 151, p. 1–32, Apr. 2014.

[25] S. Panikkar, S. Nair, P. Brody, and V. Pureswaran, ''ADEPT: An IoT practitioner perspective,'' IBM Inst. Bus. Value, New York, NY, USA, White Paper, 2015, pp. 1–18.

[26] (2018). Cryptokitties.[Online]. Available: https://www.cryptokitties.co/

[27] S. Matthew English and E. Nezhadian, ''Application of bitcoindatastructures& design principles to supply chain International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 08 Issue: 03 | Mar 2021 www.irjet.net p-ISSN: 2395-0072 © 2021, IRJET | Impact Factor value: 7.529 | ISO 9001:2008 Certified Journal | Page 1358 management,'' 2017, arXiv:1703.04206. [Online]. Available: http://arxiv.org/abs/1703. 04206

[28] F. Tian, ''Anagri-food supply chain traceability system for China based on RFID &blockchain technology,'' inProc. 13th Int. Conf. Service Syst. Service Manage. (ICSSSM), Jun. 2016, pp. 1–6.

[29] Q. Lu and X. Xu, ''Adaptable blockchain-based systems:A case study for product traceability,'' IEEE Softw., vol. 34, no. 6, pp. 21–27, Nov./Dec. 2017. VOLUME 8, 2020 77651 J. Ma et al.: Blockchain-BasedApplication System for ProductAntiCounterfeiting

[30] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, ''A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain,'' IEEE Access, vol. 5, pp. 17465–17477, 2017.