KALYANI GOVERNMENT ENGINEERING COLLEGE

Affiliated to

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY

Department of Computer Application

Kalyani – 741235, Nadia, WB

Project report on

Authentication of Product & Counterfeits Detection Using Blockchain (AuthDApp)

Submitted by

Prayag Dey
Roll No: - 10271022020

Ananya Kundu
Roll No: - 10271022026

Sudipa Biswas
Roll No: - 10271022027

Under the guidance of

Mrs. Arpita Nath (Assistant Professor)

Phone: 25826680 (PBX)
Fax : 25821309

Email : contact@kgec.edu.in

কল্যাণী - ৭৪১ ২৩৫
নদীয়া, পশ্চিমবঙ্গ

Kalyani 741 235
Nadia, West Bengal,India

পত্রাঙ্ক /Ref. No.:
তারিখ / Date :

কল্যাণী গভঃ ইঞ্জিনিয়ারিং কলেজ
Kalyani Government Engineering College
(Govt. of West Bengal)

CERTIFICATE OF APPROVAL

This certifies that the project report titled "Authentication of Product & Counterfeits Detection Using Blockchain" is a record of project work completed by the following students of Kalyani Government Engineering College:

1. Prayag Dey (Roll: 10271022020)
2. Ananya Kundu (Roll: 10271022026)
3. Sudipa Biswas (Roll: 10271022027)

The project work was carried out under the guidance of Mrs. Arpita Nath. It was submitted as a requirement for the partial fulfillment of the Degree of Master of Computer Application from Maulana Abul Kalam Azad University of Technology (MAKAUT) for the 2nd year 3rd semester examination in the subject “Minor Project and Viva-voce (MCAN-381)” for the academic year 2023-24.

Head of Department
Department of Computer Application
Kalyani Government Engineering College

Supervisor
Department of Computer Application
Kalyani Government Engineering College

Examiner

Department
Seal

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to our principal, Dr. Sourabh Kumar Das, our Headof Department, Dr. Surya Sarathi Das, and our project supervisor, Mrs. Arpita Nath, for providingus with the opportunity to work on the "Authentication of Product & Counterfeits Elimination Using Blockchain" project.Their guidance and support enabled us to conduct extensive research and learn about new technologies.

We would also like to extend our gratitude to all the faculty members who contributed to the successful completion of this project within the given timeframe.

Finally, we are grateful to our friends and family for their unwavering support throughout this project.

Prayag Dey
Roll: 10271022020

Ananya Kundu
Roll:10271022026

Sudipa Biswas
Roll:10271022027

DECLARATION

We, the authors of this project, affirm that the content presented herein is our original work and that we have not plagiarized any content or ideas from other sources. We have adhered to all principles of academic honesty and integrity, and we have conducted thorough research to ensurethat all information presented in this project is accurate and reliable.

We understand the importance of upholding the highest standards of academic honesty and integrity, and we are committed to demonstrating these values throughout the implementation of this project. We recognize that academic dishonesty undermines the credibility and integrity of theacademic community and can have severe consequences for individuals, institutions, and society as a whole.

As such, we pledge to continue to uphold these principles and to act with honesty, integrity, and transparency in all our academic and professional endeavors related to this project. We will alwaysattribute credit where credit is due, and we will acknowledge and cite all sources appropriately. We also pledge to hold ourselves and others accountable for upholding these principles and to work towards creating a culture of academic honesty and integrity in all our academic and professional communities related to this project.

ABSTRACT

Though it can seem like a far-off notion, counterfeits are all around us. Anything from software, digital media, gadgets, piracy, and intellectual property to fashion and retail goods. Sending money or trading commodities becomes challenging if there is a lack of confidence between the parties.

These days, authentication is done through a third-party company, which is untrustworthy. Eliminating these outside parties can speed up procedures, save total costs, and increase transparency. Blockchain has been able to demonstrate the possibility of eliminating such third parties. Blockchain technology makes it possible for immutable transactions, which are always visible to everyone. Because the data is available to the public, it is accessible and dispersed worldwide. It is cryptographically sealed and updated chronologically. It is necessary to observe the entire spectrum of potential applications for this technology, but monitoring a product's ownership and history is undoubtedly one of them. This project, "Authentication of Product & Counterfeits Elimination Using Blockchain," can assist each person in tracking the authenticity of their own products. Full transparency and the elimination of third parties' involvement are possible with blockchain technology.

TABLE OF CONTENTS

LIST OF FIGURES

INTRODUCTION

The pervasive issue of counterfeiting affects businesses and consumers in a big way. The manufacturing and distribution of counterfeit goods undermine consumer trust, destroy brand equity, and potentially jeopardize public safety, particularly in industries such as high-end retail, electronics, and pharmaceuticals. As counterfeiters become more skilled, traditional supply chain tracking and authentication methods are not working.

Blockchain technology has proven to be a workable solution for this issue. It offers a safe, decentralized ledger system that ensures data openness, participant confidence, and resistance to tampering. Blockchain is a fantastic solution for product identification and removing counterfeit items from the supply chain because it is transparent and immutable.

This project investigates how blockchain technology may be used in the real world to authenticate products and get rid of counterfeits. We want to look into how blockchain can work with the supply chain management systems that are in place now, how products can be registered, how to make goods transparent and traceable, how to automate processes with smart contracts, how to interact with customers through user-friendly interfaces, and how to identify and take out counterfeit goods.

OBJECTIVE AND GOALS

The project, "Authentication of Product & Counterfeits Detection Using Blockchain (AuthDApp)," aims to tackle the widespread problem of counterfeiting in a variety of industries, including retail items, software, digital media, gadgets, piracy, intellectual property, and fashion. The project's goal is to create a transparent and safe method for product authentication that uses blockchain technology to do away with the need for outside authentication providers. The primary objective is to improve consumer trust, safeguard brand equity, and guarantee public safety through the provision of a decentralized, tamper-proof ledger system for product authenticity tracking.

In particular, the project aims to investigate how blockchain can be integrated with existing supply chain management systems to facilitate product registration, transparent and traceable goods, automation through smart contracts, consumer engagement through user-friendly interfaces, and the detection and removal of counterfeit goods from the market. Through the accomplishment of these objectives, the project hopes to show that blockchain technology can revolutionize product authentication by providing a decentralized solution that is more effective, transparent, and economical than current techniques.

The project's broad objectives take into account practical difficulties and constraints in addition to technical elements like algorithm implementation and system design. The documentation recognizes that scaling concerns, integration hurdles, and related expenses require ongoing attention. In order to further improve the system's capabilities, the project team is also dedicated on resolving user acceptance issues, making sure smart contract and security flaws are minimized, and investigating potential future improvements including integration with IoT devices and artificial intelligence. To sum up, the project seeks to further the ideals of security, integrity, and transparency in product authentication while also pushing the continuous advancement of technology in the fight against counterfeiting.

PROBLEM DEFINITION AND ANALYSIS

- **Problem Definition:** Every industry is affected by counterfeiting: software, digital media, electronics, piracy, intellectual property, fashion, and retail products are just a few. The ubiquity of counterfeit goods erodes consumer confidence in transactions, making it difficult for people and companies to conduct safe money and goods exchanges. Reliance on external authentication services raises questions regarding reliability and effectiveness, which drives up expenses and obscures transactional processes.

  Existing authentication procedures, which are frequently handled by outside businesses, might be slowed down and are vulnerable to hacking. It is obvious that a more dependable and effective verification process is required, one that does not entail the participation of dubious third parties. A promising answer to these problems appears to be blockchain technology.
- **Problem Analysis:**
  1. **Prevalence of Counterfeits:**
     - A variety of industries, including software, digital media, fashion, and retail items, are affected by counterfeiting.
     - A lack of confidence in the legitimacy of products makes transactions difficult and may result in losses of money.
  2. **Dependency on Third-Party Authentication:**
     - Current authentication procedures frequently depend on outside businesses.
     - Inefficiencies and hazards are introduced into the system by untrustworthy third-party authentication.
  3. **Challenges in Transactions:**
     - A lack of trust between parties as a result of the widespread presence of counterfeits.
     - Slow and expensive transaction procedures including the use of outside authentication services.
  4. **Blockchain as a Solution:**
     - A transparent and decentralized authentication system is provided by blockchain technology.
     - The blockchain's immutable transactions offer a safe, unchangeable record of the ownership and usage of a product.
  5. **Benefits of Blockchain (Why we are using Blockchain):**
     - Blockchain is a distributed ledger that runs on a peer-to-peer network and is decentralized. This lessens the dependency on third-party authentication services by doing away with the necessity for a central

authority or middleman. Because transactions are validated by a network of nodes rather than a single central authority, the decentralized character of blockchain increases user confidence in the system.

- Data that has been recorded into the blockchain cannot be changed or tampered with beyond that point. The integrity of the data pertaining to product authentication is guaranteed by this functionality. Due to blockchain's transparency, every user on the network can see the complete history of transactions, making the record transparent and auditable.
- Blockchain secures transactions via cryptographic methods. Every member of the network possesses a set of public and private keys, and all transactions are signed cryptographically. As a result, the system is more secure and impervious to fraud and illegal access.
- The transparency and immutability of blockchain technology make it especially useful for identifying fake goods. Users can confirm the validity of a product by cross-referencing its unique identifier with the blockchain records, as each authentic product's details are recorded on the blockchain. This contributes to the decrease in the market's prevalence of fake items.
- Blockchain can help lower costs and improve operational efficiency by doing away with the requirement for centralized authentication services and streamlining procedures through smart contracts. Direct transactions between users and owners can cut down on related costs and delays.

REQUIREMENT ANALYSIS

- **Context Diagram**: The "AuthDApp" serves as the core, encompassing both the "Owner Section" and the "User Section." Here's a simple context diagram for this project:

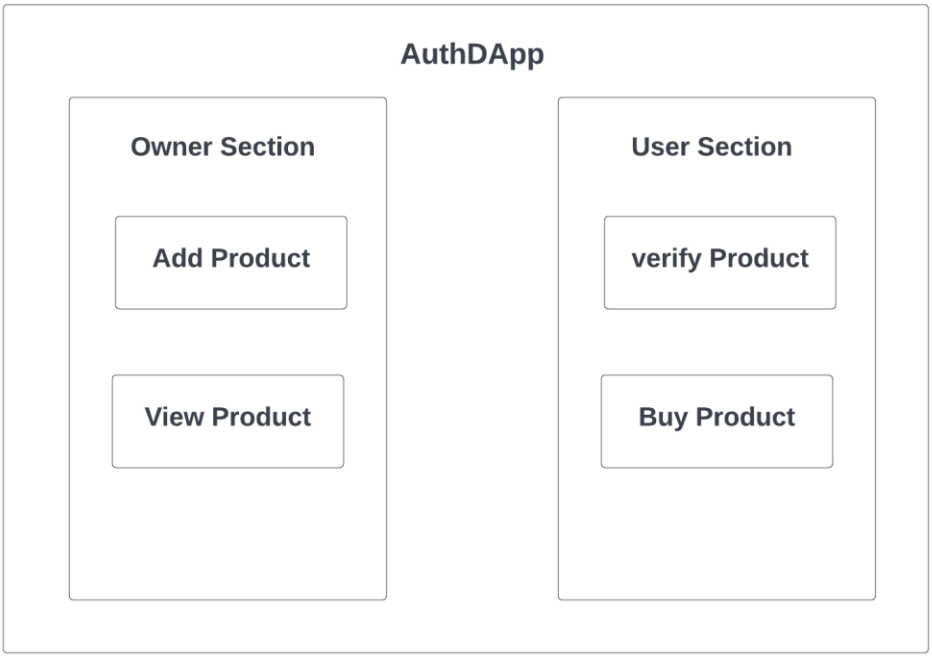


Fig 1: Context Diagram

- **The Hardware used:** While developing the system, the used hardware are:
  1. 11th Gen Intel(R) Core (TM) i5-1135G7 @ 2.40GHz   2.40 GHz
  2. 8 GB of RAM.
  3. intel iris xe graphics 4 GB

- **The Software used:**
  1. Microsoft Windows 11
  2. Visual studio code
  3. React.JS 17.0.1 as Front-end.
  4. Ganache 2.7.1 for local blockchain.
  5. MetaMask for transaction.
  6. Truffle for building decentralized applications (dapps) on the blockchain.
  7. Solidity is used for writing smart contracts on the blockchain.
  8. MS Word for documentation.

- **Packages used:**
  1. Web3(v3.0.3)
  2. bootstrap(v4.5.3)
  3. formik(v2.2.5)
  4. jquery(v3.5.1)
  5. keccak256(v1.0.2)
  6. react(v17.0.1)
  7. react-bootstrap(v1.4.0)
  8. react-dom(v17.0.1)
  9. react-icons(v4.1.0)
  10. react-router-dom(v5.2.0)
  11. react-scripts(v4.0.1)
  12. react-transition-group(v4.4.1)
  13. recoil(v0.1.2)
  14. web3(v1.3.3)
  15. yup(v0.31.0)
  16. @openzeppelin/contracts(v3.4.0)
  17. @openzeppelin/gsn-helpers(v0.2.4)
  18. dotenv(v8.2.0)
  19. eslint(v7.14.0)
  20. tabookey-gasless(v0.4.5)
  21. truffle-hdwallet-provider(v1.0.17)

SYSTEM DESIGN & ARCHITECTURE

➢ System Overview

Our system has some key components, and now we discuss those components.

- **Owner Prospect**
  First, the Owner has to log in to our website using their MetaMask account. If the owner doesn't have an account at MetaMask then they will have to create an account to log in. (We are constraining the login through MetaMask account only to ensure the authenticity of the account and better security).

  There exist two sections under the owner's prospect.

  - **Add Product Section:**
    In this section, owners can add their authenticated products along with other essential details (The owner has to provide a unique product Id for each of their products).
  - **Product List Section:**
    In this section, owners can see their registered products along with the details in a list format.

- **User/Customer Prospect**
  The user has to log into the system through a MetaMask account using a valid user ID and password.
  There exist two sections under the User's Prospect.
  - **Verify Section:**
    In this section, the user can verify if a product is actually an authenticated one rightfully registered by its owner or just a counterfeit. The user will use the unique ID of the product to check this.
  - **Buy Section:**
    After checking the product's authenticity user can buy the product in this section using the same unique ID of the product.

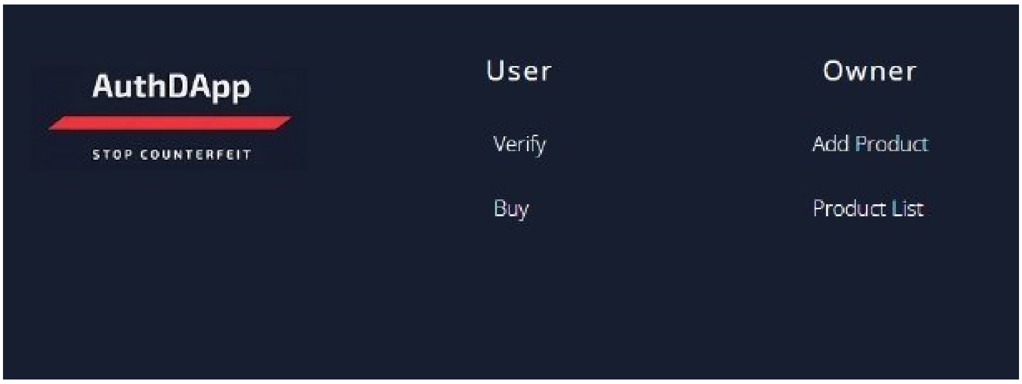


Fig 2: Sections under User and Owner

- **Blockchain Module**
  This module, which makes data transfer on the blockchain easier, is one of the most important parts of our project.

  The technology immediately establishes a link to the blockchain when the owner logs in by logging into their MetaMask wallet. This module contacts the smart contract after the product information is submitted. Upon execution, the smart contract successfully registers the product on the blockchain and debits the wallet for transaction fees.

  On the other hand, a user can connect their MetaMask wallet when they open the web interface. Since the user's account legitimacy was confirmed when they created their MetaMask account, their personal information is not needed again. This module invokes the smart contract when users connect their MetaMask wallet and log in. After the smart contract has been executed, the purchased product is successfully registered on the blockchain and a transaction fee is taken out of the customer's wallet. Since the user has already purchased the product, it is simultaneously deleted from the product list.

➢ Algorithm & Procedure

Here, we are using Keccak-256 (the hashing algorithm of Ethereum). Ethereum is the only application that uses Keccak-256. It is evident that hashing techniques are not limited to central systems. The blockchain is a type of decentralized system that makes use of hashing methods. This is required because, like any other central server or computer, sensitive data is held on the blockchain.

Everybody might view the data if it were stored in raw form on a blockchain. This would imply that the data is not entirely safe in storage. It is preferable to save data encrypted instead, as this will show you a hash. This hash does not provide any information about the appearance of the content. This hash is consequently useless to you as an outsider.

- **Keccak-256: the hashing algorithm of Ethereum**
  The hashing method used by the Ethereum blockchain is Keccak-256. Ethereum's Ethash engine specifically utilizes Keccak-256. Solidity, the programming language used by developers on the Ethereum blockchain, is where it all began. A hash function in this programming language must encode the input data. To encode all "contract calls"—that is, calls that invoke a smart contract—to the EVM, this is required. The Ethereum Virtual Machine, or EVM, is the platform on which programmers create decentralized apps or dApps.
- **Digital Signature**
  It uses public-key cryptography to provide integrity, nonrepudiation (obligation of the message sent and received by the parties), and authenticity of a message and its source. Public key cryptography or asymmetric cryptography uses a key which is a combination of public and private keys. The private key is saved only by the owner while the public key is distributed to the other user.

  On the blockchain, transactions are executed and signed using digital signatures. Keccak-256 is utilized to secure the properties of digital signature. As a result, the algorithm is crucial to the way transactions are carried out.

- **The Blockchain**

  A block is made up of several different transactions. The Ethereum network's validators have certified these transactions. After that, the transactions are combined and hashed. To do this, Keccak-256 is used.

  The previous block's hash is initially appended to the current block before that takes place. The new block isn't turned into a hash until then. The content of the block determines the hash's appearance. The hash of a block will alter in the event that a hacker or criminal attempts to alter the blockchain's history. The hashes of every block that is added after that will all alter. It is obvious that the chain has broken.

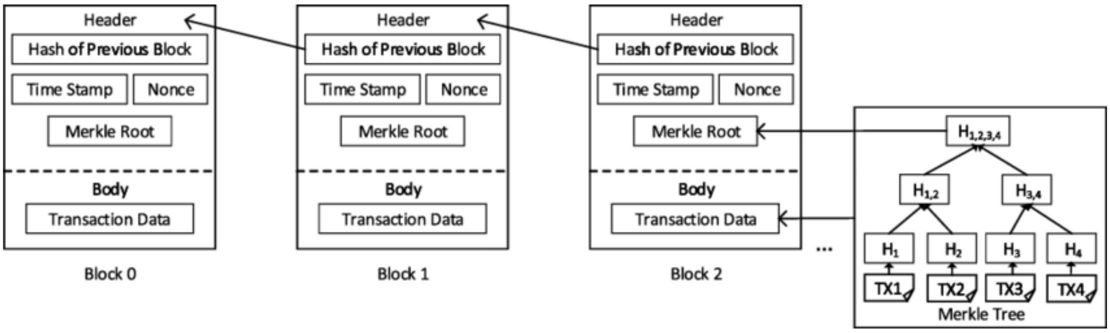


Fig 3: Blocks in Blockchain

- **Smart contract**

  Smart contracts are self-running, independent computer programs that run in response to conditions specified by the author. Blockchain technology can be used by these contracts to facilitate, enforce, and carry out agreements between two parties. Smart contracts, in contrast to traditional contracts, which necessitate the involvement of a third party, allow autonomous commerce between anonymous parties at a lower cost.

- **Merkle Trees**

  Merkle trees are data structures that are used to effectively demonstrate the presence or absence of a certain piece of data within a bigger dataset. Keccak-256 is employed in their construction. Blockchain data architectures frequently use Merkle trees to guarantee the chain's integrity.

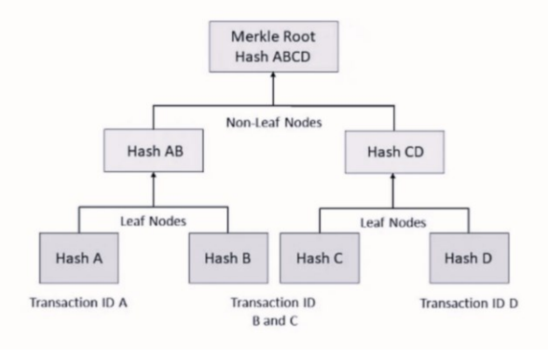


Fig 4: Merkle tree

Implementation

- **Home Page:** This is the Home page of our system.

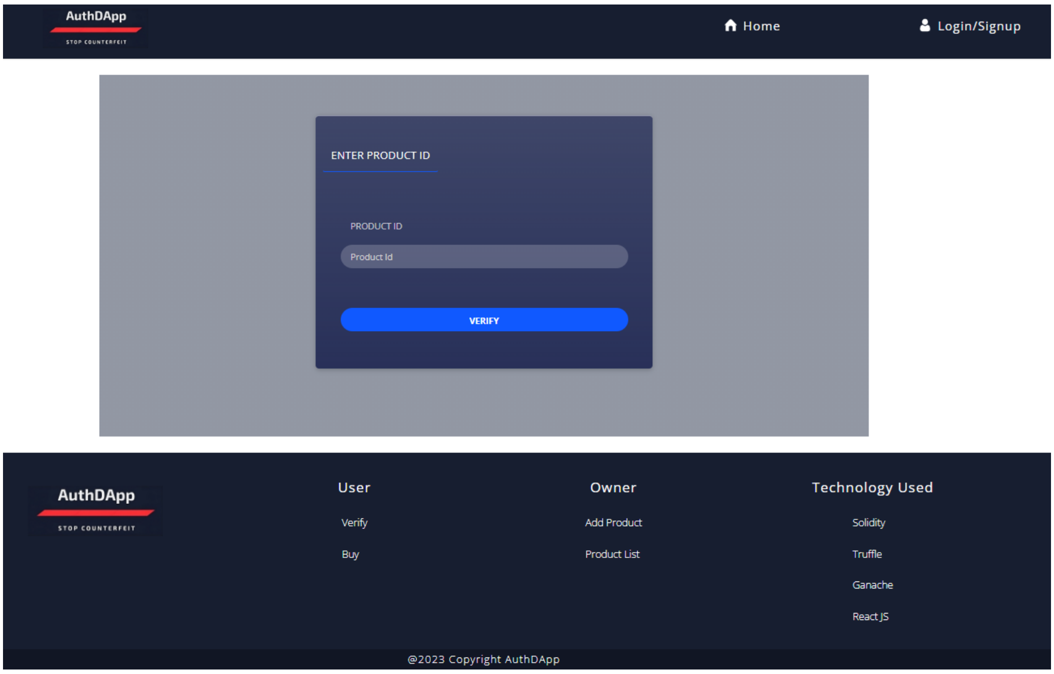


Fig 5: Home Page

- **Add Product Page:** This page is initiated to add products. The owner can add a product by giving details like Product name, price, and product ID.

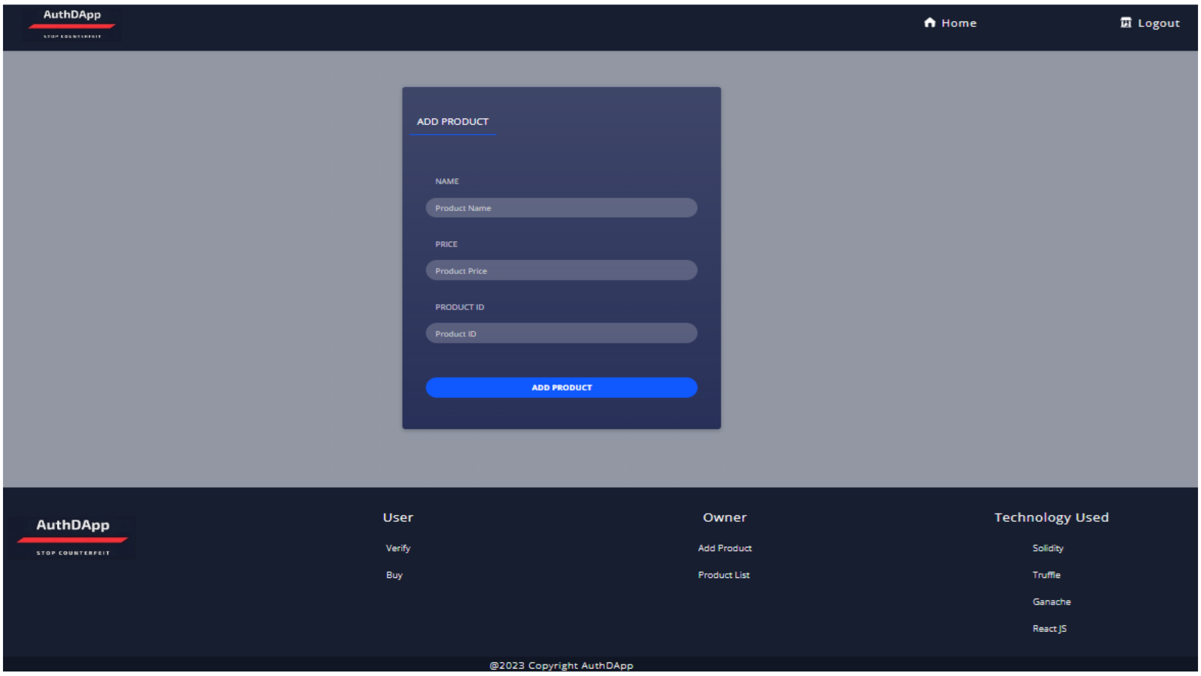


Fig 6: Add Product Page

- **Product Buy Page:** This page is initiated to buy the products through their unique product ID.

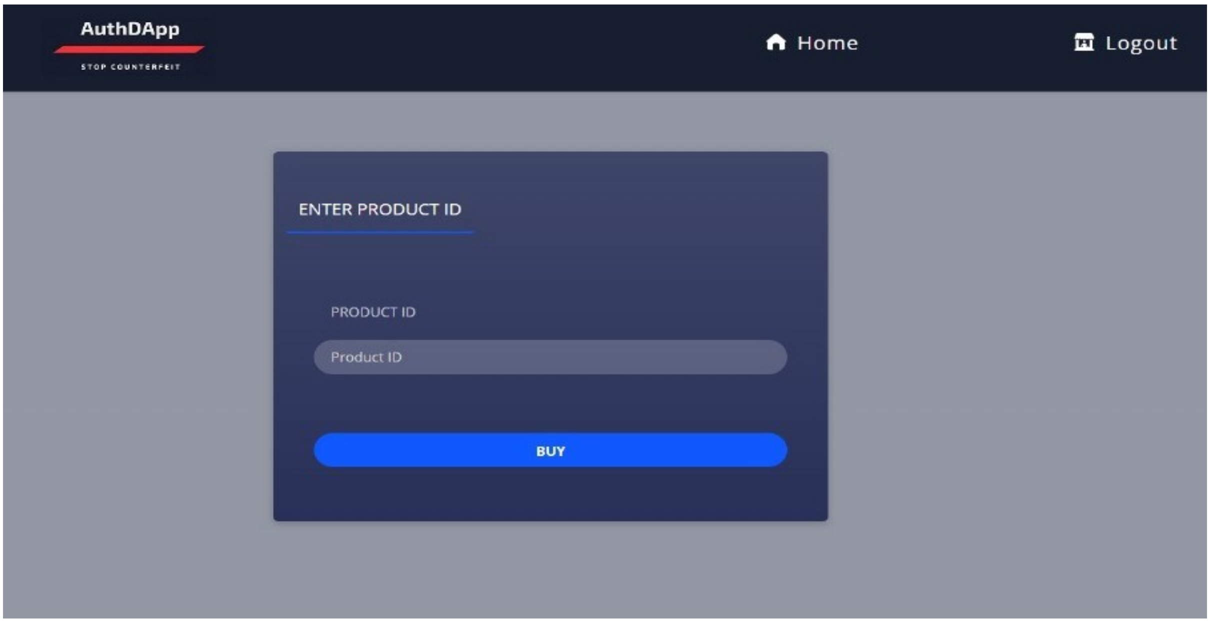
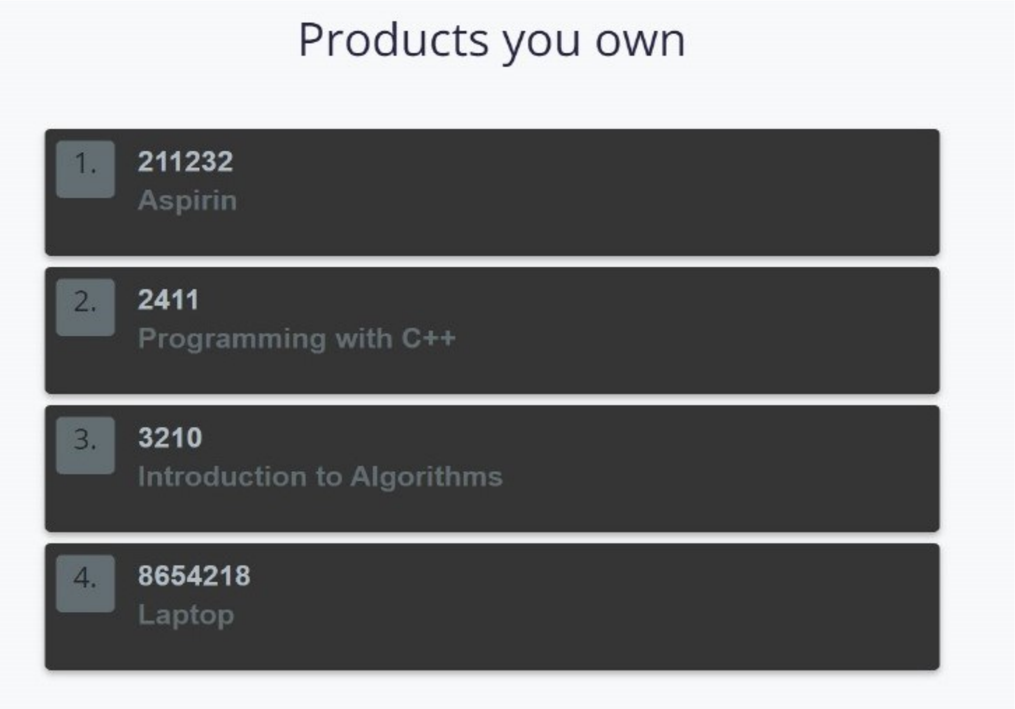


Fig 7: Product Buy Page

- **Product List:** In this section all the added products are viewed in a list format.



Products you own

1. 211232
Aspirin

2. 2411
Programming with C++

3. 3210
Introduction to Algorithms

4. 8654218
Laptop

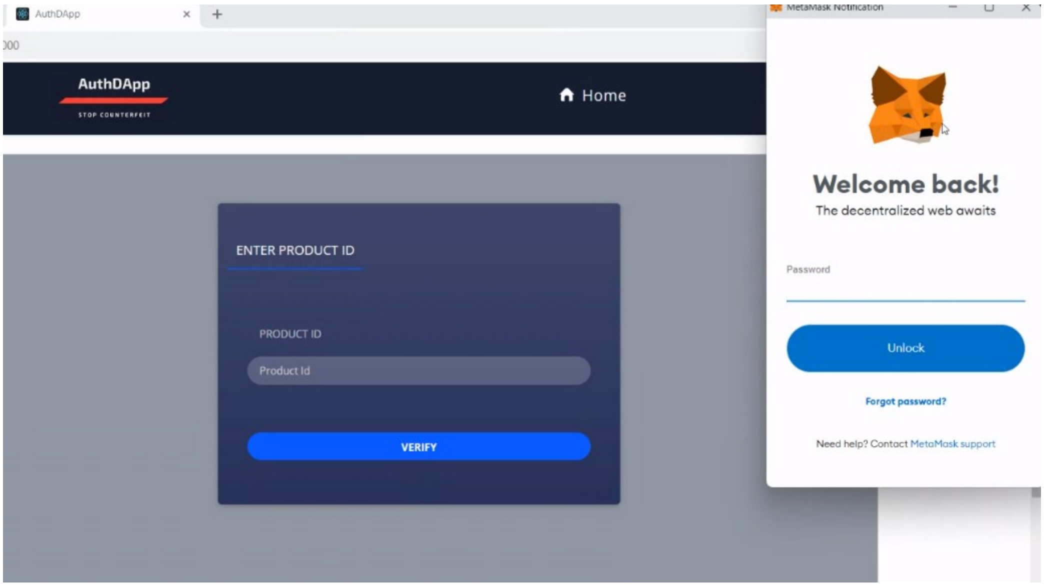
Fig 8: Products List

SOURCE CODE

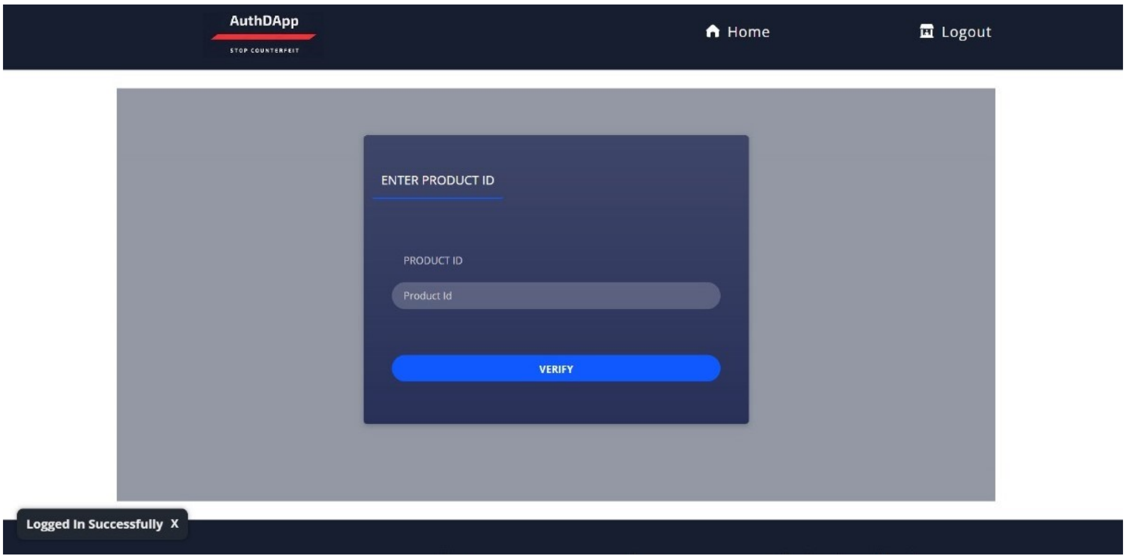
https://github.com/SudipaPiku/AuthDApp.git

RESULT

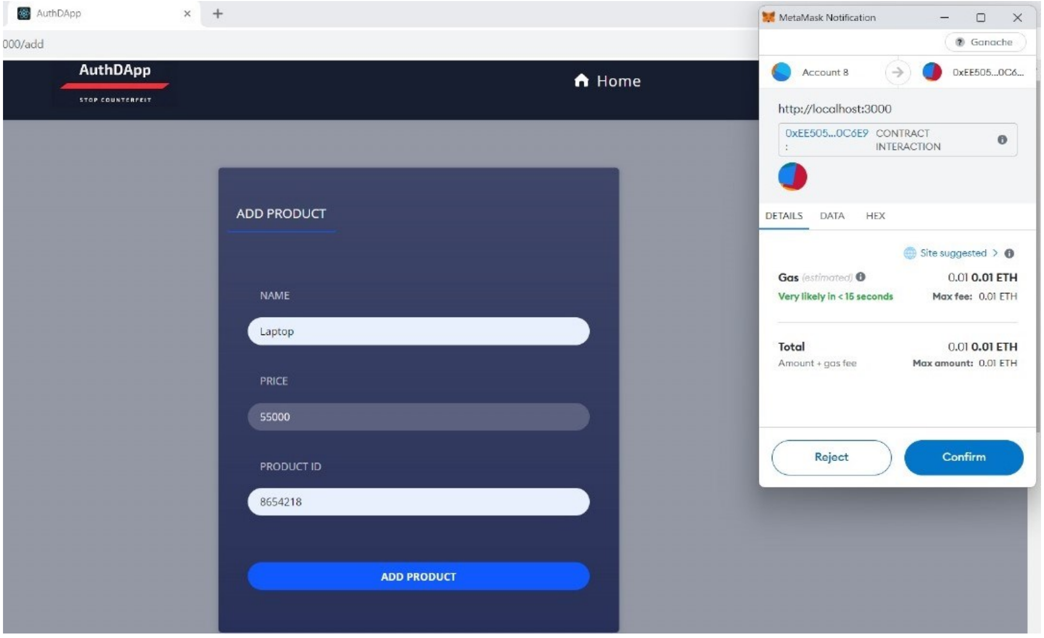
- When the owner/user clicks on the **login/sign up** button, the MetaMask will automatically pops up. Then the owner/user has to enter their password and log in to the system. (If an owner/user does not have a MetaMask account they have to create one.)



- When a valid MetaMask account will log in then a pop-up message will show ‘Logged in successfully’



- When a product is added by the owner MetaMask transaction will be shown as below. (When a product will be added a minimum transaction fee will be needed)



Account 8 → 0xEE505...0C6...

http://localhost:3000

0xEE505...0C6E9 : CONTRACT INTERACTION

Site suggested >

Gas (estimated) 0.01 **0.01 ETH**

Very likely in < 15 seconds Max fee: 0.01 ETH

Total 0.01 **0.01 ETH**

Amount + gas fee Max amount: 0.01 ETH

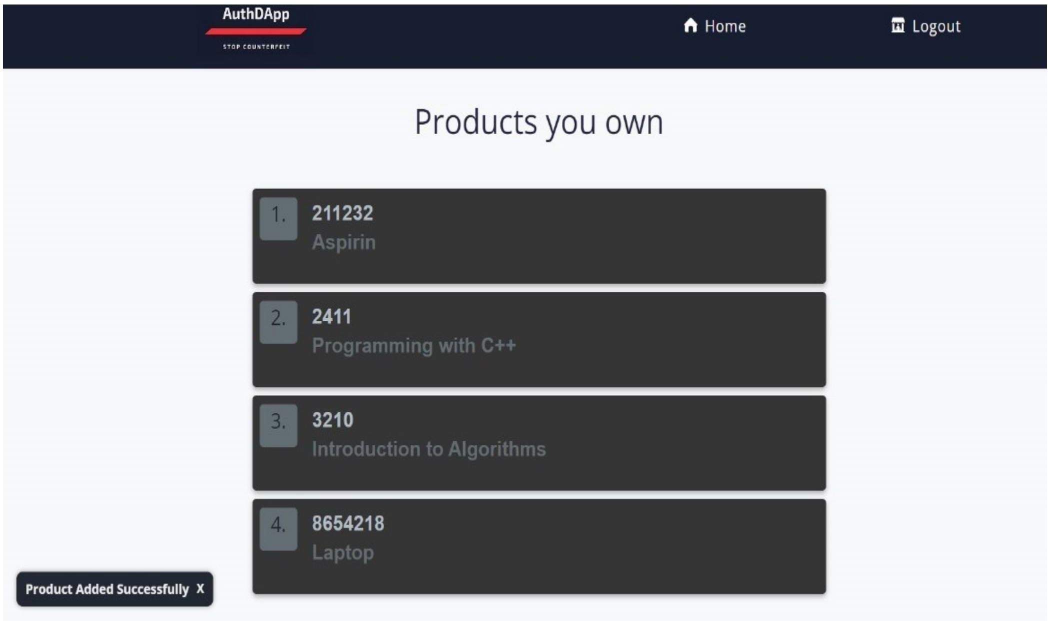
ADD PRODUCT

NAME: Laptop

PRICE: 55000

PRODUCT ID: 8654218

- When a product is registered, the registered product list will be opened automatically, and a pop-up message will appear as ‘product added successfully’

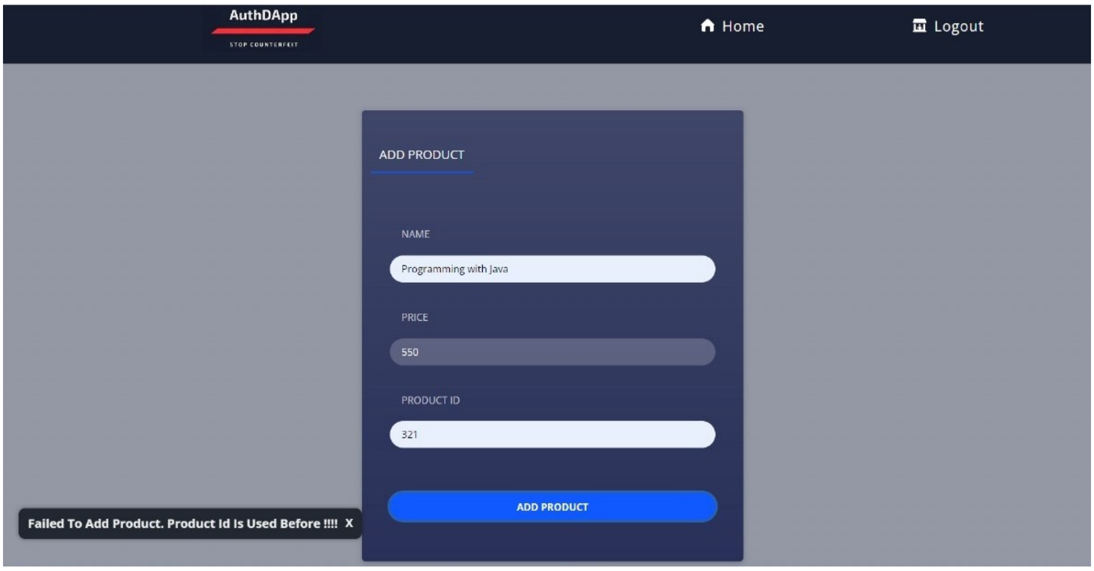


Products you own

1. 211232 Aspirin
2. 2411 Programming with C++
3. 3210 Introduction to Algorithms
4. 8654218 Laptop

Product Added Successfully X

- If an owner tries to add a different product with same product ID then an error message will be shown as ‘Failed to add product. Product ID used before..’



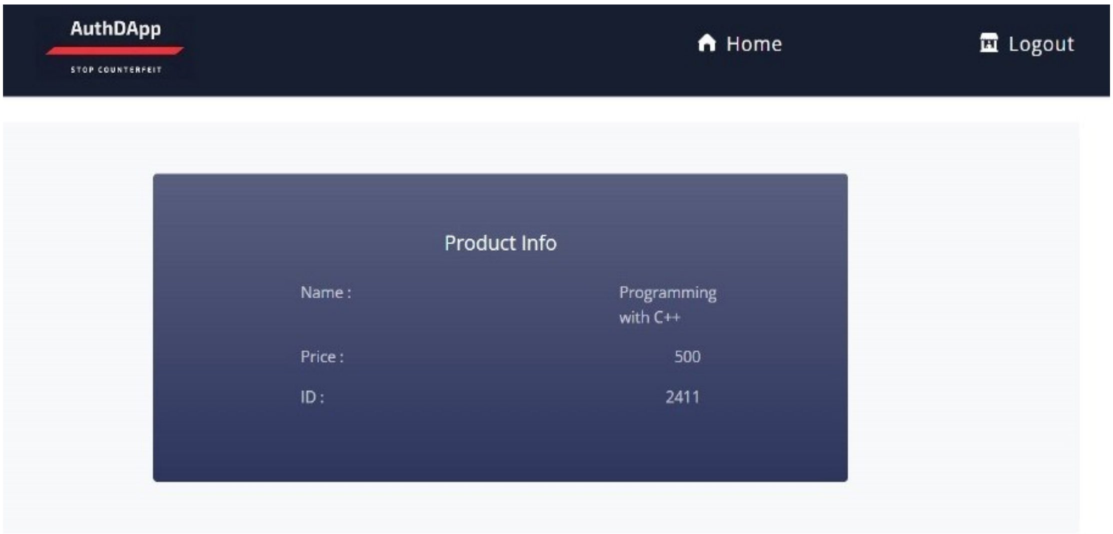
Programming with Java

550

321

Failed To Add Product. Product Id Is Used Before !!!! X

- When a user verifies a product using the product ID they can see the product details.



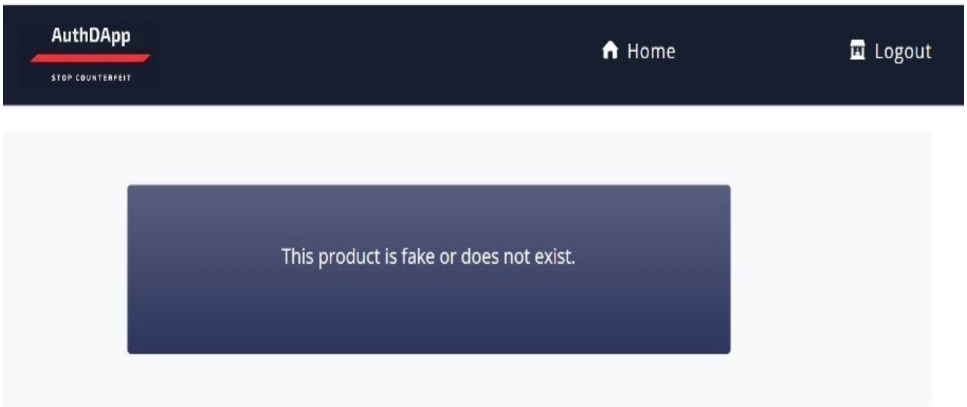
Product Info

Name : Programming with C++

Price : 500

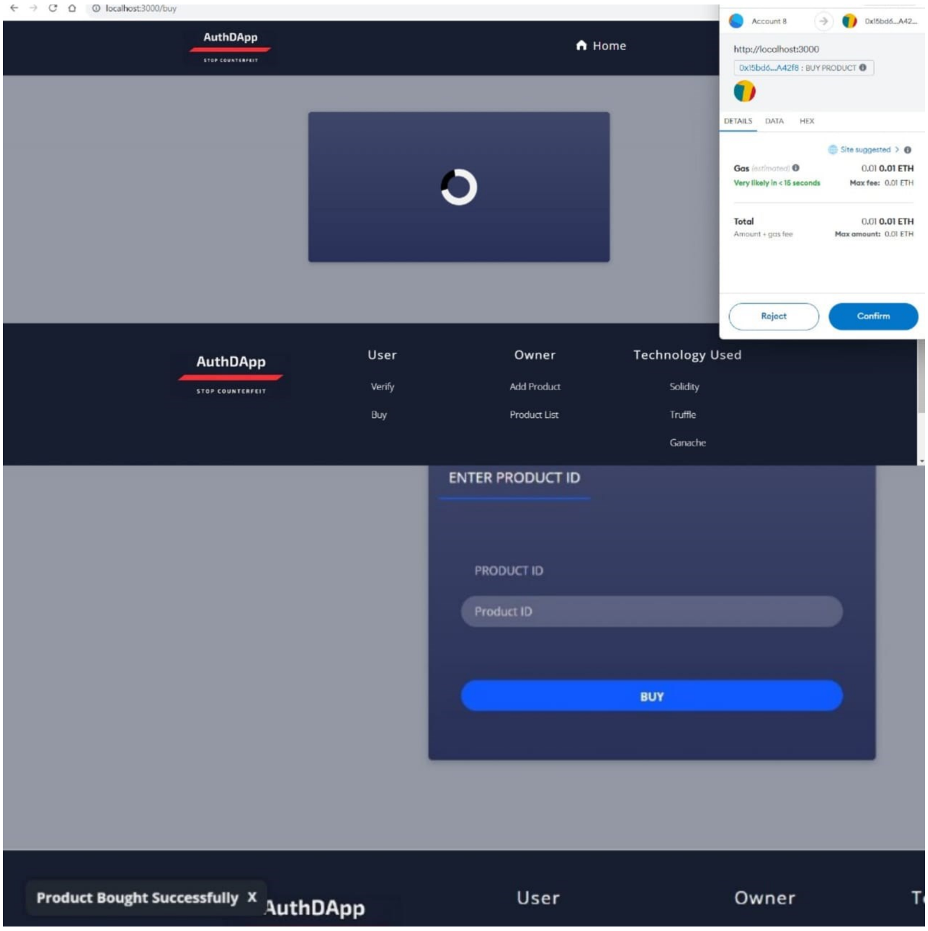
ID : 2411

- When a user tries to verify a product using wrong product ID the message below will appear.



This product is fake or does not exist.

- When a user buys a product the transaction will be shown at the side. After that, a pop-up message will appear as ‘Product bought successfully,



Account 8 → 0x15bd6...A42...

http://localhost:3000

0x15bd6...A42f8 : BUY PRODUCT

Site suggested >

Gas (estimated) 0.01 **0.01 ETH**

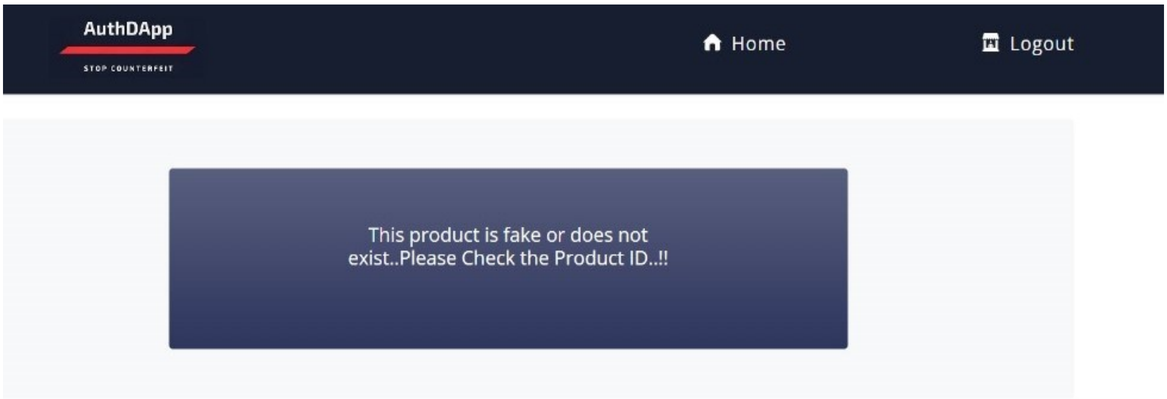
Very likely in < 15 seconds Max fee: 0.01 ETH

Total 0.01 **0.01 ETH**

Amount + gas fee Max amount: 0.01 ETH

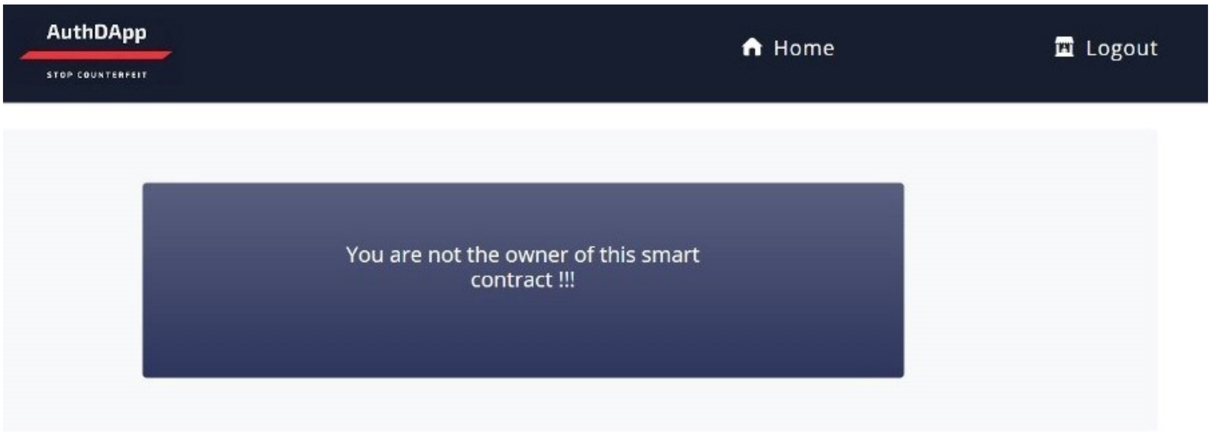
Product Bought Successfully X

- When a user tries to buy a product with the wrong product ID, the message below will be shown.



This product is fake or does not exist..Please Check the Product ID..!!

- If someone tries to add a product with another account where the smart contract is not deployed then the message below will appear.



You are not the owner of this smart contract !!!

LIMITATIONS AND CONSIDERATIONS

While this project has advanced to significant phases of implementation, a thorough comprehension requires admitting certain restrictions and limitations.

- **Integration Challenges**
  Throughout the project, blockchain technology was successfully integrated with current systems. It's crucial to remember, nevertheless, that companies utilizing outdated systems could encounter more complex integration-related difficulties.
- **Scalability**
  The project has shown to be functioning under controlled circumstances. In real-world scenarios with numerous transactions, scalability remains a challenge. Exploring optimization strategies and keeping an eye on performance are critical for sustained success.
- **Costs**
  It is critical to assess deployment and maintenance costs for the blockchain infrastructure in detail.
- **User Adoption**
  Initiatives are required to inform customers and businesses about the benefits and uses of the blockchain-based authentication system in order to overcome potential resistance to change.
- **Smart Contract vulnerabilities**
  Security for smart contracts is essential. The code for smart contracts must be updated, audited, and continuously monitored in order to minimize vulnerabilities that hostile actors can exploit.
- **Security vulnerabilities**
  The project has security measures in place to guard against threats and unauthorized access. However, it's critical to understand that the subject of cybersecurity is ever-evolving and that new threats could materialize at any time.
- **Local Blockchain Infrastructure limitation**
  The project uses a local or private blockchain infrastructure, which can differ greatly from public blockchain networks. While local blockchains offer advantages like increased control and privacy, they also have a lot of disadvantages. Compared to public blockchains, which benefit from a wide node spread, local blockchains could have a more focused structure. This could make single points of failure in the system more likely. The effectiveness of the system can be hampered by local blockchains' constrained network effect. Gaining additional users may not always be easy to achieve, and working with other systems and collaborating with them may take more effort.

FUTURE SCOPE

There are numerous opportunities for improvement and innovation when considering our project's potential in the future. Above all, integrating with state-of-the-art technology like artificial intelligence (AI) and Internet of Things (IoT) gadgets is a potential path. The real-time monitoring and data collection capabilities might be greatly enhanced by this combination, strengthening the resilience of our blockchain-based authentication system.

Enhancing the end user's experience with the blockchain authentication system is another direction for future improvement. Investing in user experience research and design could lead to the creation of mobile apps, dashboards, and user-friendly interfaces that improve consumer happiness and adoption.

Investigating interoperability solutions to connect our local blockchain with other blockchain networks is also a strategic consideration. This could enable collaboration with external parties, increasing the network effect and overall efficacy of the product authentication system.

By introducing self-executing contracts with increasingly sophisticated logic, smart contracts may advance. This innovation has the potential to enhance and automate the authentication process by including additional features to meet evolving market demands.

Concerns about cybersecurity continue to be essential for the project's future scope. Reinforcing the system against potential vulnerabilities requires regular penetration testing, investment in state-of-the-art security technology, and continuous monitoring of the latest advances in cybersecurity threats and the installation of sophisticated encryption methods.

At a later stage of the project's development, we are considering adding a "Seller Section." Owners would be able to sell goods to sellers, who could then resell them to customers, thanks to this new area. By entering the product ID in the verification box, users can view seller data. For every product the owner adds, a distinct QR code would be generated in order to expedite the purchasing and authentication procedure. Customers would have a safe and practical way to buy and confirm the product's legitimacy with this QR code. These improvements are meant to increase the project's usefulness and offer more features to users and owners alike.

CONCLUSION

In order to achieve safe and transparent product authentication, the project "Authentication of Product & Counterfeits Detection Using Blockchain" represents a critical turning point. This program has yielded a number of successes that have given important insights. Recognizing the ever-changing nature of technology and the persistent issues that require care is essential.

This paper presents the successful implementation of a blockchain-based authentication system that creates a strong foundation for identifying and stopping counterfeit goods. The product supply chain can now be more transparent, traceable, and confident thanks to blockchain technology.

As we recognize and appreciate the project's accomplishments, we must also continue to be aware of its shortcomings. Given obstacles like integration problems, scale limitations, costs, data privacy concerns, and regulatory compliance, constant attention and adaptation are crucial.

The project has a great deal of potential for advancement in the field of counterfeit detection in the future. The integration of developing technologies, global expansion, enhanced user experiences, and compatibility with various blockchain networks are all exciting prospects. Industry best practices are aligned with the dedication to ongoing security advancements, cutting-edge smart contract technology, and ecologically conscious procedures.

In conclusion, the Authentication of Product & Counterfeits Detection Using Blockchain project is evidence of how technology may revolutionize the way important issues in supply chains are handled. To guarantee the system's ongoing success, the project team will never waver in their commitment to quality, creativity, and cooperation with stakeholders.

REFERENCES

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

[2] Hyperledger, ―Hyperledger Blockchain 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] G. Wood, Ethereum: A secure decentralised generalized transaction ledger,‘‘ Tech. Rep., 2014.

[5] Smits, M. Blockchain Applications and Institutional Trust. Frontiers in Blockchain.,2020.

[6] 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

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

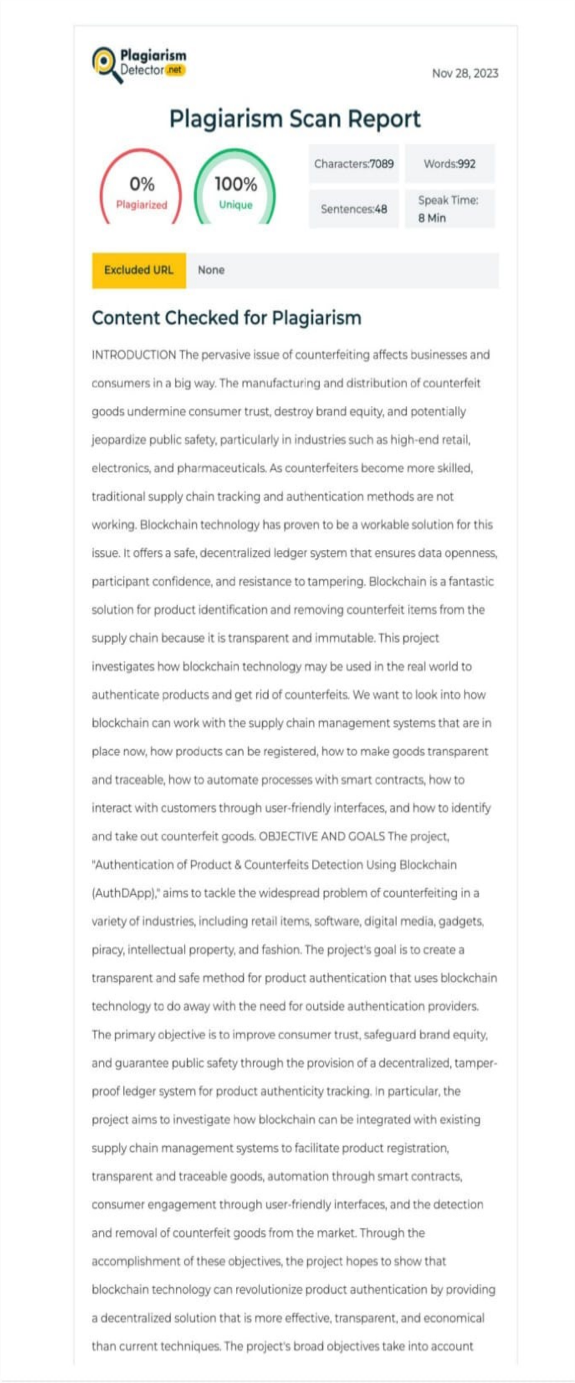
[8] Cachin, "Architecture of the hyperledger blockchain fabric" Tech. Rep., Jul. 2016..

[9] Greenspan, G. *Blockchains vs centralized databases*. Retrieved from MultiChain: http://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/

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

[11] Kumar, R.; Tripathi, R. Secure Healthcare Framework Using Blockchain and Public Key Cryptography. In *Blockchain Cybersecurity, Trust and Privacy*; Springer: Cham, Switzerland, 2020; pp. 185–202.

PLAGIARISM CHECK REPORT



Nov 28, 2023

Plagiarism Scan Report

0% Plagiarized

100% Unique

Characters:7089

Words:992

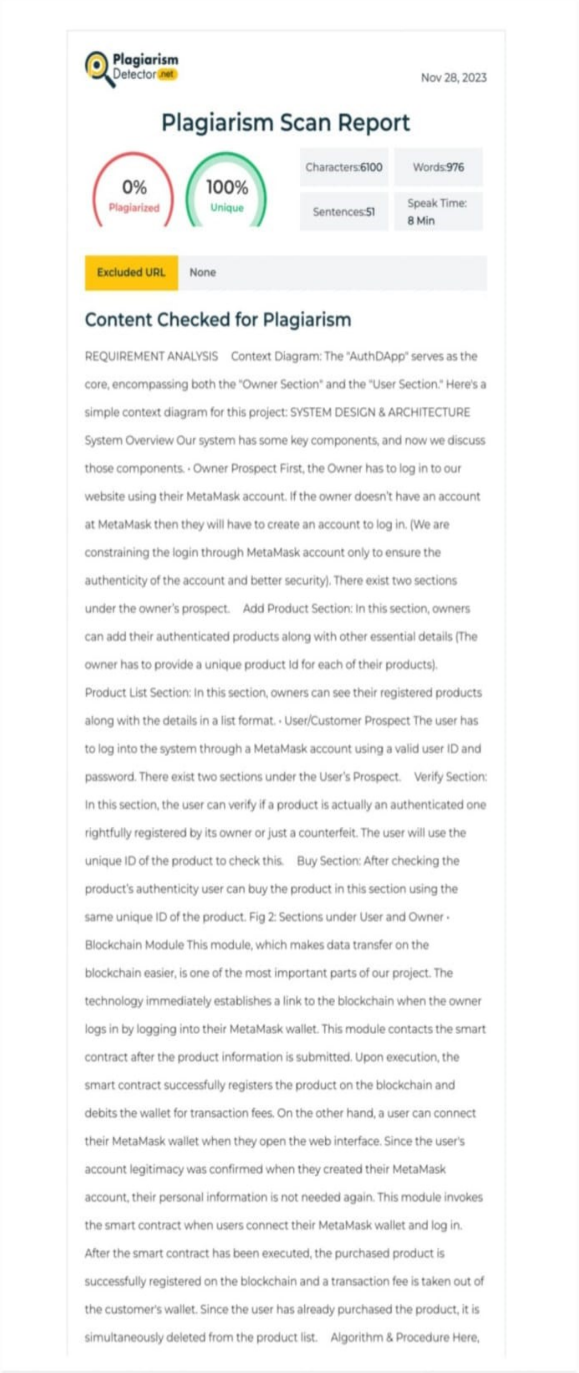
Sentences:48

Speak Time: 8 Min

Excluded URL None

Content Checked for Plagiarism

INTRODUCTION The pervasive issue of counterfeiting affects businesses and consumers in a big way. The manufacturing and distribution of counterfeit goods undermine consumer trust, destroy brand equity, and potentially jeopardize public safety, particularly in industries such as high-end retail, electronics, and pharmaceuticals. As counterfeiters become more skilled, traditional supply chain tracking and authentication methods are not working. Blockchain technology has proven to be a workable solution for this issue. It offers a safe, decentralized ledger system that ensures data openness, participant confidence, and resistance to tampering. Blockchain is a fantastic solution for product identification and removing counterfeit items from the supply chain because it is transparent and immutable. This project investigates how blockchain technology may be used in the real world to authenticate products and get rid of counterfeits. We want to look into how blockchain can work with the supply chain management systems that are in place now, how products can be registered, how to make goods transparent and traceable, how to automate processes with smart contracts, how to interact with customers through user-friendly interfaces, and how to identify and take out counterfeit goods. OBJECTIVE AND GOALS The project, "Authentication of Product & Counterfeits Detection Using Blockchain (AuthDApp)," aims to tackle the widespread problem of counterfeiting in a variety of industries, including retail items, software, digital media, gadgets, piracy, intellectual property, and fashion. The project's goal is to create a transparent and safe method for product authentication that uses blockchain technology to do away with the need for outside authentication providers. The primary objective is to improve consumer trust, safeguard brand equity, and guarantee public safety through the provision of a decentralized, tamper-proof ledger system for product authenticity tracking. In particular, the project aims to investigate how blockchain can be integrated with existing supply chain management systems to facilitate product registration, transparent and traceable goods, automation through smart contracts, consumer engagement through user-friendly interfaces, and the detection and removal of counterfeit goods from the market. Through the accomplishment of these objectives, the project hopes to show that blockchain technology can revolutionize product authentication by providing a decentralized solution that is more effective, transparent, and economical than current techniques. The project's broad objectives take into account



Nov 28, 2023

Plagiarism Scan Report

0% Plagiarized

100% Unique

Characters:6100

Words:976

Sentences:51

Speak Time: 8 Min

Excluded URL None

Content Checked for Plagiarism

REQUIREMENT ANALYSIS Context Diagram: The "AuthDApp" serves as the core, encompassing both the "Owner Section" and the "User Section." Here's a simple context diagram for this project: SYSTEM DESIGN & ARCHITECTURE System Overview Our system has some key components, and now we discuss those components. · Owner Prospect First, the Owner has to log in to our website using their MetaMask account. If the owner doesn't have an account at MetaMask then they will have to create an account to log in. (We are constraining the login through MetaMask account only to ensure the authenticity of the account and better security). There exist two sections under the owner's prospect. Add Product Section: In this section, owners can add their authenticated products along with other essential details (The owner has to provide a unique product Id for each of their products). Product List Section: In this section, owners can see their registered products along with the details in a list format. · User/Customer Prospect The user has to log into the system through a MetaMask account using a valid user ID and password. There exist two sections under the User's Prospect. Verify Section: In this section, the user can verify if a product is actually an authenticated one rightfully registered by its owner or just a counterfeit. The user will use the unique ID of the product to check this. Buy Section: After checking the product's authenticity user can buy the product in this section using the same unique ID of the product. Fig 2: Sections under User and Owner · Blockchain Module This module, which makes data transfer on the blockchain easier, is one of the most important parts of our project. The technology immediately establishes a link to the blockchain when the owner logs in by logging into their MetaMask wallet. This module contacts the smart contract after the product information is submitted. Upon execution, the smart contract successfully registers the product on the blockchain and debits the wallet for transaction fees. On the other hand, a user can connect their MetaMask wallet when they open the web interface. Since the user's account legitimacy was confirmed when they created their MetaMask account, their personal information is not needed again. This module invokes the smart contract when users connect their MetaMask wallet and log in. After the smart contract has been executed, the purchased product is successfully registered on the blockchain and a transaction fee is taken out of the customer's wallet. Since the user has already purchased the product, it is simultaneously deleted from the product list. Algorithm & Procedure Here,