

Ecommerce DApp-A Decentralised Ecommerce Project

Farhan Shikalgar, Farhaan Khan, Saud Kadiri, Anas Khan

¹University of Mumbai ,BE

² University of Mumbai ,BE

³ University of Mumbai ,BE

⁴ University of Mumbai ,BE

Abstract - Improving efficiency and performance is an important topic in the world today. As it is well-known, cooperative computing is an effective and traditional approach, and it is widely used in various fields. Inspired by this idea, take E-commerce for example, Security is one of its important indicators. In E-commerce, the security technology has become a major issue restricting the rapid development and popularization of E-commerce. With the advent of new technologies, Blockchain plays a major role in e-commerce sector. With the characteristics of decentralization, persistency, anonymity and auditability, blockchain technology is a new tool to solve the product traceability, information security and privacy, payment efficiency and cost reduction in cross-border e-business. Existing E-commerce models are trapped in a dilemma between the proof of ownership and privacy protection. To address this issue, We have made a platform Shoppingverse which is a blockchain based ecommerce. We design a privacy-preserving business protocol by employing private smart contracts in the negotiation phase. The protocol allows counterparties make deals without the disclosure of private information such as identities, addresses, and phone numbers. Moreover, we employ the zero-knowledge proof to guarantee the ownership.

Key Words: Ethereum, Blockchain, Ecommerce, Smart Contract.

1. INTRODUCTION (Size 11, Times New roman)

Improving efficiency and performance is an important topic in the world today. As it is wellknown, cooperative computing is an effective and traditional approach, and it is widely used in various fields. Inspired by this idea, take E-commerce, for example; Security is one of its important indicators. In E-commerce, security technology has become a major issue restricting the rapid development and popularization of E-commerce. With the advent of new technologies, Blockchain plays a major role in the e-commerce sector. With the characteristics of decentralization, persistency, anonymity and auditability, blockchain technology is a new tool to solve product traceability, information security and privacy, payment efficiency and cost reduction in cross-border e-business. Existing E-commerce models are trapped in a dilemma between proof of ownership and privacy protection. To address this issue, We have made a platform called Shoppingverse which is Blockchain-based e-commerce. We design a privacy-preserving business protocol by employing smart private contracts in the negotiation phase.

The protocol allows counterparties to make deals without the disclosure of private information such as identities, addresses, and phone numbers. Moreover, we employ zero-knowledge proof to guarantee ownership. It is a completely decentralized electronic currency trading system based on cryptography and distributed network. Blockchain technology underlies Bitcoin, an unstructured peer-to-peer system with its own virtual currency. In 2013, proposed that by combining the smart contract with the Blockchain and starting the Ethereum project, users can build the blockchain system through Turing complete language, create the contract to complete any state transition function, and realize the automation of business processes. In 2015, Melanie Swan first launched LINQ, a trading platform based on block trading technology, which has become an important milestone in the trend of financial securities market decentralization. Now Bitcoin, Ripple, Hyperledger, and other blockchain systems have produced a great impact on the traditional financial industry. Especially blockchain technology is applied in many fields, including financial asset clearing and settlement, which can reduce costs and risks.

The characteristics of decentralization, persistency, anonymity and auditability of blockchain technology, the properties of immutability, transparency and natural settlement, in fact, completely match the demand of the cross-border e-business payment field. Blockchain technology provides a new probability solution to innovate the cross-border e-business payment model, such as using crypto-currency as an intermediary for money exchanging and constructing a decentralization global remittance system with blockchain technology and underlying protocol by integrating global banks.

2. PURPOSE

E-commerce has become more and more popular because of rich products, fast transactions, free time, locations, stores and so on. However, the disclosure of user's personal information, such as 1) identities, 2) addresses, and 3) phone numbers, has become a big concern in online activity. Factually, it has formed a huge "grey industry" that seriously endangers users' safety and privacy. It is not uncommon for sellers to threaten and force customers to make, modify or delete product reviews that are against their will. Meanwhile, online shopping websites are also suffering from malicious bad reviews or spurious praise reviews, which reduce the Quality of Experience (QoE).

3. Project Scope

Blockchain can advance the process of electrification and improve accuracy. Once the bank transactions through their own system, and then paper or other methods to the hands of trading partners, the blockchain system, after the construction of the entire electronic process, ensures the authenticity of the content. The whole process is transparent, and everyone can see the progress of the process and the future arrangement. In addition, each action will also have a system to record it. With the increasing popularity of cryptographic currencies such as Bitcoin, blockchain technology, which is the underlying technology of Bitcoin, has attracted lots of attention. Because of its decentralization, tamper-proof and traceability nature, Blockchain has been applied in many fields, especially in finance and e-payment. In addition, smart contracts further extend the applications of blockchain technology. Recently, the logistics and supply chain management (SCM) communities realize the benefits of Blockchain to the industry.

4. Project Goals And Objectives

We protect users' private information by employing blockchain technologies, including smart private contracts and zero-knowledge proof. Specifically, each trade is represented by a private smart contract, which defines the business logic, types of trade, counterparties, underlying assets, price, and any other relevant information. Private smart contracts are implemented to be a bridge between buyers and sellers during transactions without the disclosure of private information. We employ the zero-knowledge proof to issue shielded tokens and create shielded transactions in order to provide proof of ownership. The tokenized assets and shielded transactions prevent the disclosure of buyers' private information due to the zero-knowledge property of the zero-knowledge proof. The tokenized assets can be cash or other tradable goods. Information about the shielded transaction is confidential during the transaction. This technology has already been implemented in several different industries, including e-commerce. By using blockchain, retailers can ensure that buyers' data is safe and secure from theft or misuse. The blockchain can be used to encrypt customers' data, preventing it from being stolen or corrupted. Blockchain technology can help to secure customer data by creating a tamper-proof ledger of all transactions. This would make it difficult for hackers to steal or manipulate customer information.

The blockchain-based Goals to innovate the e-commerce industry :

- Security of customers' data
- Fraud prevention in the e-commerce system process
- Faster checkout in e-commerce
- Efficient payment system
- System that allows for easier tracking with NFT based Contracts
- Providing a more transparent and efficient system for reviewing customer data
- System that allows for easier returns and refunds

The Objective of the E-commerce Dapp are as follows :

- To provide a protection of users private information.
- To Implement Private smart contracts.
- To be a bridge between buyers and sellers during transactions.

- To develop an E-commerce platform based on blockchain.
- To provide a platform where NFT based Warranties help in smooth role of trade.

5. Organization of Report

This System, "E-commerce Dapp", is all about a Decentralised E-commerce platform. Blockchain is a public ledger that can be used to track the digital movements of assets. It allows buyers and sellers to securely exchange data without worrying about third parties stealing their information. This Report provides an overview of a decentralised e-commerce website. The purpose of this website is to allow individuals and businesses to conduct secure and trust less transactions without the need for intermediaries or centralised authorities. The Report examines the features and benefits of a decentralised e-commerce platform. This Report was made in the years 2022-2023 by students of the University of Mumbai. This Report was Written for the Final year Project of students of B.E. Mumbai University.

5. Project Management Approach

The SDLC RAD model is a combination of the traditional System Development Life Cycle (SDLC) and the Rapid Application Development (RAD) model. It combines the structured approach of SDLC with the rapid prototyping approach of RAD to create a development process that is both efficient and flexible.

The SDLC RAD model typically consists of the following phases:

- Business Modelling/Requirements Planning: This phase involves gathering and analysing user requirements. In this phase, the project manager works closely with the users to identify their needs and expectations. Once the requirements are identified, the project manager creates a plan for the development process.
- Modelling Flow/User Design: The User Design phase involves creating a prototype of the software. The prototype is created with the help of the users, who provide feedback on the design. This phase allows the project manager to identify any design flaws and make necessary changes.
- Construction: The Construction phase involves building the software. In this phase, the project manager uses the prototype created in the User Design phase as a basis for building the software. The software is developed in an iterative manner, with each iteration adding new features or functionality.
- Testing: The Testing phase involves testing the software to ensure that it meets the user requirements and functions as intended. Testing is performed throughout the development process to ensure that defects are identified and fixed in a timely manner.
- Deployment: The Deployment phase involves deploying the software. In this phase, the project manager ensures that the

software is ready for use by the users. This includes testing the software, training the users, and migrating data from old systems to new systems.

6. Software Requirements Specification

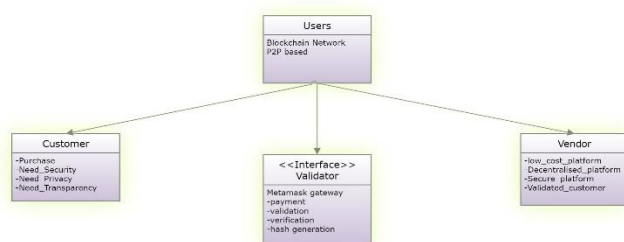
This document outlines the software requirements for a blockchain-based ecommerce platform. The platform will allow buyers and sellers to transact using cryptocurrency and will be built on a blockchain network to ensure transparency, security, and immutability of transactions.

7. Product Features

Product Features	Description
Decentralized Transactions	Blockchain-based e-commerce products offer decentralized transactions, which means that there is no need for a third party like a bank or payment processor to authorize and process transactions. Transactions are verified and recorded on the blockchain, making them more secure and transparent.
Cryptocurrency Payments	Since blockchain-based e-commerce products often use cryptocurrency as their primary payment method, they allow users to make payments without having to worry about the traditional banking system.
Smart Contracts	Smart contracts are self-executing contracts that are stored on the blockchain. They automate the execution of certain actions, such as payments and deliveries, based on predefined rules, which can reduce the need for intermediaries in transactions.
Immutable Records	Blockchain-based e-commerce products offer immutable records of transactions, which means that once a transaction is recorded on the blockchain, it cannot be altered or deleted. This makes transactions more secure and transparent.
Decentralized Marketplaces	Blockchain-based e-commerce products can create decentralized marketplaces that allow buyers and sellers to transact without the need for intermediaries. This can reduce transaction costs and increase efficiency.
NFT Warranties	NFT-based warranties is that the buyer of a product would receive an NFT along with their purchase. This NFT would represent the warranty for the product, and would be stored on the blockchain

8. User Classes and Characteristics

- **Customers:** Customers are the end-users of the e-commerce platform who purchase goods and services. Some characteristics of customers are: They create an account on the platform to make purchases. They can browse products, add them to their cart, and make payments using cryptocurrency or fiat currency. They can track their orders and view their purchase history. They may leave ratings and reviews for products.
- **Vendors:** Vendors are the businesses or individuals who sell goods and services on the ecommerce platform. Some characteristics of vendors are: They must register as a vendor on the platform and provide proof of identity and business registration. They can create product listings, set prices, and manage their inventory. They receive payments for their sales and may need to pay a commission to the platform. They may be subject to customer ratings and reviews.



USER CLASSES AND CHARACTERISTICS

9. System Features

Cryptocurrency payments: The ecommerce platform should allow for payments to be made using cryptocurrencies such as Bitcoin, Ethereum, or other altcoins. This allows for faster and more secure transactions with lower transaction fees.

Identity verification: Since the platform is decentralized, identity verification is important to prevent fraud and ensure that users are who they claim to be. This can be achieved through methods such as digital identity verification, biometric verification, or other forms of identity verification.

User privacy: The ecommerce platform should ensure that user data is kept private and secure. This can be achieved through encryption and other security measures.

Tokenisation of assets: The platform may allow for the tokenisation of assets, which means that assets can be represented as digital tokens on the blockchain. This allows for fractional ownership of assets and can help to increase liquidity. The blockchain smart contract allows users to prove ownership. Provide the purchasing history, warranty period, and other item information. The warranty card includes the item's serial number and buyers wallet address that proves ownership. The NFTs are decaying in nature, in that, after a certain period their use for the redemption of warranty benefits offered by the brand/retailer will expire.

10. Functional Requirements

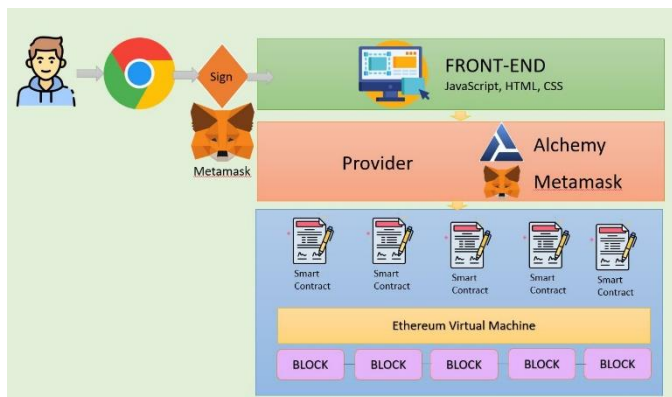
1. **User registration:** The platform should allow users to create accounts and manage their personal information, such as name, email address, and shipping address.
2. **Product catalog:** The platform should allow users to browse and search for products, view product details, and add items to their shopping cart.
3. **User feedback and reviews:** The platform should allow users to leave feedback and reviews about products and sellers, which can help other users make informed purchase decisions.
4. **Integration with third-party tools:** The platform should be able to integrate with thirdparty tools and services. Here we used Metamask

11. Non-Functional Requirement

1. **Scalability:** The platform should be able to handle a large volume of transactions and users, without compromising performance or security.
2. **Usability:** The platform should be easy to use, with intuitive navigation and clear instructions, to ensure that users can complete tasks quickly and efficiently.
3. **Reliability:** The platform should be highly reliable, with minimal errors or failures, to ensure that users can complete transactions and access their data at all times.

4. Extensibility: The platform should be easily extensible, allowing for the addition of new features and functionalities, to adapt to changing user needs.

12. System Architecture Design



13. Sub-system development

Module1-Login

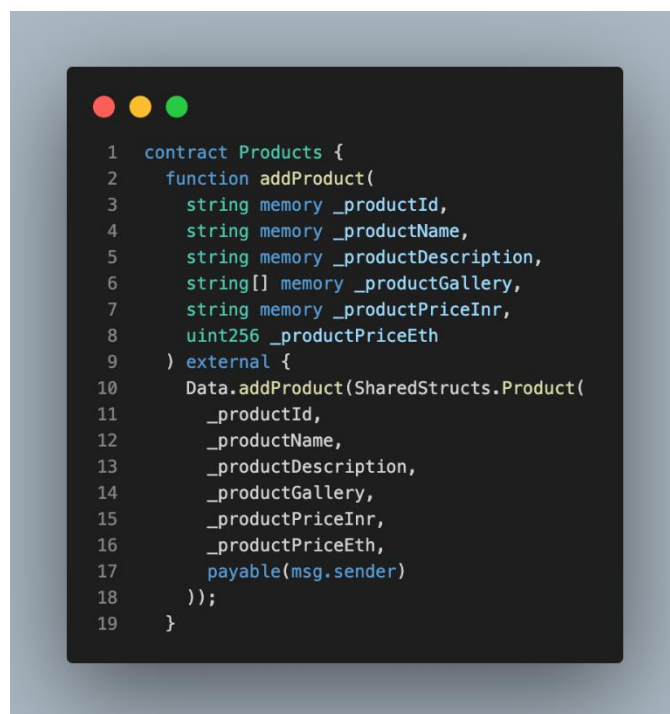
Create a Metamask account, A user would need to create an account on the Metamask platform. The user would enter their personal information, such as their name, email address, and a password. Smart contracts can be used to enforce access control rules. For example, a smart contract can be used to check if a user has the necessary authorization to perform a certain action, such as adding a new product or processing a payment.



Module2-Add Product

The product description should include the name of the product, a detailed description, and any additional information such as specifications or features. This information will help buyers make informed decisions about the product. Upload clear and high-quality images of the product to help buyers visualize the product before making a purchase. A smart contract is a self-executing contract that automatically executes when certain conditions are met. Create a smart contract that contains the product details, price, and the unique identifier. Once the smart contract is deployed, the product will be available for purchase

on the blockchain ecommerce platform. Buyers can purchase the product using cryptocurrency, and the smart contract will automatically execute, transferring ownership of the product to the buyer.

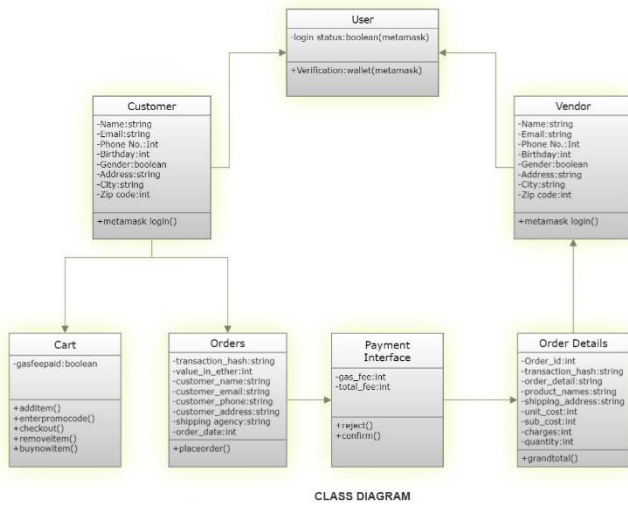


Module3-NFT Warranty

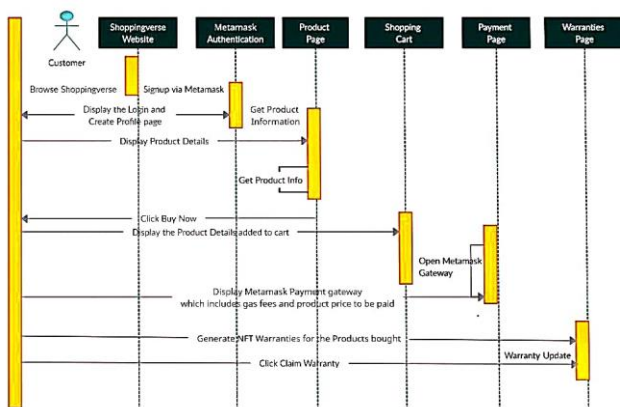
When a buyer purchases an NFT, the smart contract should automatically validate the warranty based on the terms and conditions defined in the smart contract. If the NFT fails to meet the warranty terms and conditions, the smart contract can be used to enforce the warranty. For example, if the NFT is damaged or lost during shipping, the smart contract can be used to refund the buyer or replace the NFT. If warranty claims should be recorded on the blockchain to provide an immutable record of the transaction.



14. CClass Diagram



15. Sequence Diagram



16. Implementation

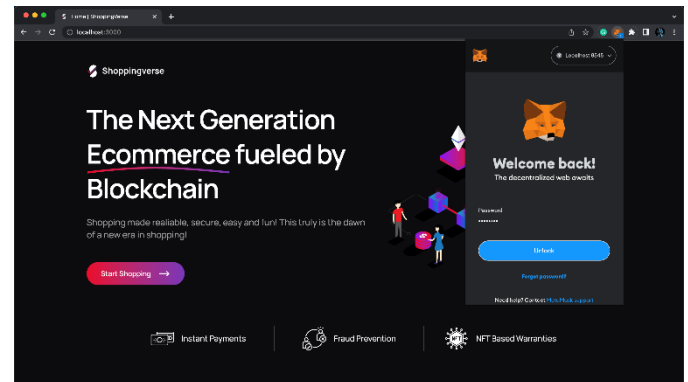
1. Determine what products to offer on the blockchain ecommerce platform. identify the type of blockchain you need and the features you require.
2. Choose a blockchain platform that is Ethereum, Hyperledger, and EOS are some popular blockchain platforms for ecommerce.
3. Develop smart contracts, Smart contracts are self-executing contracts that automatically execute when certain conditions are met. Develop smart contracts that will manage the transactions between buyers and sellers, including payments, order processing, and dispute resolution.
4. Develop a user interface, Develop a user interface that enables buyers to browse products, place orders, and make payments. The user interface should be user-friendly and easy to navigate.
5. Implement payment gateway(Metamask): Implement Metamask that supports cryptocurrency payments. The payment gateway should integrate with the blockchain platform and the smart contracts.

6. Test the system thoroughly to ensure that it is functioning correctly. Test the smart contracts, payment gateway, and user interface to identify and fix any issues.

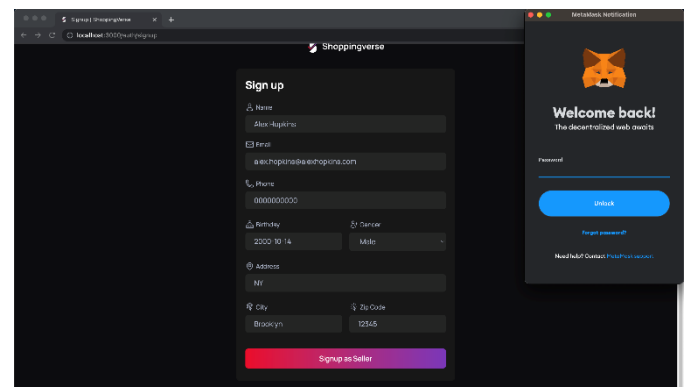
7. Launch the platform

17. System testing

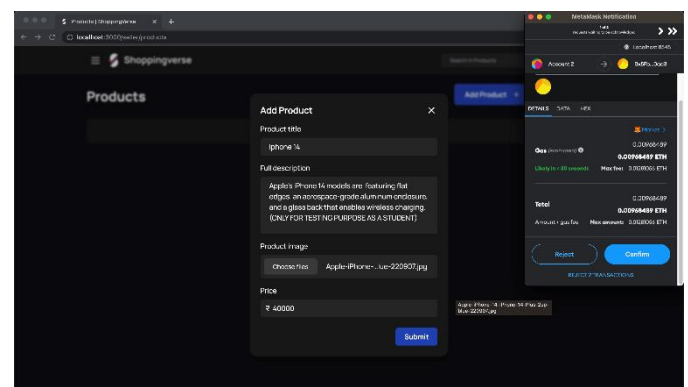
1)Authentication: Test the authentication process to ensure that users can access their accounts securely and that their personal data is protected.



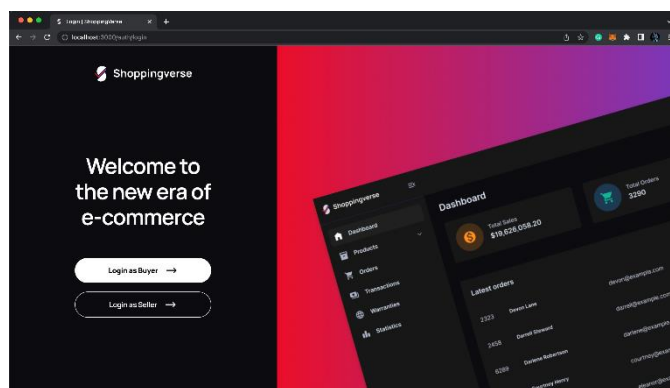
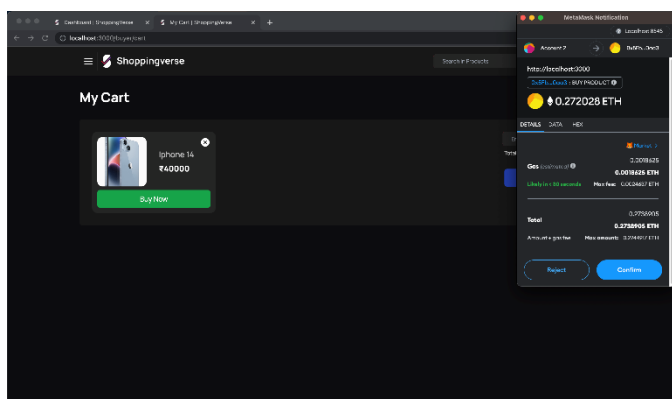
2)Login: Test the login process to ensure that users can access their accounts securely and that their personal data is protected.



3)Product listing: Test the product listing process to ensure that products are displayed correctly



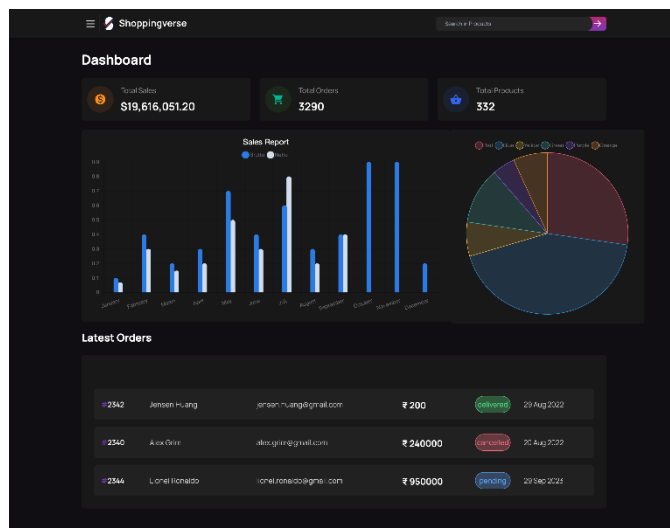
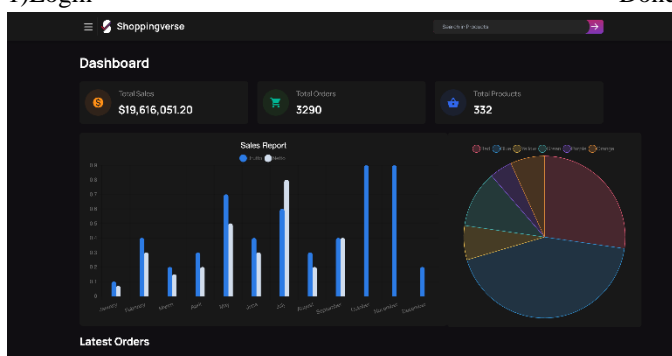
4)Product buying: Test the product buying process to ensure that products are displayed correctly



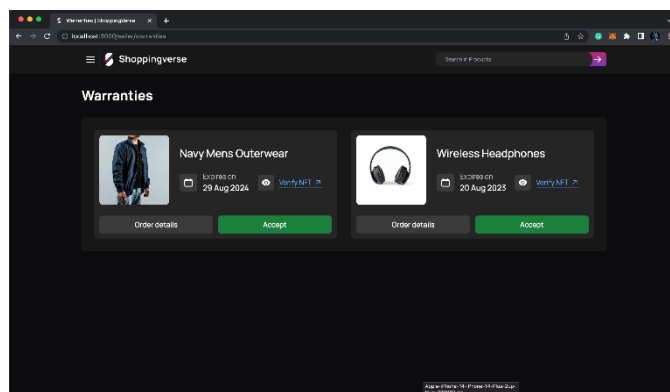
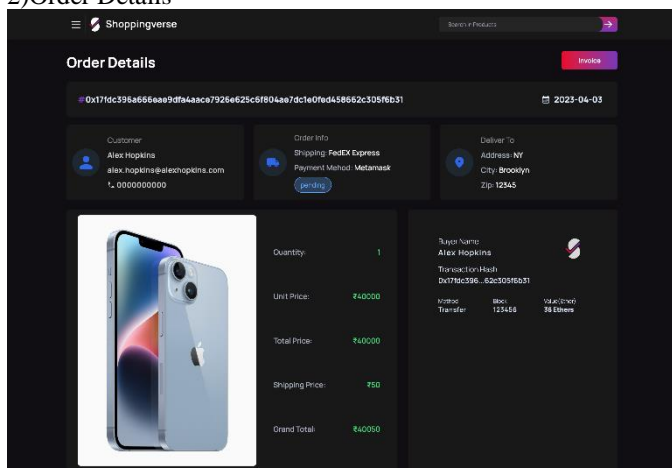
RESULT:

1)Login

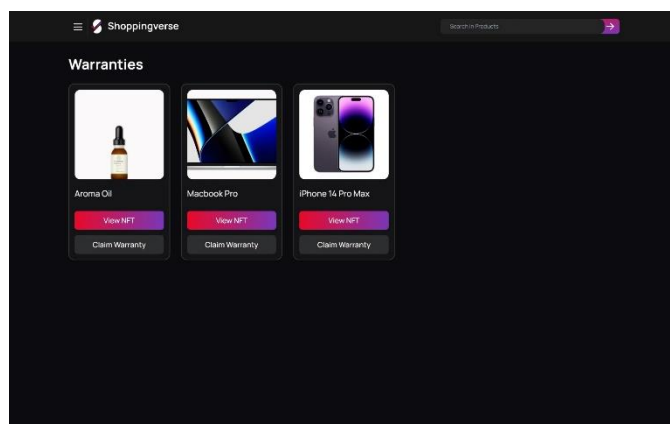
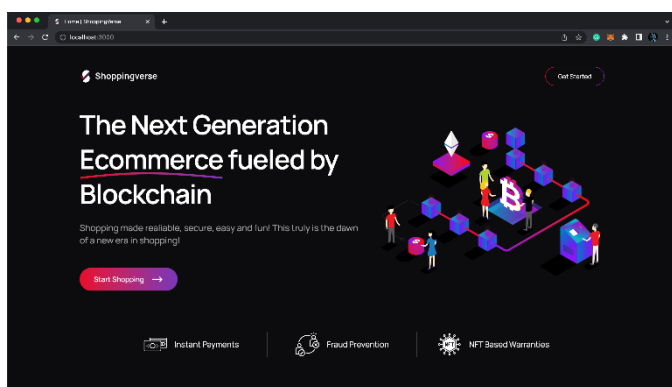
Done

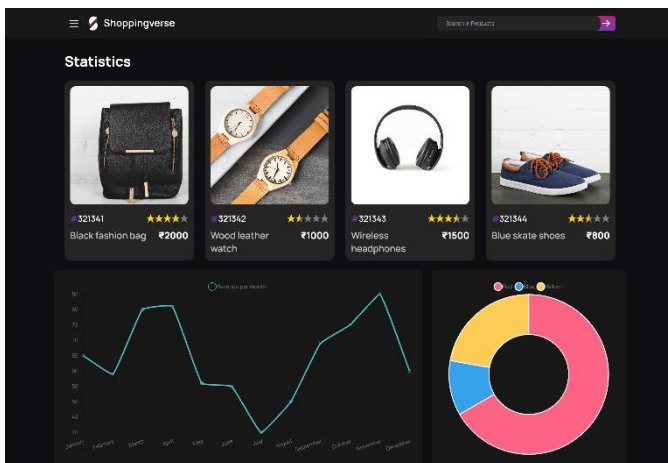
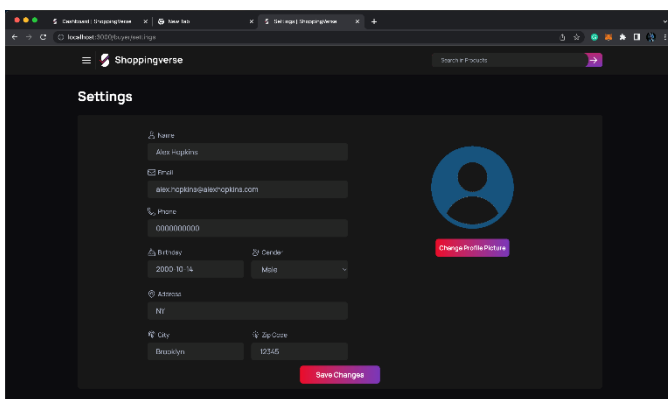
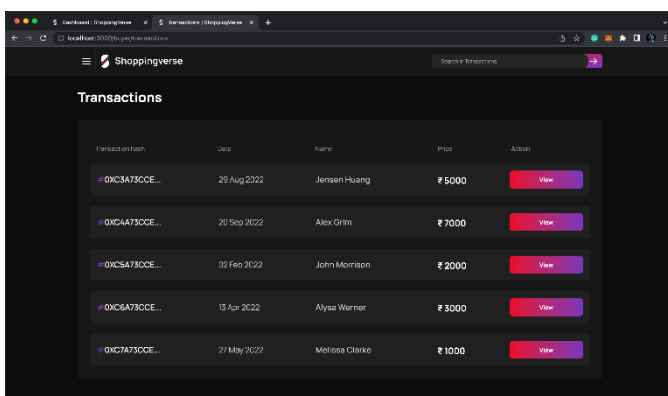


2)Order Details

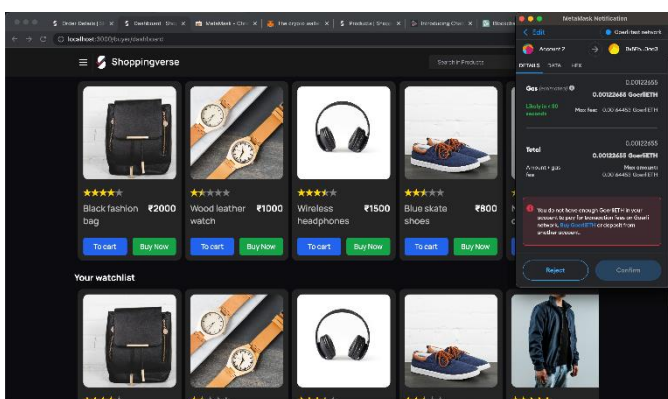


18. Screenshot of Website



Transaction Hash	Date	Name	Price	Action
0XC3A73CCE...	29 Aug 2022	Jensen Huang	₹ 5000	View
0XC4A73CCE...	20 Sep 2022	Alex Grim	₹ 7000	View
0XC5A73CCE...	02 Feb 2022	John Morrison	₹ 2000	View
0XC6A73CCE...	13 Apr 2022	Alysa Warner	₹ 3000	View
0XC7A73CCE...	27 May 2022	Melissa Clarke	₹ 1000	View



19. CONCLUSIONS

In today's society, e-commerce has been an important part of our life, from mobile payment to bank deposits, so safety and efficiency have become high-profile topics. Cryptography is the main research direction on the issues. The Ether-derived blockchain, with a series of technology combinations such as distributed storage, timestamp, hash-encryption, etc., achieves a highly trusted E-commerce environment. The blockchain saves data in a brand new block in a linear manner and from all previous blocks. Here, data is accurately encrypted with lot of encryption algorithm . When particular stakeholder adds some change data to a blockchain technology, the transaction must pass validation by miners which has mining setup based on hashing. Here, miners earn some recompense in terms of money, such as cryptocurrencies. This is advantage of blockchain technology. The network is decentralized in nature, and no single entity rule the data within a blockchain architecture. All transactions are immutable and transparent, . You cannot change, takedown, or hide any transaction once someone does it. The cross-border e-commerce payment platform based on blockchain supports point-to-point transactions between suppliers and customers without the need for exchange settlement. We design a privacy-preserving model for E-commerce systems based on blockchain technology. In order to protect users' identities and guarantee proof of ownership, we designed E-commerce Dapp, which is based on the blockchain. Blockchain does not allow any middlethings to come in between of the system. In addition to that, data once recorded in the blockchain ledger is untouchable ,immutable and unchangeable, It makes the whole transaction transparent and accurate where no one can change it but can only see stuff of trade. . Blockchain technology is based on the principle of decentralization. Here, no one entity controls the system, and centralization, which leads to inaccuracies,security risk and other issues, overcome this by decentralisation. In addition, it develops trust among stakeholders. Blockchain technology's shared data is encrypted with various encryption algorithm and offers superior security against any possible cyber attacks. recompense Any stakeholder can add a transaction to the system as a one entity does not control it. Thus, all stakeholders have transactional freedom.

20. REFERENCES

- [1]. X. H. Li, "Blockchain-based cross-border e-business payment model," in 2021 2nd International Conference on E-Commerce and Internet Technology (ECIT), pp. 67–73, 2021.
- [2]. Y. Jiang, C. Wang, Y. Wang, and L. Gao, "A privacy-preserving e-commerce system based on the blockchain technology," in 2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE), pp. 50–55, Feb 2019.
- [3]. W. Xie, W. Zhou, L. Kong, X. Zhang, X. Min, Z. Xiao, and Q. Li, "Ettf: A trusted trading framework using blockchain in e-commerce," in 2018 IEEE 22nd International Conference on Computer Supported

- Cooperative Work in Design ((CSCWD)), pp. 612–617, 2018.
- [4]. Y. Xia, Q. Li, and L. Wang, “Research on decentralized e-commerce architecture in p2p environment,” in 2010 International Conference on Electrical and Control Engineering, pp. 2929–2932, June 2010.
- [5]. A. Murugesan, K. Ramasamy, P. Aravind, V. Bathri Narayanan, and J. Daniel Raja, “A systematic survey of e-commerce applications with blockchain in agro sector,” in 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), vol. 1, pp. 1199–1204, March 2021.
- [6]. C.-N. Yang, Y.-C. Chen, S.-Y. Chen, and S.-Y. Wu, “A reliable e-commerce business model using blockchain based product grading system,” in 2019 IEEE 4th International Conference on Big Data Analytics (ICBDA), pp. 341–344, March 2019.
- [7]. G. Kumar, R. Saha, W. J. Buchanan, G. Geetha, R. Thomas, M. K. Rai, T.-H. Kim, and M. Alazab, “Decentralized accessibility of e-commerce products through blockchain technology,” *Sustainable Cities and Society*, vol. 62, p. 102361, 2020.
- [8]. S.-I. Kim and S.-H. Kim, “E-commerce payment model using blockchain,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 3, pp. 1673–1685, 2022.
- [9]. A. K. Shrestha, S. Joshi, and J. Vassileva, “Customer data sharing platform: A blockchainbased shopping cart,” in 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 1–3, May 2020.