Blockchain-Based Decentralized E-commerce Using Ethereum and Smart Contracts

Asan Nainar (Assistant Professor)
Department of Information Technology SRM Valliammai Engineering college
Chennai, India

Vigneshwaran
Department of Information Technology SRM Valliammai Engineering college
Chennai, India

Surya
Department of Information Technology SRM Valliammai Engineering college
Chennai, India

Saran Kumar
Department of Information Technology
SRM Valliammai Engineering college
Chennai, India

Santhosh Kanna
Department of Information Technology
SRM Valliammai Engineering college
Chennai, India

Abstract:- This blockchain-based decentralized e-commerce project aims to create a platform that enables buyers and sellers to interact and transact directly without the need for intermediaries. The project utilizes blockchain technology to ensure security, transparency, and immutability of transactions, and also incorporates Firebase and Moralis Web3 to provide seamless integration with existing web platforms. Firebase is a cloud-based platform that offers various services, including authentication, real-time database, and hosting, which are crucial in providing a secure and efficient e-commerce experience. Moralis Web3, on the other hand, provides a backend-as-a-service for web3 applications, allowing developers to interact with the Ethereum blockchain easily. In summary, this blockchain-based decentralized e-commerce project offers an efficient, secure, and cost-effective platform for buyers and sellers to engage in transactions without intermediaries. The integration of Firebase and Moralis Web3 enhances the platform's usability, making it accessible to a wider audience.

Keywords:- *Blockchain, Firebase, Web3, Ethereum.*

I. INTRODUCTION

In recent years, e-commerce has become an integral part of our daily lives. With the increasing use of digital transactions, security and transparency have become more important than ever. One of the major concerns of e-commerce is trust between buyers and sellers. It is not always easy for buyers to trust sellers they have never met, and for sellers to trust buyers who they do not know. This is where blockchain technology can come into play, as it provides decentralized and transparent transactions that can help build trust between buyers and sellers.

In this project, we propose a blockchain-based decentralized e-commerce platform that uses Firebase and Moralis Web3 to provide a reliable and secure platform for e-commerce transactions. Firebase provides a backend-as-a-service platform, which helps in managing and storing data, while Moralis Web3 provides an interface between the blockchain and the web application.

The platform we are proposing is decentralized, which means that it does not require intermediaries such as banks or other financial institutions. The platform runs on a blockchain, which is a distributed ledger technology that allows transactions to be recorded in a secure and transparent manner. The blockchain is maintained by a network of computers that work together to ensure the integrity of the system.

By using blockchain technology, we can ensure that transactions are secure and transparent. Each transaction is verified by the network, and once it is added to the blockchain, it cannot be altered or deleted. This means that there is no possibility of fraud, as all transactions are recorded on the blockchain and can be verified by anyone.

Furthermore, by using Firebase, we can ensure that the data stored on the platform is secure and can be accessed quickly and easily. Firebase provides a real-time database, which means that data is updated in real-time, and all changes are synchronized across all devices. This ensures that buyers and sellers can access up-to-date information about their transactions at all times.

Moralis Web3 provides an interface between the blockchain and the web application. It allows us to interact with the blockchain using JavaScript, which is the language used for web development. This makes it easy to develop and deploy decentralized applications on the blockchain.

Overall, this project aims to create a secure and decentralized platform for e-commerce, where users can buy and sell products without the need for intermediaries, and with the assurance of transparency and security provided by blockchain technology. By using Firebase and Moralis Web3, we can ensure that the platform is reliable, scalable, and can be accessed from anywhere in the world. This project has the potential to revolutionize the e-commerce industry by providing a secure and transparent platform for buying and selling products online.

II. IMPORTANCE OF BLOCKCHAIN

Security: Blockchain technology provides a decentralized and immutable ledger that can help secure transactions and data. It uses cryptographic techniques to ensure that data is tamper-proof and cannot be altered without consensus from the network participants.

Transparency: The transparency of blockchain technology can help increase trust between buyers and sellers. Every transaction on the blockchain is visible to all participants, and once a transaction is recorded, it cannot be deleted or altered.

Efficiency: Blockchain technology can help increase the efficiency of e-commerce transactions by removing intermediaries and reducing transaction costs. Smart contracts, which are self-executing contracts with the terms of the agreement directly written into code, can automate processes and reduce the need for intermediaries.

Decentralization: Integrating blockchain technology can help remove centralized intermediaries and reduce the risk of a single point of failure. This can help increase the resilience and availability of the e-commerce application.

Improved Payment processing: Blockchain technology can improve the payment processing by allowing near-instant transactions, reducing the need for intermediaries such as banks, and making cross-border payments easier.

III. FIREBASE AUTHENTICATION

A cloud-based platform called Firebase offers several tools and services for creating, deploying, and managing mobile and web applications. Firebase Authentication is one of its services, allowing programmers to quickly add authentication and user management to their apps. In contrast, Metamask is a browser extension that enables users to connect with blockchain-based applications and manage their cryptocurrency wallets. In this note, we'll go over using Metamask and Firebase Authentication together for secure, decentralized authentication.

It is crucial to comprehend the idea of decentralized authentication before getting into the specifics of Firebase Authentication with Metamask. Decentralized authentication refers to a type of authentication where users are authenticated independently, without the aid of a central authority or server. Instead, it makes use of blockchain technology to confirm users' identities. A decentralized authentication system is exemplified by Metamask, a bitcoin wallet.

Let's now examine the integration of Firebase Authentication with Metamask. Software Development Kits (SDKs) for platforms like web, iOS, Android, and others are offered by Firebase. These SDKs make it simple for programmers to include Firebase Authentication into their projects. Using the web SDK and the following steps, developers can combine Metamask with Firebase Authentication:

- Activate the Metamask login option in Firebase Authentication. Firebase Authentication offers support for a number of login options, including Google, Facebook, email, and password. Developers must establish a custom authentication provider in the Firebase interface and set it up to accept Metamask credentials in order to allow Metamask login.

- Integrate the Metamask login flow in the application: Once Firebase Authentication has enabled the Metamask login mechanism, developers must incorporate the Metamask login flow into their applications. It entails asking the user to sign a message with their Metamask wallet and then utilizing the Ethereum network to validate the signature.

- The application may authenticate the user in Firebase Authentication after the user has signed the message with their Metamask wallet and the signature has been confirmed. This entails giving the Firebase SDK the Metamask credentials in exchange for an access token that can be used to access Firebase services.

Compared to conventional authentication methods, using Metamask has a number of benefits. It is more secure and decentralized because it does not require a central authority or server to verify users. Second, it offers a smooth user experience because users can utilize their Metamask wallet to authenticate themselves with just a few clicks. The ability to create applications that are fully connected with the blockchain ecosystem also enables developers to create new applications, which opens up a vast array of opportunities.

In conclusion, Firebase Authentication and Metamask work well together to give developers the tools they need to create safe and decentralized applications. Developers must comprehend the advantages and constraints of decentralized authentication as well as how to incorporate it into their applications in light of the rising popularity of blockchain technology and decentralized applications.

IV. FLOW OF PROPOSED SYSTEM

The proposed system of a blockchain-based decentralized e-commerce project using Firebase and Moralis Web3 would have the following flow:

- User registration and login: With Firebase Authentication, users would be able to sign up for the platform and login. Other login options, such as Metamask and other blockchain wallets, will be supported by the platform.
- Product listing and management: On the platform, sellers will be able to list and control their products. On the blockchain, each product would be represented by a

smart contract that would include details about the item, including its name, description, price, and seller.

- Searching for things on the platform and buying them using cryptocurrency would be possible for buyers. The smart contract that represents the product would transfer ownership from the seller to the buyer when a buyer made a purchase.

- Processing payments: The platform would handle bitcoin payments through a cryptocurrency payment gateway like Coinbase or BitPay. Payment for an item purchased by a customer is transferred to the vendor's bitcoin wallet.

- Order tracking and management: Buyers and sellers will be able to track their orders on the platform. When a buyer purchases a product, the order status would be updated to "pending." As soon as the payment is verified, the order status is changed to "paid." Order status is changed to "shipped" when the product is shipped.

- Rating and feedback: On the site, buyers and sellers can rate and provide feedback for one another. This would support the development of customer and vendor reputations and trust.

- Blockchain integration: The platform would be fully integrated with the blockchain ecosystem, using Moralis Web3 to interact with the blockchain. This would enable the platform to access smart contracts and other blockchain-based services.

The process involved in a project of blockchain-based decentralized e-commerce using Firebase, Metamask, and Moralis Web3 can be divided into several stages. These stages include:

Planning and Research: This stage involves conducting market research to identify customer needs and preferences. It also involves identifying the technical requirements for the project, such as the blockchain platform to be used and the features to be implemented.

Design: In this stage, the architecture and design of the decentralized e-commerce platform are developed. This includes designing the user interface, the smart contracts that will power the platform, and the database schema that will store data.

Development: This stage involves the actual coding and development of the platform. Developers will write code to implement the features and functionality identified in the design stage. They will also develop and test smart contracts to ensure that they function as intended.

Testing: In this stage, the platform is tested to identify and fix any bugs or errors. This includes testing the platform's user interface, smart contracts, and database functionality.

Deployment: Once the platform has been tested and is deemed ready, it can be deployed to the production environment. This involves deploying the platform's smart contracts to the blockchain platform, setting up the database, and configuring the server infrastructure.

Maintenance and Support: After deployment, the platform requires ongoing maintenance and support. This includes fixing bugs that arise, adding new features, and providing technical support to users.

Overall, the proposed system would provide a secure, and transparent platform for e-commerce transactions. The use of blockchain technology, Firebase Authentication, and Moralis Web3 would ensure that the platform is secure, reliable, and scalable. By leveraging the power of blockchain technology, the platform would provide a level of trust and transparency that traditional e-commerce platforms cannot match.

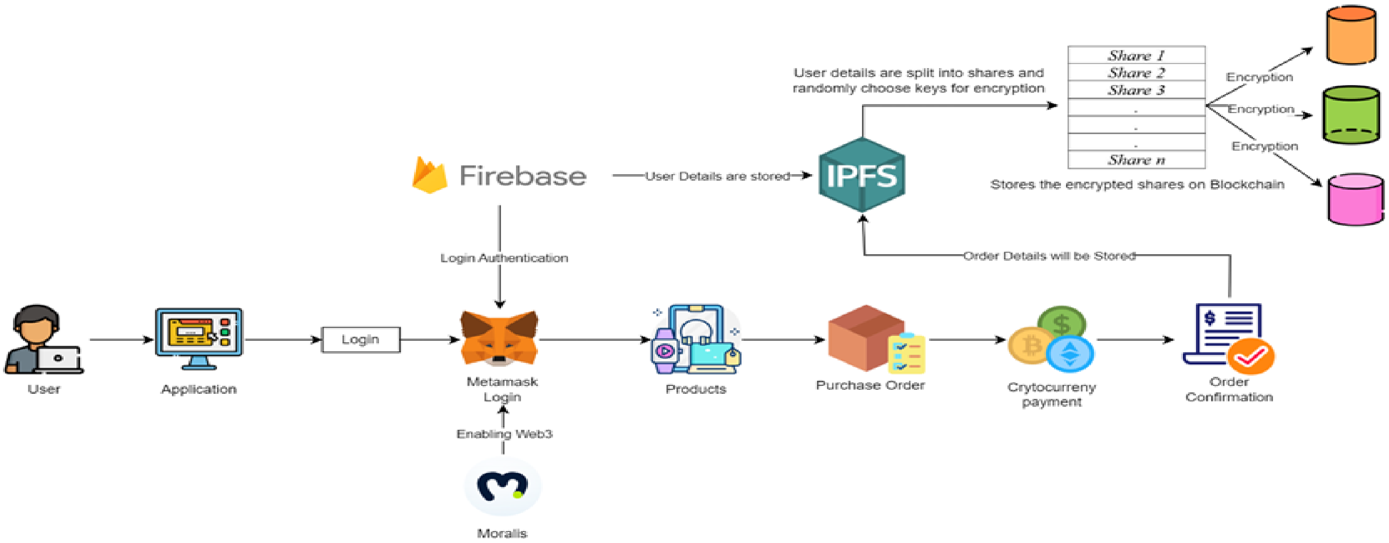

Fig 1 Proposed System

V. ETHEREUM GOERLI

In a project of blockchain-based decentralized e-commerce using Firebase, Metamask, and Moralis Web3, Ethereum Goerli can be used as a testnet for developers to test their smart contracts and decentralized applications before deploying them to the mainnet. The usage of Goerli can provide several benefits to the project, including:

- Safe Testing Environment: Ethereum Goerli provides a safe testing environment for developers to test their smart contracts and decentralized applications without risking real funds on the mainnet. This enables developers to identify and fix any bugs or errors in their code before deploying it to the mainnet.

- Fast Transactions: Goerli has a fast block time of 15 seconds, which enables developers to test their transactions quickly and efficiently. This can help speed up the development process and reduce the time it takes to deploy new features to the platform.

- Easy Integration: Goerli can be easily integrated with other Ethereum tools and services, such as Metamask and Moralis Web3. This makes it easy for developers to test their applications and smart contracts in a familiar environment.

- Lower Costs: Transactions on the Goerli testnet are free, which means that developers can test their applications and smart contracts without incurring any costs. This can be particularly beneficial for smaller projects or teams that have limited resources.

In this project, Goerli can be used to test the smart contracts that represent the products on the platform, the payment gateway, and the order tracking and management system. This can help ensure that the platform is secure, reliable, and scalable before deploying it to the mainnet.

Overall, the usage of Ethereum Goerli in a project of blockchain-based decentralized e-commerce using Firebase, Metamask, and Moralis Web3 can provide developers with a safe and efficient testing environment, while reducing costs and improving the overall quality of the platform.

VI. ALGORITHMS

These are the algorithms used in the project of a blockchain based decentralized e-commerce application:

Proof of Work (PoW) - PoW is an algorithm used by many blockchain networks, including Bitcoin and Ethereum. It involves solving complex mathematical problems in order to verify transactions and add new blocks to the blockchain. PoW requires a significant amount of computing power, which can make it expensive and energy-intensive.

Proof of Stake (PoS) - PoS is an alternative algorithm that is less energy-intensive than PoW. Instead of solving complex math problems, PoS involves validators (or "stakers") putting up a stake (i.e., a certain amount of cryptocurrency) to verify transactions and add new blocks to the blockchain. Validators are chosen based on the amount of stake they hold, and they receive rewards for their participation.

Byzantine Fault Tolerance (BFT) - BFT is an algorithm designed to ensure that a distributed system (such as a blockchain network) can function correctly even if some of the nodes are faulty or malicious. BFT involves a consensus mechanism where nodes must agree on the validity of transactions before they are added to the blockchain.

Elliptic Curve Digital Signature Algorithm (ECDSA) - ECDSA is a cryptographic algorithm used to verify the authenticity and integrity of transactions on the blockchain. It involves using public and private keys to sign and verify transactions, ensuring that they have not been tampered with.

Merkle Trees - Merkle trees are a data structure used to efficiently verify the integrity of large amounts of data. In the context of blockchain, Merkle trees are used to verify that a particular transaction is included in a particular block without having to download and verify the entire blockchain.

Blockchain algorithm that generates a continuous hash value of 256 every time, bits. Another component of encryption technology is this algorithm. This contains some 256-bit data, referred to as IV. Now, the input we receive will be enormous.

Hence, divide it into 512-bit chunks. Since the input will never be a perfect multiple of 512 bits, some input will always be missing. We padding concatenate the input with 10 bits before this left input. Now that our input is a perfect multiple, we may go on.

This output 256 bit is once more combined with the input 512 bits from block B2. To get a 256-bit output, the sum is once more placed through the compression process. The final block is filled by this loop (block n).

Once more, a compressing function begins and produces a final output of 256 bits, or what is known as a hash of the input data. Message Length: The clear text portion of the message shouldn't be longer than 264 bits.

Digest Length: The length of the hash digest for the SHA-256 algorithm should be 256 bits, for the SHA-512 algorithm 512 bits, and so forth. Larger digests typically imply a lot more calculations at the expense of performance and storage.

All hashing algorithms, including the SHA 256, are intended to be irreversible. If you already have the digest, you shouldn't receive the plaintext, and if you run the digest through the hash function once more, it shouldn't return the original value.

VII. METAMASK

Metamask plays a crucial role in a project of blockchain-based decentralized e-commerce using Firebase, Metamask, and Moralis Web3. Metamask is a browser extension that acts as a digital wallet, allowing users to store, manage, and interact with cryptocurrencies and decentralized applications (DApps) on the Ethereum network.

In a decentralized e-commerce platform, Metamask allows users to securely and seamlessly make transactions using Ethereum and other ERC-20 tokens. Users can connect their Metamask wallet to the platform, and use it to make payments for purchases or receive payments for sales.

Metamask also enables seamless interaction with the Ethereum network and its smart contracts. This is important for the platform's functionality, as it allows for the execution of smart contracts that automate various aspects of the e-commerce process such as order processing, payment settlement, and dispute resolution.

Additionally, Metamask provides an easy-to-use interface for interacting with decentralized applications, making it simpler for users to navigate the platform and complete transactions. It also enhances security by providing features such as password protection and two-factor authentication.

Overall, Metamask is a critical component of a blockchain-based decentralized e-commerce platform, as it provides a user-friendly interface for interacting with the Ethereum network and its smart contracts, and enables secure and seamless transactions using cryptocurrencies.

VIII. CONCLUSION

In conclusion, the project has the potential to revolutionize the e-commerce industry by providing a more secure, transparent, and efficient way to buy and sell goods and services.

By leveraging the benefits of blockchain technology such as immutability, transparency, and decentralization, this type of platform can offer a higher level of trust and security to both buyers and sellers. Smart contracts can be used to automate various aspects of the e-commerce process, such as order processing, payment settlement, and dispute resolution, which reduces the need for intermediaries and results in faster and more cost-effective transactions.

Firebase, Metamask, and Moralis Web3 provide essential tools for the development and deployment of a blockchain-based decentralized e-commerce platform. Firebase offers a scalable and secure backend infrastructure, while Metamask provides a user-friendly interface for interacting with the Ethereum network and its smart contracts. Moralis Web3 offers a range of services and tools for building decentralized applications, making it easier to integrate blockchain technology into the e-commerce platform.

To successfully develop and deploy a project of blockchain-based decentralized e-commerce using Firebase, Metamask, and Moralis Web3, it is important to follow best practices for blockchain development and security. This includes conducting code reviews, ensuring that smart contracts are audited, and implementing security measures such as multi-factor authentication and encryption.

Overall, a project of blockchain-based decentralized e-commerce using Firebase, Metamask, and Moralis Web3 has the potential to disrupt the traditional e-commerce industry and offer a more secure, transparent, and efficient way for buyers and sellers to transact. By leveraging the benefits of blockchain technology and the essential tools provided by Firebase, Metamask, and Moralis Web3, developers can create a platform that offers a higher level of trust and security to all participants in the e-commerce ecosystem.

REFERENCES

[1] C Shangping Wang “A Block chain-Based Distributed Storage Network to Manage Growing Data Storage Needs” 2019IN IEEE ACCESS, VOL. 9, PP. 57426- 57439, 2021, DOI: 10.1109/ACCESS.2019.52108..

[2] Jiangang Shu and Xing Zou “Block chain-Based Decentralized Public Auditing for Cloud Storage” 2021 International Conference on Information and Communications Technology (ICOIACT),2019,pp.206 doi:10.1109/ICOIACT46704.2019.8938570.

[3] Vijay A.Kanade “A Secure Cloud Storage Framework With Access Control Based on Block chain” 2021 pp. 1-5, DOI: 10.1109/ICETAS.2017.8277548.

[4] Customer Data Sharing Platform: A Blockchain-Based Shopping Cart Publisher: IEEE, Authors: Ajay Kumar Shrestha; Sandhya Joshi; Julita Vassileva. DOI: 10.1109/ICBC48266.2020.9169421

[5] A Blockchain based model for Curbing Doctors Shopping and Ensuring Provenance Management Publisher: IEEE, authors: Shekha Chenthara; Hua Wang; Khandakar Ahmed; Frank Whittaker; Ke Ji. DOI: 10.1109/NaNA51271.2020.00040

[6] Blockchain based Confidentiality and Integrity Preserving Scheme for Enhancing E-commerce