Decentralized Cryptocurrency Wallet

Dr. Jyothi A P
Assistant Professor, Dept. of CSE,
Faculty of Engineering and Technology,
Ramaiah University of Applied Sciences,
Bengaluru, India
jyothiarcotprashant@gmail.com

Dr.Pushphavathi T P
Associate professor & HOD, Dept. of CSE,
Faculty of Engineering and Technology,
Ramaiah University of Applied Sciences
Bengaluru, India
pushphavathi.cs.et@msruas.ac.in

ABSTRACT

A cryptocurrency is an encrypted data string that denotes a unit of currency. It is monitored and organized by a peer-to-peer network called a Blockchain, which also serves as a secure ledger of transactions, e.g., buying, selling, and transferring. The main advantages are that crypto-currencies don't have a central issuing or regulating authority, instead using a decentralized system to record transactions and issue new units, which makes it secure. The main motive of this paper is to make a platform where people can send crypto currency, receive cryptocurrency and along with that they can also send Messages and Gif's along with those transactions. In this paper Decentralized Cryptocurrency Wallet where people can have interactive crypto data and have safe Ethereum transfer is discussed. The application is primarily a decentralized cryptocurrency wallet, which will be able to send and receive transaction between two accounts. The application is also able to send messages and gifs with the transactions as an attachment. The application is also able to display the transaction history.

Keywords— Ethereum, Decentralized Cryptocurrency Wallet, transaction history, Blockchain.

I. INTRODUCTION

This section gives complete knowledge and understanding of the different technologies and frameworks that were required for implementation of project discussed in this paper.

React.js:

React.js is the most popular front-end JavaScript library for building Web applications. React.js or Reactjs or simply React are different ways to represent React.js. React.js is an open-source JavaScript library that is used for building user interfaces specifically for single-page applications. It is used for handling the view layer for web and mobile apps. React also allows us to create reusable UI components. React was first created by Jordan Walke, a software engineer working for Facebook. React allows developers to create large web applications that can change data, without reloading the page. The main purpose of React is to be fast, scalable, and simple. It works only on user interfaces in the application. This corresponds to the view in the MVC template. It can be used with a combination of other JavaScript libraries or frameworks, such as Angular JS in MVC. Some important features of React.

- React is declarative
- React is simple yet powerful
- React is component-based
- React supports server-side
- React supports mobile support
- React is extensible

CSS:

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation of a document written in a markup language such as HTML. CSS is a cornerstone technology of the World Wide Web, alongside HTML and JavaScript. CSS is designed to enable the separation of presentation and content, including layout, colors, and fonts. This separation can improve content accessibility; provide more flexibility and control in the specification of presentation characteristics; enable multiple web pages to share formatting by specifying the relevant CSS in a separate .css file, which reduces complexity and repetition in the structural content; and enable the .css file to be cached to improve the page load speed between the pages that share the file and its formatting. Separation of

formatting and content also makes it feasible to present the same markup page in different styles for different rendering methods, such as on-screen, in print, by voice (via speech- based browser or screen reader). The name cascading comes from the specified priority scheme to determine which style rule applies if more than one rule matches a particular element.

JavaScript:

JavaScript is one of the core technologies of the World Wide Web alongside HTML and CSS. All major web browsers have a dedicated JavaScript engine to execute the code on the user's device and websites use it client-side for web page behavior, often incorporating third-party libraries. As a multi-paradigm language, JavaScript supports event-driven, functional, and imperative programming styles. It has application programming interfaces (APIs) for working with text, dates, regular expressions, standard data structures, and the Document Object Model (DOM). JavaScript engines were originally used only in web browsers, but they are now core components of some servers and a variety of applications. The most popular runtime system for this usage is Node.js.

Hardhat:

It is an Ethereum development environment for professionals. It facilitates performing frequent tasks, such as running test, automatically checking code for mistakes or interacting with a smart contract. This means compiling, running and testing smart contracts at the very core. Hardhat comes built-in with Hardhat Network, a local Ethereum network designed for development. Its functionality focuses around Solidity debugging, featuring stack traces, console.log () and explicit error messages when transactions fail.

Solidity:

It's used to create smart contracts that implement business logic and generate a chain of transaction records in the Blockchain system. It acts as a tool for creating machine-level code and compiling it on the Ethereum Virtual Machine. It has a lot of similarities with C and C++ and is pretty simple to learn and understand. For Like other programming languages, solidity programming also has variables, functions, classes, arithmetic operations, string manipulation, and many other concepts. It is and object-oriented programming language created specifically by the Ethereum Network team for constructing and designing smart contracts on Blockchain platforms. Example, a "main" in C is equivalent to a "contract" in Solidity.

Alchemy:

It is a blockchain scaling platform that allows developers to securely create, test, and monitor their decentralized apps. This platform provides dependable network connectivity and node management endpoints. Alchemy simply decentralized development and go beyond just providing remote nodes with features like Notify, which allows developers to send real-time push notifications to users for critical events based on blockchain activities and their NFT API that provides a suite for services allowing us to instantly find, verify and display and NFT across multiple blockchains.

Ethereum:

It is a decentralized blockchain platform that establishes a peer-to-peer network that securely executes and verifies application code, called smart contracts. Smart contracts allow participants to transact with each other without a trusted central authority. Transaction records are immutable, verifiable, and securely distributed across the network, giving participants full ownership and visibility into transaction data. Transactions are sent from and received by user-created Ethereum accounts. A sender must sign transactions and spend Ether, Ethereum's native cryptocurrency, as a cost of processing transactions on the network.

Smart Contract:

Smart contracts are computer programs that are hosted and executed on a blockchain network. Each smart contract consists of code specifying predetermined conditions that, when met, trigger outcomes. By running on a decentralized blockchain instead of a centralized server, smart contracts allow multiple parties to come to a shared result in an accurate, timely, and tamper-proof manner. Smart contracts are a powerful infrastructure for automation because they are not controlled by a central administrator and are not vulnerable to single points of attack by malicious entities. When applied to multi- party digital agreements, smart contract applications can reduce counterparty risk, increase efficiency, lower costs, and provide new levels of transparency into processes.

Scope of the paper:

- Send transaction to any account.
- View the balance in the Ethereum card.
- Send messages and Gif's along with the transaction.
- Is accessible from many browsers as a web application.

II. LITERATURE SURVEY

Dejan Vujičić, Dijana Jagodić, Siniša Ranđić [1], Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview The objective of the project is toprovide an early development and ideas on Decentralized Digital Currencies how it evolvesand grow into such large scale In this survey paper1 Research trends have been specified as:

(1) Understandingconsumer's (non)acceptance ofcryptocurrencies
(2) Ethical aspectsand trust in cryptocurrencies,
(3) Blockchain technology as atrust-free technology,
(4) The blockchain/trusteconomy
(5) Blockchain technology: challenging trust.

Bitcoin and Ethereum today arethe most known and valuable cryptocurrencies. They are based on blockchain technology that is intended to promote a trust mechanism in apeer-to-peer network based on the consensus of the majority ofthe nodes. In the past few numerous cryptocurrencies,hashing algorithms, and consensus agreements in the networks. Some of the cryptocurrencies worth mentioning are Ripple, Cardano, NEO, Stellar, Litecoin,EOS, IOTA and many more.

Abderahman Rejeb, Karim Rejeb2, John G. Keogh [2], Cryptocurrencies in Modern Finance. The focus on cryptocurrencies inthe finance and banking sectors is gaining momentum. In this paper, we investigate therole of cryptocurrencies in modern finance. We apply a narrative literature review method to synthesize prior research and draw insightsinto the opportunities and challenges of leveraging cryptocurrencies instantly without having face to face conversation. Method done in this literature review is using different academic databases, such as Google Scholar, Scopus, Web of Science and Springer Link. In this the narrativeliterature review enables us to investigate the different ways that cryptocurrencies have been conceptualized inprior studies as well as to assess thetheoretical under pinning of this emerging paradigm in finance. In this paper, we have synthesized the literature on the role and challenges of cryptocurrencies in modern business and financial systems.

Saeed Alzahrani Portland State University Tugrul Daim Portland State University,[3] Analysis of the Cryptocurrency Adoption Decision on year 2019, The goal is to offer a currency that is not tied, created or backed by a government. Cryptocurrency use the block chain technology. Cryptocurrency adoption level has increased, and the market has grown dramatically. The aim of this paper is to fill the gap in the current literature by investigating the current cryptocurrency adoption level is used in this literature survey. Adoption level includes recognition of increased cryptocurrency using indicators. The main goal is to classify the existing adoption level. The blockchain wallet is used in this method. The goal of this paper is to investigate the cryptocurrency adoption decision. We examined the factor influencing the adoption decision and provided an in- depth analysis of each factor.

Shamili Prabakaran and B. Muruganantham, Enhancing theDecentralizedApplication (DApp) for E- commerce by Using the Ethereum Blockchain [4] January2022, Research mainly focuses on building the blockchain based decentralized application by using the web3 library along with the ganche and metamask in the localhost. To secure the online shopping transactions upon theuser's privacy concern. For the front end they used web3 to interact with smartcontract and React.js for theclient-side UI. For the wallet they have used MetaMask for managing personal accounts and privatekeys. For developing framework forsmart contracts, they used Truffle as a back-end. Ganache-Local private network for smart contracts development. Testnets- Public test networks for smart contracts development before deployingto the main network. Main Network- Public networks for actual smart contracts development. The implementation of the DApp could done with the othertest networks also for the efficient working of the nodes and the performance of the nodes with different test networks can be analyzed in future work. Also, the quantumcomputing under blockchain is the current research for high computational power and to mine the mathematical crypto puzzle easily in future work.

Sandeep Kumar Panda and Suresh Chandra Satapathy, An Investigation into Smart Contract Deployment on

Ethereum Platform UsingWeb3.js and Solidity Using Blockchain [5] May 2021, Here in this paper, they mainly focus onthe consensus algorithms that are used to manage and control blocks on theblockchain. Also, on the Ethereum which is used to implement DApp using smart contracts. Lately focuses on the implementation methodology on Ethereum blockchainfor creating and deploying and also interaction with the smart contract. For the front end they used web3 to interact with Ethereumsmart contract. MetaMask is used as Ethereum client for managing personal accounts and private keys. The smart contract was deployed on Rinke by Test network. For developing framework forsmart contracts, they used Truffle as a back-end. Ganache- Local private networkfor smart contracts development. Addressing the fundamentals ofthe visionary blockchain technology to develop, discussed on the consensus algorithms. Proposed a novel approach for deploying smart contract and interacting with it.Also explore the unexplored areas related to Ethereum, smart contract and Web3.

III. PROPOSED TECHNIQUE

We present a system to implement a decentralized Cryptocurrency wallet application with Web3.0 Technologies and Ethereum blockchain as shown in Figure 1.

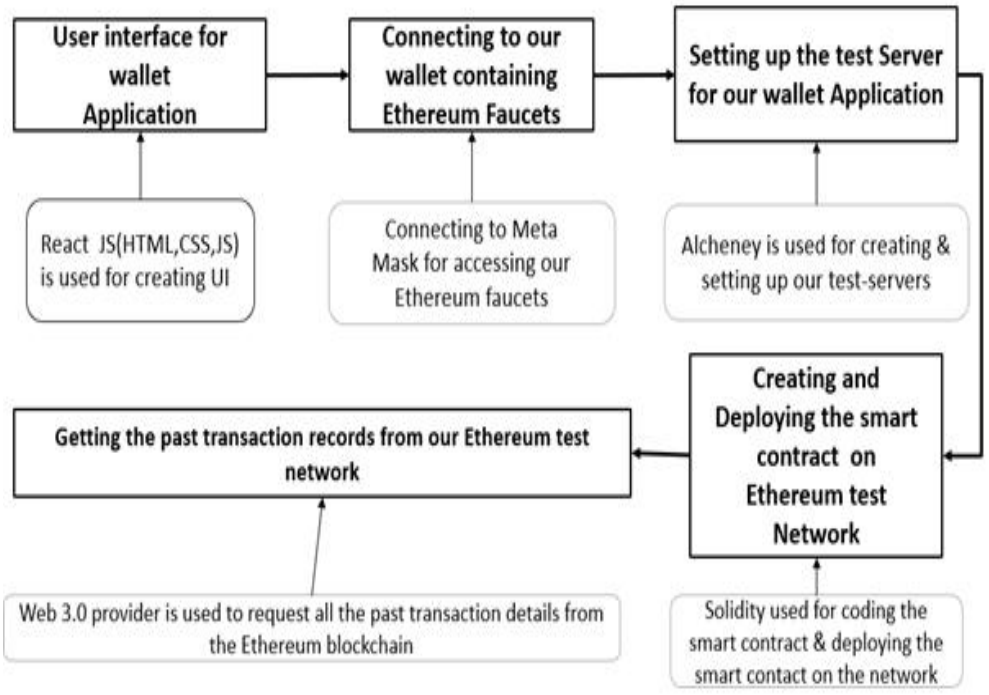


Figure 1: Proposed System.

Algorithm

1. Start.
2. Connect to MetaMask:
   If account present do: Login
   Else do:
   write create Account.
3. Enter R_Add, Amt, Message, Gif and click send button;
4. T_Fee := G_Units + (B_Fee + tip); Final_Amt := Amt + T_Fee;
5. Check the wallet balance:
   If Wallet Balance < Final_Amt do:

write Error ;

else do: proceed ;

6. Authenticate the Transaction in the MetaMask;
7. Store the Transaction on the Test-Server Address and on Ethereum Blockchain;
8. Show past transactions on the Wallet User Interface := S_Add, R_Add, Message and Gif;
9. End.

Keywords:

1. **R_Add** : Receiver's Address.
2. **S_Add** : Sender's Address.
3. **Amt**: Amount to be sent.
4. **T_Fee**: Charges incurred on the transaction.
5. **G_Units**: Ethereum gas charges for the Transaction.
6. **B_Fee**: Base Fees of the Ethereum Blockchain.
7. **Final_Amt**: Amount after adding all the charges as per the Transaction Amount.

IV. RESULTS AND DISCUSSION

Functional Requirements No.	Expected	Obtained
FR1	The application should allow user to connect with their Ethereum blockchain which stores the Ethers.	System successfully allows to connect to the wallet.
FR2	The application should allow the user to login using credential in the Meta Mask.	The user was successfully able to login in the MetaMask.
FR3	The application should allow the user to see balance in the Ethereum card	The user was successfully able to view the balance in the Ethereum card.
FR4	The application should allow to send cryptocurrency to their friend's wallet address, and receive cryptocurrency on their wallets also.	The user was successfully able to send cryptocurrency to and receive too by wallet address.
FR5	User should have an option to send a text attached to the transaction so that the receiver may find it easier to recognize from whom he has received the cryptocurrency.	The user was successfully able to send text attachment.

FR6	User should be able to send Gif attachments along with the transaction message so that the wallet looks attractive.	The user was successfully able to send Gif's attachments along with the transaction.
FR7	All the transactions taking place in the user's wallet must be reflected in the Ethereum Blockchain	All the transactions taking place in the users wallet was successfully reflected in the Ethereum Blockchain.

Table 1: Results obtained for Functional requirements

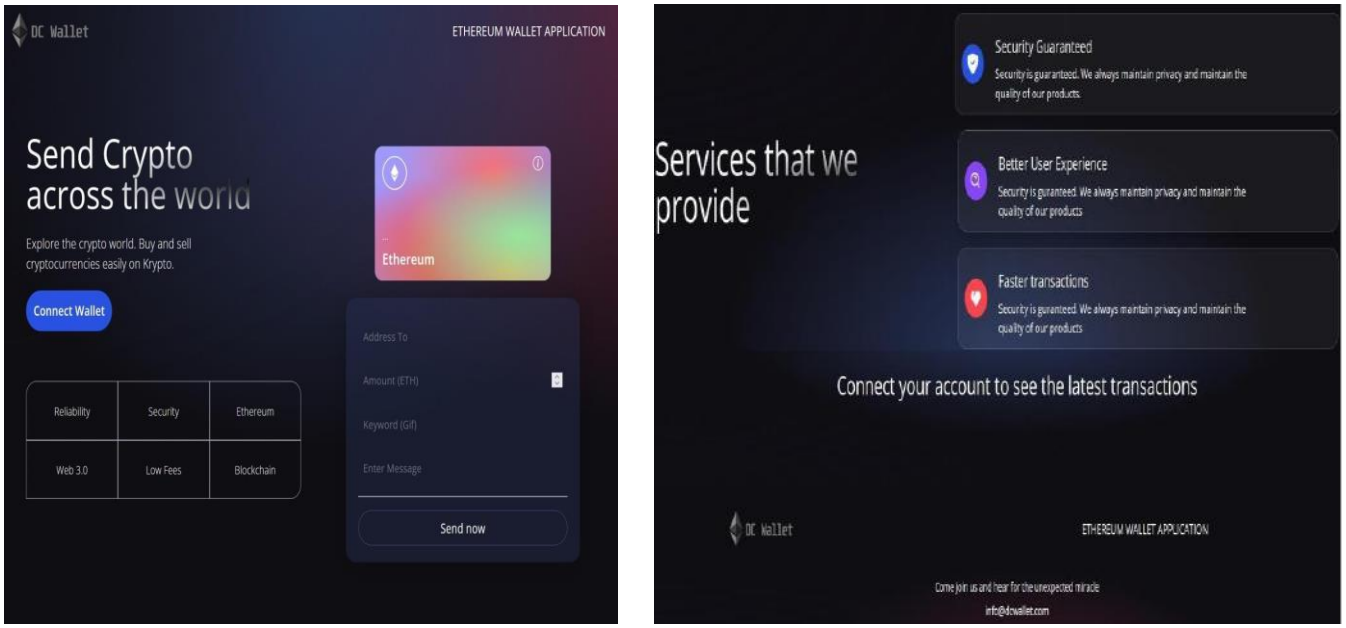


Figure 2: Shows the User Interface for the wallet application

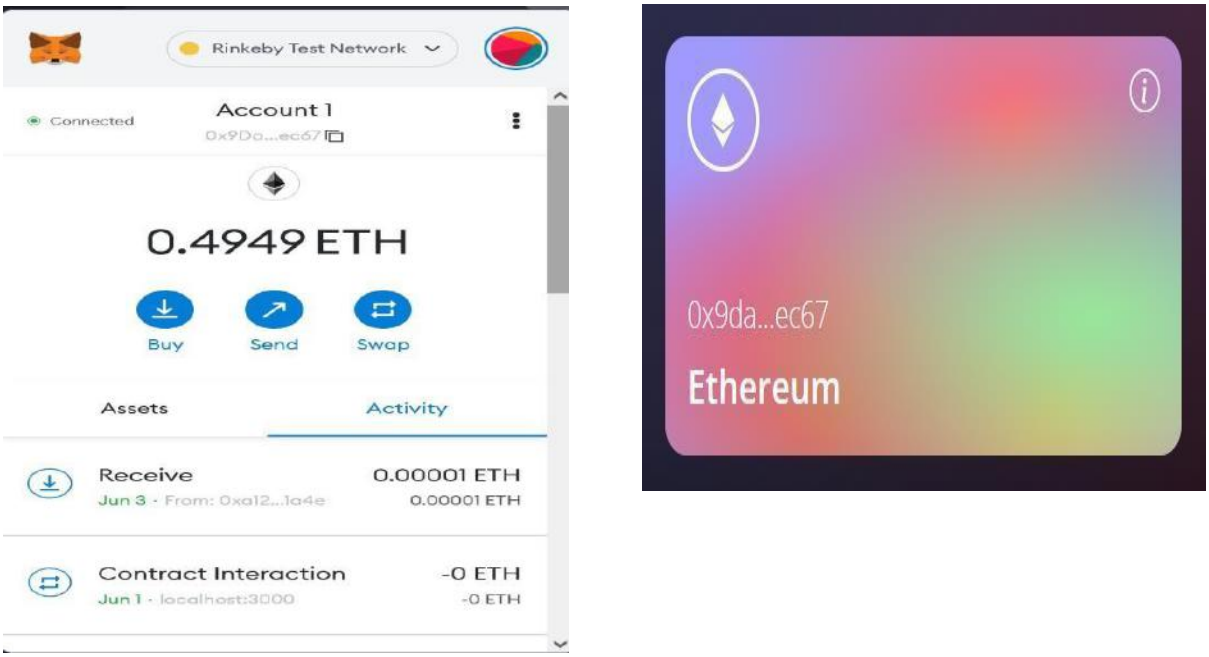
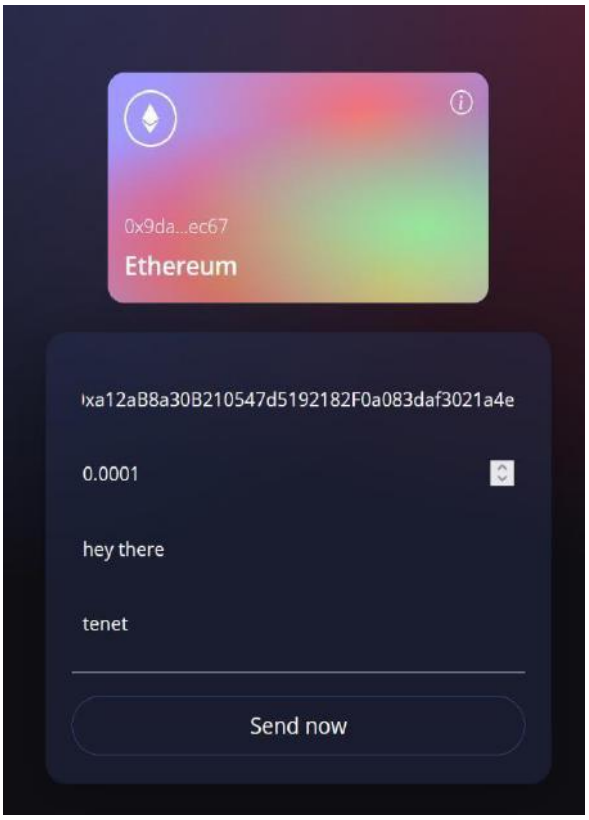
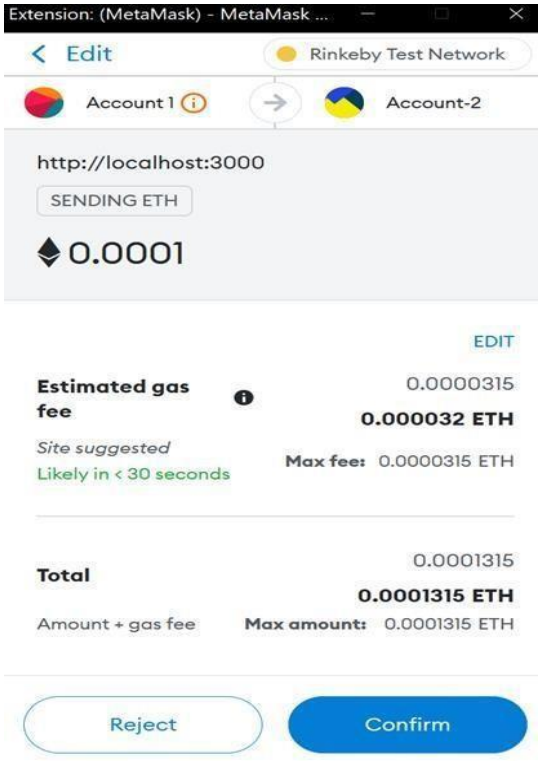


Figure 3: Shows the MetaMask Connected for the wallet application and the Address on the Ethereum Card.





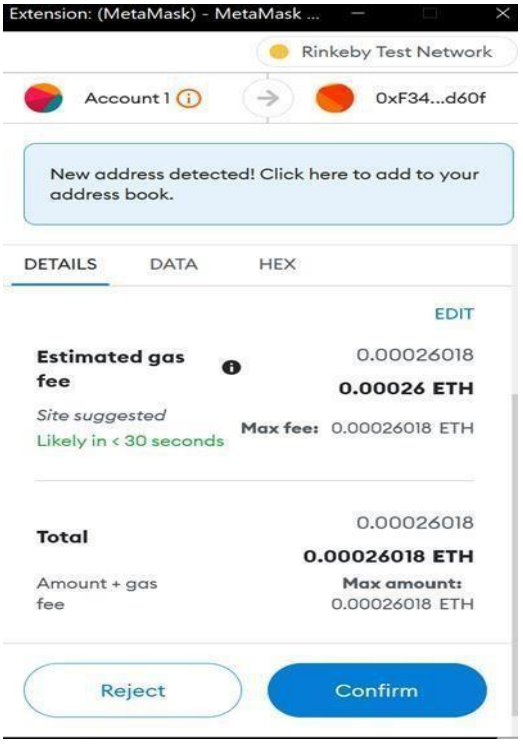


Figure 4: Shows the transactions made through the wallet application on our Test Network on Ehterum Blockchain.

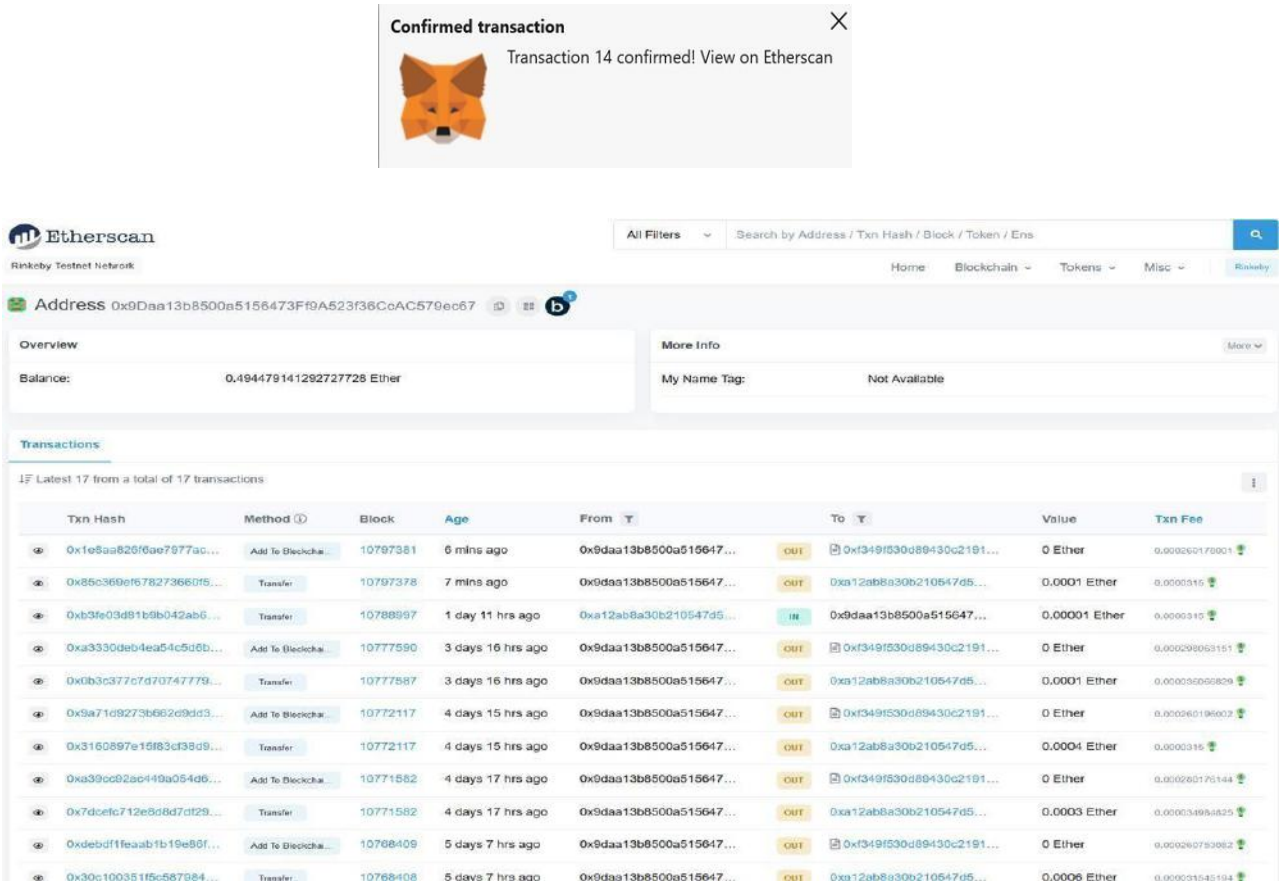


Figure 5: Shows the Transaction confirmation on MetaMask and Storing the Transaction on the Ethereum Blockchain

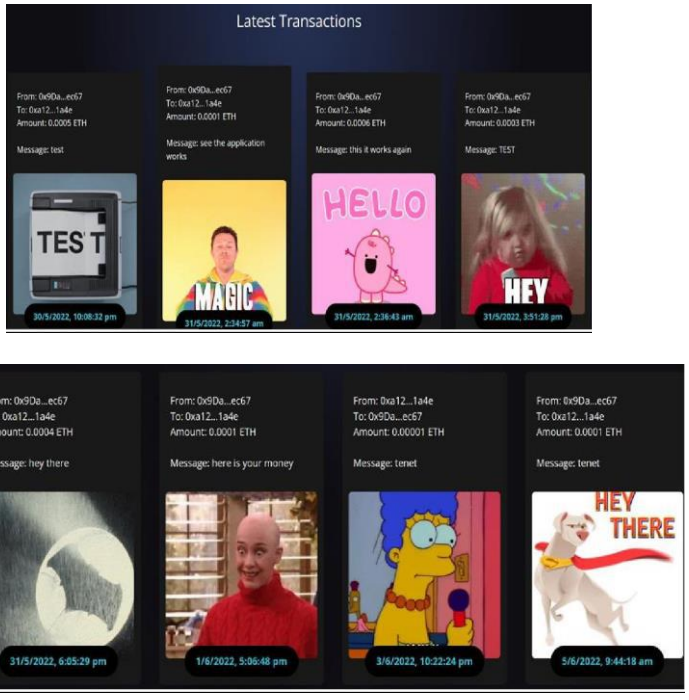


Figure 6: Shows the Transactions made from the wallet application with date, time, Address of both Sender and Receiver and Gif's/Attached Message in the transactions.

V. CONCLUSIONAND FUTURE WORK

Conclusion:

- Literature survey has been successfully conducted on different papers, journals which were on decentralized cryptocurrency wallets and Ethereum blockchain.
- The project successfully delivered on all requirement specifications.
- Care was ensured during the design to make sure data integrity is maintained and to avoid all forms of redundancies associated with data.
- The user is assured a friendly interface, behind which there are wide ranging technical details.
- This project has also been built in such a manner that future changes or modifications that are required can easily be implemented without affecting the functionality of the system.
- Documentation has been successfully completed in every phase of the project.

Future work:

- There is always room for improvement in any solution, however good and efficient it may be done. But most importantly it should be extremely flexible to accept further modification. For now, we are just dealing with ethers transactions and messages and gifs attachment.
- We can extend further this project by monetizing the platform as it is just a prototype. And we can also include decentralized exchange of different crypto currencies.
- Also, In the future the application provides many other services such as stock market rates of different cryptocurrencies as well as NFT's.

REFERENCES

[1]"Enhancing the Decentralized Application (Dapp)for E-commerce by using the Ethereum Blockchain" by: P.Shamili and Dr.B.Muruganantham, SRM Institute of Science and Technology, Department of Engineering and Technology, Kattankulathur, Chennai.

[2] "Blockchain technology, bitcoin, and Ethereum: A brief overview" by: Dejan Vujičić, Dijana Jagodić, Siniša Ranđić, Faculty of Technical Sciences in Čačak University of KragujevacČačak, Serbia.

[3] "An Investigation into Smart Contract Deployment on Ethereum Platform Using Web3.js and Solidity using Blockchain" by: Sandeep Kumar Panda and Suresh Chandra Satapathy.

[4] "Survey on Blockchain-Based Smart Contracts: Technical Aspects and Future Research" by: Tharaka Mawanane Hewa1, (Student Member, IEEE), Yining Hu2, (Student Member IEEE),Madhusanka Liyanage3, (Senior Member, IEEE), Salil Kanhare4, (Senior Member, IEEE) and Mika Ylianttila 5, (Senior Member, IEEE) (PDF) Survey on Blockchain-Based Smart Contracts Technical Aspects and Future Research.

[5] "Decentralized apps of the future implementing Web3." by: Aditya Patil, Prof. Santosh S (Computer Science and Engineering, Jain (Deemed to be University))

[6] https://imaginovation.net/blog/crypto-wallet-app-development-guide/ "DECENTRALIZED WALLET APPLICATION (Dapp wallet) ".

[7]"Building Blockchain Projects: Building decentralized Blockchain applications with Ethereum and Solidity "by Narayan Prusty (Author).

[8] https://docs.soliditylang.org/en/v0.8.14/ "Solidity Language documentation".

[9] https://reactjs.org/docs/getting-started.html, "React JS official documentation",

[10] https://www.dappuniversity.com/articles/how-to-build-a-blockchain-app , "Building a Blockchain application".