IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 4, April 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204305 |

Decentralized Cryptocurrency Exchange

Shivam Pal, Sunny Patil, Pankaj Parte, Bharati Gondhalekar

Dept. of Information Technology, Vidyavardhini's College of Engineering & Technology (VCET),Vasai, India

Dept. of Information Technology, Vidyavardhini's College of Engineering & Technology (VCET),Vasai, India

Dept. of Information Technology, Vidyavardhini's College of Engineering & Technology (VCET),Vasai, India

Assistant Professor, Dept. of Information Technology, Vidyavardhini's College of Engineering & Technology (VCET), Vasai, India

ABSTRACT: On today's digital exchange platforms, trading cryptocurrencies is a trust-based procedure where both parties to the exchange must have complete faith in the service provider. This could result in money being stolen, as has been demonstrated numerous times, either as a result of dishonest service providers who simply vanish or as a result of possible hacks on these sites. In this work, we propose and create an open, verifiable, and trustless decentralized exchange solution based on smart contracts operating on the Ethereum network. The platform allows two parties to trade other currencies, but as of right now, only Ethereum. As an escrow, a smart contract running on the Ethereum blockchain holds user funds until the other side completes a validated transaction. We put our method into practice by using an oracle to enable the smart contract to recognize a Bitcoin transfer. We establish a workable platform and outline the system architecture. We then test it in a fictitious situation by successfully exchanging Bitcoin and Ether on test blockchain networks. In the paper's conclusion, we list potential obstacles and dangers to such a system.

I. INTRODUCTION

A decentralized exchange, or DEX for short, is a peer-to- peer marketplace where cryptocurrency traders conduct transactions directly with one another. One of the fundamental uses of cryptocurrencies is the promotion of financial transactions without the involvement of banks, brokers, payment processors, or any other type of middle- man. On the other hand, decentralized exchanges are nothing more than a collection of smart contracts. DEX transactions are settled immediately on the blockchain, in contrast to centralized exchange transactions, which are stored in the exchange's own database.

II. PROBLEM STATEMENT

The goal of this project is to develop a blockchain application that will enable decentralized bitcoin trading. All participants would have access to the market through a pure peer-to-peer trade mechanism instead of relying on a central authority. The plat- form allows two parties to trade other currencies, but as of right now, only Ethereum. As an escrow,a smart contract running on the Ethereum blockchain holds user funds until the other side completes a validated transaction.

III. LITERATURE SURVEY

a) Agent Chain[1] :

Agent Chain, a new cross-chain solution with improved compatibility, effectiveness, and decentralization, was presented. Users can map assets from other blockchain projects to Agent Chain through a chosen trading group's multi-signature deposit pool. Trading operators can be coupled to form a variety of decentralized trading groups. To maintain the system's security, multi-signature, assets locking, arbitration, and pertinent mechanisms severely restrict the actions of trade operators. This system offers a deeper understanding of the cross-chain exchange technique and is appropriate for use in real-world scenarios.

b) Facilitating the Decentralized Exchange of Cryp-tocurrencies in an Order-Driven Market [2] :

This paper describes their ongoing investigation into the start of decentralized ex- changes using a supporting DLT infrastructure. For the purpose of establishing HTLC- based trades amongst possibly dishonest actors, they suggest a

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204305 |

protocol and message format for communicating trade data and technical attributes. They describe the decentralized exchange space as an order-driven market and demonstrate how this protocol might reduce friction during the initial stages of trade by making it easier to find trading partners. They demonstrate how lowering the chance of trades failing can minimize opportunity costs as a result of performance rating. They demonstrate how a reliable exchange rate between cryptocurrencies may be established using a rollingbenchmark rate of verified deals. With the exception of its ability to function cross chain and the inclusion of the idea ofa consortium of market services operators, this solution is comparable to previous protocols that make use of off-chain order books. They demonstrate that the protocol is susceptibleto assaults by dishonest operators who conspire with other network participants, even though it is effective on the premise that the majority of market services operators are honest. Given these results, greater decentralization of the protocol utilizing tools like zero-knowledge proofs to make ex- change rate and reliability score discovery independent ofa central actor or centralized consortium should be the main goal of future study.

c) A Payment Channel Based Hybrid Decentralized Ethereum Token Exchange [3] :

The on-chain layer and the off-chain layer are the two layersthat make up the suggested system framework. For users' assets to be protected, the on-chain layer is essential. The off-chain layer is in charge of matching and placing orders. Although the suggested platform is promising, this study highlights a number of shortcomings that we plan to addressin our subsequent work to improve it: 1) To increase the HEX's profit, more complex token allocation methods should be created. Individual users will receive a higher quality of service and the HEX will be able to serve fewer users by allocating more tokens to each user.2) Because of the way token locks are used to create payment channels, hostile HEX users may start attacks on the system by setting up lots of channels with substantial deposits. In order to stop these attacks, a strong incentive- and-punishment mechanism should be created. 3) To reduce the gas cost associated with opening and shutting a payment channel, more effectivealgorithms should be developed. Allowing the trader to selectthe desired exchange tokens while opening a payment channel is an option.

IV. METHODOLOGY

Proposed system workflow diagram shown in fig. 1 uses reactjs for creating frontend as well as backend of the web application, hard hat for Ethereum development environmentwhich is used to compile and run contracts on development network. It uses smart contracts that automatically runs as theparties to an agreement to fulfill its terms. Metamask is an Ethereum wallet which are used by both parties to perform atransaction.

Detailed working of each section:

a) Creating frontend using react js:

To create a fully functional web application we are using vitejs which is used to setup the development environment in ReactJs. Installation and configuration of tailwind.css Tailwind is Css framework which makes it quicker to write and maintain the code of your application.

b) Creating Smart Contracts:

Required Tools to be installed for creating blockchain includes hardhet (etherium dev env), @nomiclabs/hardhat-waffle ,etherium-waffle, chai, @nomiclabs/hardhat-ethers,Ethers.

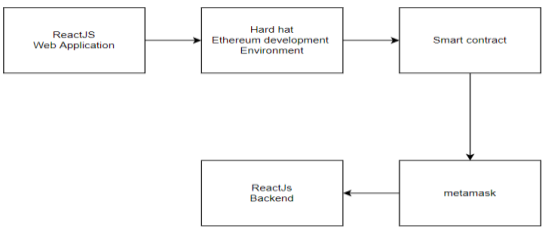

Fig. 1. Methodology Used For Proposed System

c) Transaction.sol code:

Contains business logic of the proposed system which consists of smart contract that defines system with features such as users can deposit or withdraw cryptocurrencies, track users balances and create market orders .

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204305 |

d) Metamask Setup:

We are using metamask which is a software cryptocurrency wallet used for interaction with the Ethereum blockchain. To access the Ethereum wallet via a browser extension, create a Metamask account. Connect metamask to goerli test networkand take the dummy ether from goerli faucet. 1.Create account using Metamask .Switch to goerli test network and add dummy ether using test network through goerli faucet.2.The Dashboard shows the current amount of ethereum present in the account. It also shows the recent transaction logs. It provides the ether scan for the created account.3. Through QR code we can perform transactions. It also showsthe ether scan which consists of digital passbook .

e) Alchemy for testing purposes:

Alchemy is used as web3 development platform . 1)Setting up the currency as an Ethereum. 2)The network selected as goerli.3)Generate the application HTTPS key.

V. ADVANTAGES OF THE PROPOSED SYSTEM

With all the advantages cryptocurrencies have over fiat money and other asset classes, it's difficult to claim that usingor investing in them isn't worthwhile. Several users who desire quick and secure transactions find considerable value in the functionality that many cryptocurrencies offer. Apart from that some of the important advantages of the proposed system are listed below.

a) Protection from inflation
b) Self-governed and managed
c) Secure and private.
d) Currency exchange can be done easily.e)Decentralized.
f)Cost effective mode of transaction.e)Fast way to transfer funds.

VI. CONCLUSION AND FUTURE SCOPE

A decentralized cryptocurrency exchange would enable the vast majority of the world's cryptocurrency users to swap their holdings at some point in the future. In this project, we intended to create and put into practice a system that allows two users to exchange the cryptocurrency Ethereum in a distributed and secure manner. The system is based on the Ethereum platform and runs mostly on smart contracts. Untilthe other side of the transaction from the other party has been made, the smart contract keeps the users' funds. Any kind of Ethereum asset, including the Ethereum cryptocurrency itselfand any tokens based on Ethereum, can be traded through theprogram. Additionally, the transaction history will be shown. To add smart contracts for different currencies like Bitcoin ,Dogecoin etc which will increase the flexibility to perform the transactions. To upgrade the application to perform cross-chain cryptocurrency transactions. Add and upgrade the additional features in Frontend part

VII. RESULT

In essence, we started by building a reactjs frontend. Then, we created a smart contract, which is a set of instructions on which transactions would be carried out. Then, using metamask, transactions from several accounts had to be made. The web application and the blockchain application were linked using web3.
1)Homepage of the web application contains ethereum card provided with options to connect to metamask wallet. Transaction form is provided for users.
2)Metamask notification which prompts the user for selectingthe required account to do the transaction.
3) Metamask notification which prompts the user to confirmwhether you want to connect to the designated account or not.
4) After connecting the account shows the user that theaccount is connected and removes the connect wallet button as the account is already connected.
5) Form for user to provide details of the transaction to be performed. Ethereum Card is shown in which address of the connected account is reflected.
6). After clicking on the send now button a confirmation message is displayed to user. It is metamask notification which prompts the user to confirm the amount of Ethereum which the user wants to transfer.
7) Metamask notification that prompts the user to check whether the selected total amount with charges applied is to be transferred or not.
8) After successful transaction of Ethereum a message is printed in console showing that the transaction performed

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204305 |

was successful.

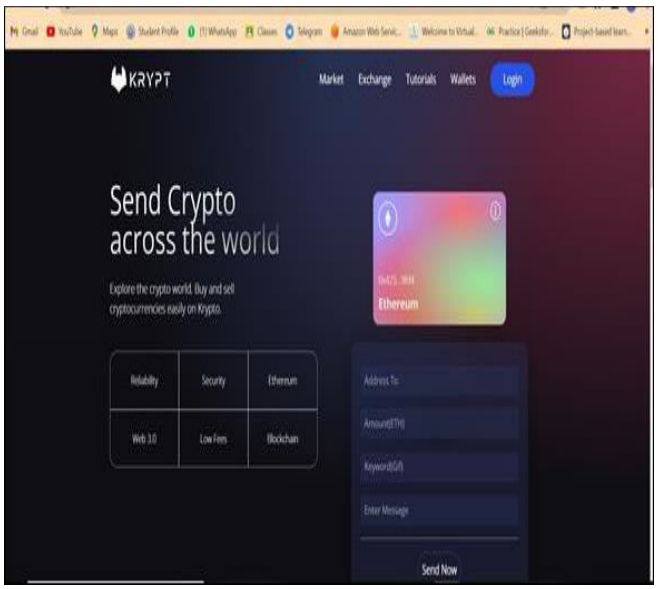

Fig. 2. System Prototype

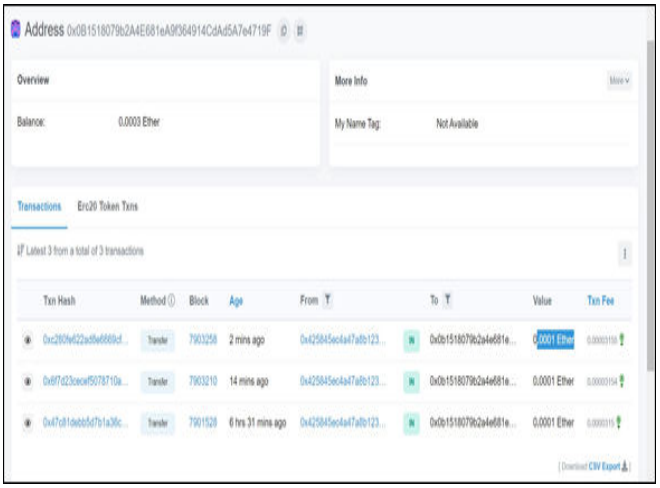

Fig. 3. Cryptocurrency Exchange History

REFERENCES

[1] Dawei Li,Zongxun Tang," AgentChain: A Decentralized Cross-ChainExchange System", 2019. [Online]. Available:https://ieeexplore.ieee.org/document/8887310

[2] Moritz Platt, Francesco Pierangeli, Giacomo Livan,Simone Righi, SYED ATTIQUE SHAH, "Facilitating the Decentralised Exchange of Cryptocurrencies in an Order- Driven Market", 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9223286

[3] Robert Annessi, Ethan Fast, "Improving Security for Users of Decentralized Ex- changes", 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9680483

[4] Hangyu Tian, Kaiping Xue, "A Decentralized Cryptocurrency Exchange Proto- col",2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9478888

[5] Xuan Luo,Wei Cai,Zehua Wang,Xiuhua Li,C. M. Victor Leung, "A Payment Chan- nel Based Hybrid Decentralized Ethereum Token Exchange", 2019. [Online]. Avail- able: https://ieeexplore.ieee.org/abstract/document/8751454

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details