

Decentralized Crypto Exchange with Multi-Deployment

Meehir Choudhary¹, Hrithik Dwivedi², Anas Khan³, Asst Prof. Madhuri Gedam⁴

^{1,2,3} Bachelors of Engineering in Information Technology

⁴Department of Information Technology, Shree L.R. Tiwari College of Engineering, India.

ABSTRACT

Blockchain technology's decentralized structure has completely changed the financial industry and opened the door for creative solutions like decentralized exchanges (DEX). This work presents a revolutionary method of decentralized cryptocurrency exchange, emphasizing multi-deployment as a crucial component. The suggested method makes use of blockchain technology to offer a safe, open, and effective digital asset trading platform. The exchange's multi-deployment feature solves the scalability issues that conventional decentralized exchanges have. The exchange can function simultaneously on several blockchain networks by putting into practice a multi-chain deployment method, which enables higher transaction throughput and lower latency. This architecture guarantees durability and resilience in the face of network congestion in addition to improving the exchange's overall performance.

Keywords - Decentralized exchange (DEX), Multi-chain support, Interoperability, Cross-chain trading, Decentralized finance (DeFi), Smart contracts, Automated market making (AMM), Liquidity pools, non-custodial trading, Token swaps, Multi-chain deployment, Blockchain agnostic, Layer 2 scaling solutions, Atomic swaps, Governance tokens.

I INTRODUCTION

A new era of financial reform began with the introduction of blockchain technology, which disrupted the applications of centralized systems. Among new uses, exchanges (DEX) have become the main players in the digital asset exchange. In this context, this article proposes a new approach to decentralized cryptocurrency exchanges, highlighting an important part called multi distribution. Issues such as maintenance risks, capacity constraints, and security vulnerabilities have long plagued centralized exchanges. The decentralized model of blockchain technology provides customers with transparency, security and asset management; offers practical answers to these questions. The proposed decentralized cryptocurrency exchange expands this framework by offering multiple distribution channels. Thanks to multiple distributions, transactions can be executed simultaneously across multiple blockchain networks, overcoming the scalability bottlenecks they often encounter. This positive sentiment leads to change protection for network collaboration while increasing business. Therefore, users can benefit from a responsive and efficient marketplace that is different from centralized exchanges and distribution. [2]

II PROPOSED WORK

1. How to Create a Decentralized Cryptocurrency Exchange:

In this tutorial, you will combine your JavaScript proficiency with the power of Moralis and 1 inch aggregator to create your own cryptocurrency DEX instance. To make the process as simple as possible, we decided to divide the process into several stages and substages. First, we will walk you through the initial setup. Next, we will show you how to set the header for a decentralized cryptocurrency exchange. Next, we will focus on creating a transaction page that will be the front end for all business-related transactions. Once the frontend is in place, we will walk you through the process of using the backend of a cryptocurrency exchange. Here you will finally learn how to use the above code snippet. [3]

2. Build a Decentralized Cryptocurrency Exchange:

Please provide your Moralis Web3 API key before continuing. Create your free Moralis account this way. Once your account is up and running, you will be able to access your admin area. From here you can copy your API key in two clicks: Then place your key in ".environment". example" file is waiting for you in the "Dex Back" folder. Then rename the file to ".environment". The basis of the NodeJS backend dap is the "index.js" script. This is the file text you need to edit to get the value of the coin. But first, use a new terminal and type "cd" into the "dexBack" folder. Then reinstall the dependencies by entering the "npm install" command. With the dependency present, open "index.js" and use the "getTokenPrice" line of

code in the input section. You also need to modify the "app.get" function, which retrieves the USD token price and feeds it to the "/token Price" endpoint. [2]

2.1 Fundamentals of Building a Decentralized Exchange for Cryptocurrency:

Knowing the theory about decentralized cryptocurrency exchanges and the tools to build them is by no means a must. After all, you might have already built your own decentralized exchange following the above tutorial without a more profound knowledge of the theory.[4] However, if you wish to learn what decentralized exchanges are, how they work, how they compare to centralized exchanges, and the gist of the tools to build a decentralized exchange for crypto, dive into the following sections.[7]

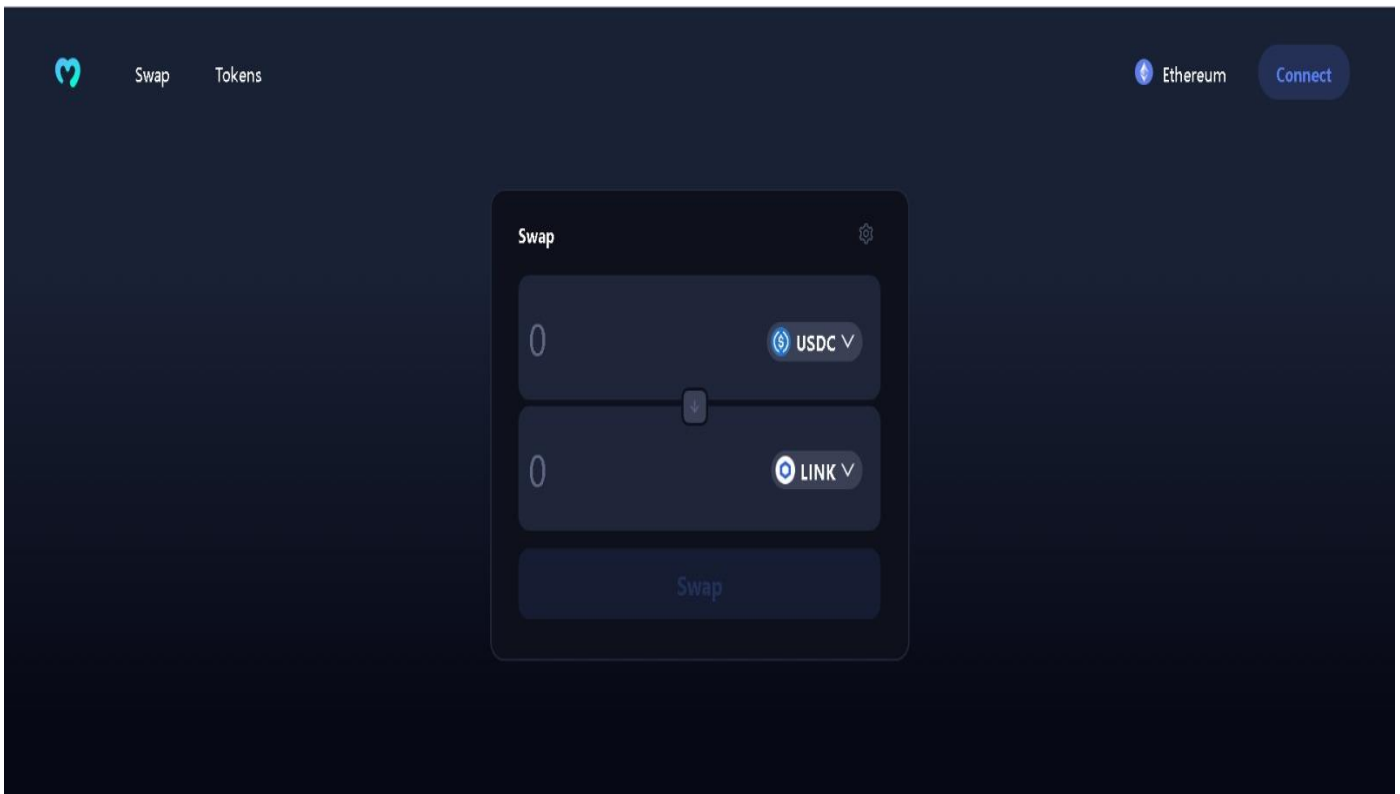


Fig 1

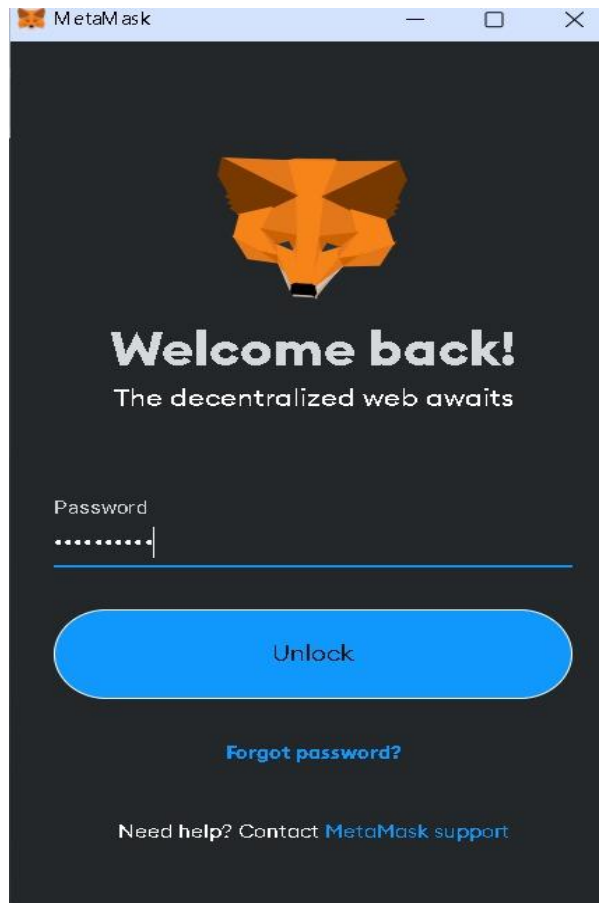
2.2 What is a Decentralized Exchange:

A decentralized exchange (DEX) is a peer-to-peer marketplace where users get to trade cryptocurrency without any middlemen. These types of exchanges are decentralized because there is no central entity involved and, thus, no single point of failure. After all, the backends of DEXs exist on the blockchain. So, thanks to decentralized exchanges, we can execute financial transactions without banks, brokers, payment processors, or any other type of traditional intermediary.[2]

2.3 How Does a Decentralized Cryptocurrency Exchange Work:

DEX options and decentralization levels will vary; But smart contracts are the main technology behind transparent and trustless transactions. Decentralized exchanges rely on "liquidity pools," which are a collection of cryptocurrency assets located downstream of the exchange. Therefore, the pool must be sufficient to complete the buy or sell order. [8] The assets in the pool are owned by investors who make profits by paying transaction fees to users in the "pool." When using an exchange, users must connect their Web3 wallet such as MetaMask. This allows them to control their existence. Once connected, users can exchange assets, invest resources, and perform other DeFi (financial management) transactions. Actual options vary; but the easiest option is a DEX with a token exchange, which you can create in the instructions above. [6] The basic elements that enable the direct exchange of assets are smart contracts. This on-chain software is programmed to execute a pre-order when certain prerequisites are met. Therefore, the transaction is completed or

refunded. It is important to note that token exchanges involve on-chain transactions. Therefore, users must pay a fuel change fee that varies depending on the blockchain network and current demand. [4]



3.1 Decentralized vs Centralized Exchange:

The following list outlines the main differences between DEXs and CEXs:

Decentralization:

CEX: Operated by a central organization.

DEX: Operated by clients and business providers; There is no central management and control.

Custody of assets:

CEX: The exchange has successfully managed access to crypto assets.

DEX: Users have control over their assets.

Impermanent loss:

CEX: You don't have to worry about frequent losses due to high consumption.

DEX: Regular losses are likely to occur when the market changes.

Regulations:

CEXs: Regulated – not anonymous.

DEXs: No KYC and AML standards – anonymous.

Liquidity:

CEXs: Institutional investors and a large user base ensure higher liquidity.

DEXs: Lack of regulatory standards and competition from CEXs reduce liquidity.

Trading options:

CEX: Advanced tools – spot trading, futures trading, etc. Various options trading including.

DEX: Simple transactions - mostly limited to stock markets, mortgages and speculative investments; However, DEXs are constantly changing and new trading options are frequently introduced.

Security:

CEX: Higher risk of hacking and server outages.

DEX: Reduce security risk.

Fig 2

DEXs: It can be tricky for newcomers.

Source of funding:

CEX: Debit and credit card.

DEX: Crypto wallet (e.g. MetaMask).

Trading:

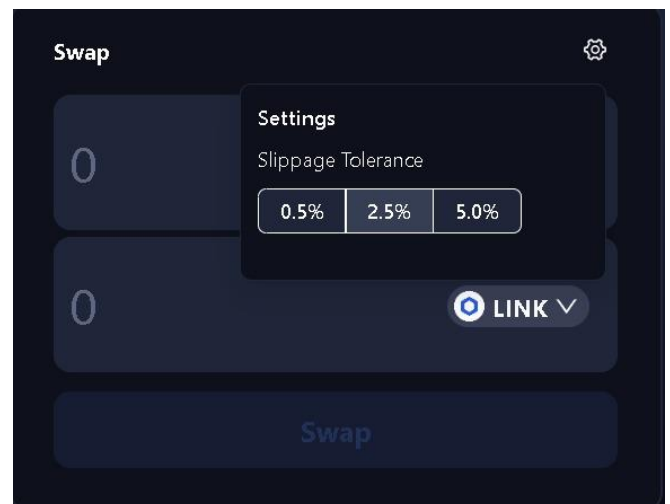
CEX: Order book from central broker.

DEX: Peer-to-peer trading based on automated trading.

Tradable tokens:

CEX: Option token limit.

DEX: There are many options.

**3.2 Tools to Build a Decentralized Cryptocurrency Exchange:**

If you further explore how to build a decentralized cryptocurrency exchange, you'll learn that the above-covered tutorial is not the only way. As such, the tools required to build a DEX also vary. However, when it comes to building a neat-looking and fully functional DEX with minimum effort, the method outlined herein is the way to go. In that case, you need the following tools to build a decentralized cryptocurrency exchange [4]

JavaScript:

o ReactJS framework to cover the frontend.

o NodeJS framework to cover the backend.

- The Moralis Web3 API to fetch on-chain data.
- The 1inch aggregator to implement the exchange features.
- Axios to effortlessly bridge the data from the backend to the frontend.

- The wagmi library to easily implement Web3 authentication.
- CSS for frontend styling.
- MetaMask to connect to your DEX and test its functionalities.
- You need test net crypto faucets to get testnet cryptocurrencies and test your DEX without any actual cost (e.g., a Goerli faucet, Mumbai faucet, BNB faucet, Aptos testnet faucet, etc.).

Of course, if you want to create a more flexible exchange or even introduce some features of the chain, you will need other Ethereum development tools. In this case, you also need to understand smart contracts and smart contracts. You may want to replace the NodeJS backend with Python, in which case you should check the "Web3 Python" option. Now if you want to stay away from Ethereum and EVM along the chain and focus on the Solana example, you should know Solana blockchain application development and related tools.

4 Evaluation:

A decentralized cryptocurrency exchange's security, usability, scalability, decentralization, and overall performance are just a few of the factors that must be considered. The following are important standards for assessing a decentralized cryptocurrency exchange [2]

4.1 Safety:

Smart Contract Security: Evaluate how secure the exchange's smart contracts are. Make sure a thorough audit was conducted on them to find and fix any vulnerabilities.

Custodial Security: Look into the procedures in place to protect user money. Non-custodial solutions should be given priority by decentralized exchanges in order to guard against hacks and illegal access to user assets.

4.2 Usability:

The user interface, or UI: Consider how easy and straightforward the user interface is to use. It takes a user-friendly design to draw in and keep users.

Examine how simple it is for users to create accounts, integrate wallets, and deposit money using the platform's onboarding process.

4.3 Scalability:

Transaction Throughput: Evaluate the exchange's capability to handle a large number of transactions per second. Solutions like sharding or layer 2 scaling may be considered to improve scalability.

Multi-Chain Deployment: If applicable, analyze how well the exchange leverages multi-chain deployment to distribute the load across multiple blockchain networks.

4.4 Decentralization:

Node Distribution: Examine the distribution of nodes across the network. A higher degree of decentralization is desirable one solitary area of vulnerability

Governance Model: Investigate the governance model in place to ensure decisions about the exchange's operation are decentralized and community-driven.

4.5 Interoperability:

Cross-Chain Compatibility: Assess the exchange's compatibility with various blockchain networks. Cross-chain interoperability allows users to trade assets across different blockchains seamlessly

Integration with External Wallets: Evaluate support for external wallets, enhancing interoperability and allowing users to maintain control over their private keys.

III CONCLUSION

In this project, we suggested, created, and put into practice a system that permits two parties to trade bitcoins in a distributed and safe manner. Smart contracts were utilized to power the system's basic functionality, and it was developed on the Ethereum platform. The users' money is held by the smart contract until the other party completes the transaction. We created an Android prototype to illustrate the procedure and prove that switching from Ethereum to Bitcoin and back again is feasible without the aid of a centralized service. Moving to the real blockchain networks is simple and merely requires deployment, even if we ran the tests on the testing ones, testnet3 and Kovan. As part of our future development goals, we want to primarily focus on the next two elements: Use of Multiple Nodes. We will extend the system to employ numerous nodes to eliminate the problem of a single node, since the node might refuse to complete a transaction or the provider could simply go offline. Utilizing several Blockchain Explorers and Oracles. The system currently in use only makes use of one blockchain explorer provider and one oracle. In the same way as the node, if one of the two fails, they could stop transactions from occurring. Using several oracles, each of which queries a separate blockchain explorer, is one potential option.

IV ACKNOWLEDGEMENT

We extend our gratitude to our educational institution, mentors, students, and administrative staff for their wonderful assistance and feedback. We acknowledge the contributions of homomorphic encryption researchers and our dedicated team members; whose commitment and creativity made this project possible. Furthermore, we would want to share our appreciation to the open-source community for providing the necessary tools, libraries, and resources that enabled us to build upon existing technologies and realize our vision for a cryptocurrency exchange that is decentralized with multi-deployment capabilities. We are also grateful to our project supervisor/advisor for their guidance, support, and valuable feedback at every stage of the project. Their insights helped steer us in the right direction and ensured that we stayed on track to achieve our goals.

V REFERENCES

- [1] Ellis, Juels, and Nazarov. "Chainlink: A decentralized Oracle Network" *Economics Letters* 150 (2017):69.
- [2] Jang, Huisu, and Jaewook Lee. "An empirical study on modeling and prediction of bitcoin prices with Bayesian neural networks based on blockchain information." *Ieee Access* 6 (2017): 5427-5437.
- [3] I. J. Pérez, F. J. Cabrerizo, S. Alonso, Y. C. Dong, F. Chiclana, and E. Herrera-Viedma, "On dynamic consensus processes in group decision making problems," *Inf. Sci.*, vol. 459, pp. 20–35, Aug. 2018
- [4] Mao, Xiao-Bing, Min Wu, Jiu-Ying Dong, Shu-Ping Wan, and Zhen Jin. "A new method for probabilistic linguistic multi-attribute group decision making: Application to the selection of financial technologies." *Applied Soft Computing* 77 (2019): 155-175.
- [5] Tripathi, Surendra, K. K. Mishra, and Shailesh Tiwari. "Modified Differential Evolution Algorithm with Updated Mutation and Crossover Operator." *Journal of Multiple-Valued Logic & Soft Computing* 38 (2022).
- [6] Dong, Jiu-Ying, Yang Chen, and Shu-Ping Wan. "A cosine similarity based QUALIFLEX approach with hesitant fuzzy linguistic term sets for financial performance evaluation." *Applied Soft Computing* 69 (2018): 316-329.
- [7] Merkle, R. (April 1980). Protocols for public key cryptosystems. Symposium on Security and Privacy, IEEE Computer Society, , 122-133.
- [8] Nakamoto, S. (2011). Bitcoin: A Peer-to-Peer Electronic Cash System. Project, N. (2011). Retrieved from <https://github.com/namecoin/namecoin>.
- [9] S. H., & W. S. (1991). How to time-stamp a digital document., *Journal of Cryptology* vol 3 no 2 , 99-111.
- [10] Alkurdi. The rise of decentralized cryptocurrency exchanges *Forbes* (2020)
- [11] AllowayT. et al.Hayden Adams explains Uniswap and the rise of DeFi (2021)