WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Decentralised Token Exchange

[1]Prof. Shweta Shah, [2]Rajat Vyawahare, [3]Harshal Hole, [4]Mahesh Zalte, [5]Shashwat Biyani

[1,2,3,4,5]*Dept. of Computer Engg, Pune Institute of Computer Technology,* Pune, India.

Abstract—

In today's technology world security is of utmost importance. Blockchain technology helps solves this problem by removing third party people and making the process secure. The first completely digital assets that asset managers have included are cryptocurrencies. The trend of financial institutions adding cryptocurrencies to their portfolios has grown in recent years. The blockchain technology adopted in using the cryptocurrency has raised the eyebrows within the banking sector, government, stakeholders and individual investors. Cryptocurrency is expected to be the future currency that can replace the current fiat currency worldwide. This project gives an overview of the origins and principal characteristics of the cryptocurrency market as well as price dynamics,capitalization market size and trading volumes

***Index Terms*—Blockchain, Cryptocurrencies, Ethereum, Smart Contracts, Token, Consensus Algorithm**

I. INTRODUCTION

A decentralised blockchain network, such as Ethereum, serves as the foundation for a platform called a decentralised exchange, or DEX. It enables users to transact in cryptocurren- cies and other digital assets without the aid of a middleman or centralised authority. Contrast this with centralised exchanges, which have a single company in control and demand that customers deposit their funds with the exchange. Decentralized exchanges also provide greater trade autonomy and trans- parency. Since transactions are tracked on a public blockchain, it is simple to follow the movement of assets and make sure the exchange is fair.

A. Motivation

For transferring the tokens we require a secure platform which must be easy to handle. There is need to develop such platform because in centralised way we have to give fee as well as depend on third party for exchange of tokens. This platform will help to create our own token and transfer it with other tokens without third party interventions. As there is no third party interventions it will be secure. We can trade, buy and sell tokens using these platforms.

B. Problem Statement

To develop a decentralised application platform for the Blockchain-based trading and token exchange. It must be user-friendly, secure, and independent. Create a platform that uses the proof-of-work consensus algorithm and can exchange tokens efficiently with very low response time using the Ethereum blockchain.

C. Project Scope

The scope of the project is to securely storing records such as crypto tokens and facilitating efficient exchange of such tokens without third party interventions.

D. User Classes and Characteristics

Our application can be used by different types of users for different use cases or purposes. General users those users who wish to visit the platform and to see the functionalities of it. They must have an account on metamask wallet to see all the functionalities.

E. What is Blockchain?

A distributed digital ledger of transactions is known as a blockchain. It holds copies of all executed transactions or events that are shared throughout the blockchain's partici- pating nodes. Blocks are separated into a blockchain. Each block includes encrypted information about the transaction, the sender and recipient, and the hash of the preceding block. The blockchain gets its name when the block is then chronologically added to the chain. Blockchain is trustworthy and immutable. Blockchain is decentralised, distributed, peer- to-peer, not controlled by a single entity, and requires no third party for verification.

CONSENSUS ALGORITHMS

- Proof of Work (PoW): Miners will need to use a lot of computing power to solve a mathematical puzzle for each block generation. The next block will be mined by the first node to solve the puzzle.
- Proof of Stake (PoS): Validators stake some of their own coins in a Proof of Stake (PoS) transaction. If a validator finds a block that they believe can be added to the chain, they will validate it by placing a bet on it. Rewards are given based on the validator's bet to incentivize them. Their payout will rise in proportion to their bet. A validator is ultimately selected to create a new block based on their financial stake in the network.

F. What is Ethereum?

Developers may write and use smart contracts on a variety of blockchain platforms. An international, open- source platform for decentralised applications is Ethereum (@ https://ethereum.org/) (dapps). One of the top programmable blockchains, Ethereum was introduced in 2015 and may be used to create new blockchain applications including decen- tralised markets, games, financial apps, and cryptocurrency wallets. Ethereum has a native cryptocurrency called Ether (ETH), which is comparable to Bitcoin, like other blockchains. Ethereum is consists of:

a. The Ethereum Virtual Machine (EVM) is a state machine that lets you run programmes.

b. Solidity: an EVM-based programming language for creat- ing smart contracts, sending and receiving digital tokens, and storing states

c. Gas: Each smart contract on the Ethereum blockchain is processed by a single miner, and the resulting block is then added to the network. Any smart contract on the EVM must be paid for with gas in order to be executed since miners must be compensated for their efforts. Any smart contract you build must have a gas cost specified before it can be executed.

A user requires a wallet address with some ether in it in order to transact on the Ethereum network (ETH). After establishing a connection to the network, one can initiate a transaction and pay a modest fee to have it added to the blockchain. Gas is the name given to this transaction cost. To execute this transaction, miners—a group of the network's nodes—compete. The Ether is given to the miner who completes this transaction.

It is crucial to remember that while using the blockchain to retrieve data is free, using it to write data is not.

G. What are Smart Contracts?

With the Ethereum Virtual Machine, we can run code from smart contracts using the Ethereum blockchain (EVM).

The business logic of our dapp is contained in smart contracts. It is their responsibility to read from and write to the Ethereum blockchain. Solidity, a programming language that resembles JavaScript, is used to create smart contacts.

II. FUNCTIONAL REQUIREMENTS

A. Create Token request

Developer can create the token and decides the value of the token and can exchange it with other tokens.

B. Exchange Token

Users can exchange the tokens with other tokens on Ethereum Blockchain.

C. Transaction records

Using the Ethereum API we can withdraw, deposit and display balance and account details.

D. Communication Interfaces

The user needs to communicate with the Metamask wallet which holds the Ethereum account of the user. It is required to validate all the transactions made through the account.

III. NON FUNCTIONAL REQUIREMENTS

A. Performance Requirement

- User satisfaction:

It evaluates if the application and services offered meet or exceed the customer's expectations.

- Accuracy:

Accuracy is depends on the how well the system performs the transaction.

- Average response time:

The time it takes the Application Server to respond to a user's request and return the results is known as the average response time. Minimum response time would be appreciated.

- Application Availability:

The degree to which an application is operational, func- tional, and usable for completing or satisfying a user's or business's requirements is referred to as its availability.

B. Safety and Security Requirements

- User Account Security:

Account address and information related to it is well secured by the metamask wallet. In order to get back your account, you should remember Security Recovery Phase which was given at the time of account creation.

- Metamask credential Requirements:

In order to successful login into your Metamask wallet a password of minimum eight character should be remem- bered which was given at the time of account creation on it.

C. Software Quality Attributes

- Reliability:

The possibility that a software package will carry out a function (provided by particular requirements) over a specified amount of input trials under a defined number of input circumstances in a specified time frame is the defined as reliability.

- Correctness:

Software system correctness is determined by the programme code's adherence to specifications and the independence of the system's actual application.

- Robustness:

Robustness lessens the effects of operational errors, in accurate input data, and hardware breakdowns.

IV. SYSTEM REQUIREMENTS

A. Database Requirements

We have the following data that needs to be stored:

- Ethereum address of user.
- Token information.

This data is stored in Ethereum Blockchain.

B. Software Requirements

- Solidity
- Javascript
- React.js: 18.0.0
- Node.js: 18.12.0
- Redux: 4.2.0
- Ethers: 5.35.4
- Hardhat: 2.10.1
- Blockchain: Ethereum
- VS Code
- Chrome Browser

C. **Hardware Requirements**

- Processor (i5 or higher): A fast and efficient proces-sor is needed to perform transaction fasts on Ethereum blockchain network.

- RAM (8GB): Helps to boosts the performance of system.
- GPU : Integrated or dedicated GPU sufficient as there is small scale of processing of data on client end.

D. Analysis Model

There are several models to choose like waterfall models, iterative models, and spiral models, but the agile model is one of the best. Our project contains several modules and each module depends on each other, so it is recommended to use agile methods when developing software. This methodology also allows the project to be delivered in parts and modified according to the user's requirements at any point in the SDLC cycle.

V. SYSTEM DESIGN

A. Architecture diagram

The system components are depicted in an architecture diagram along with their physical implementation.It shows system structure, its associations and relationships.

B. Data Flow Diagram

A data flow diagram shows how information is passed through any process. It displays routes between each des- tination, data inputs, outputs and storage locations, using predefined symbols such circles, rectangles, and arrows as well as text labels.

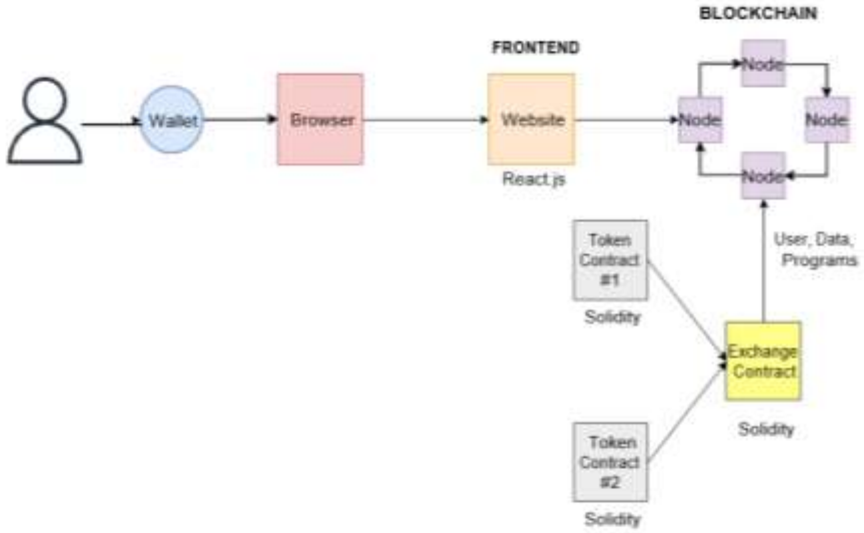

Fig. 1. Architecture diagram

C. Use Case Diagram

A use case diagram in the Unified Modeling Language (UML) can condense the description of your system's users (sometimes referred to as actors) and their interactions with the system. You'll need a specific set of connectors and symbols to construct one.

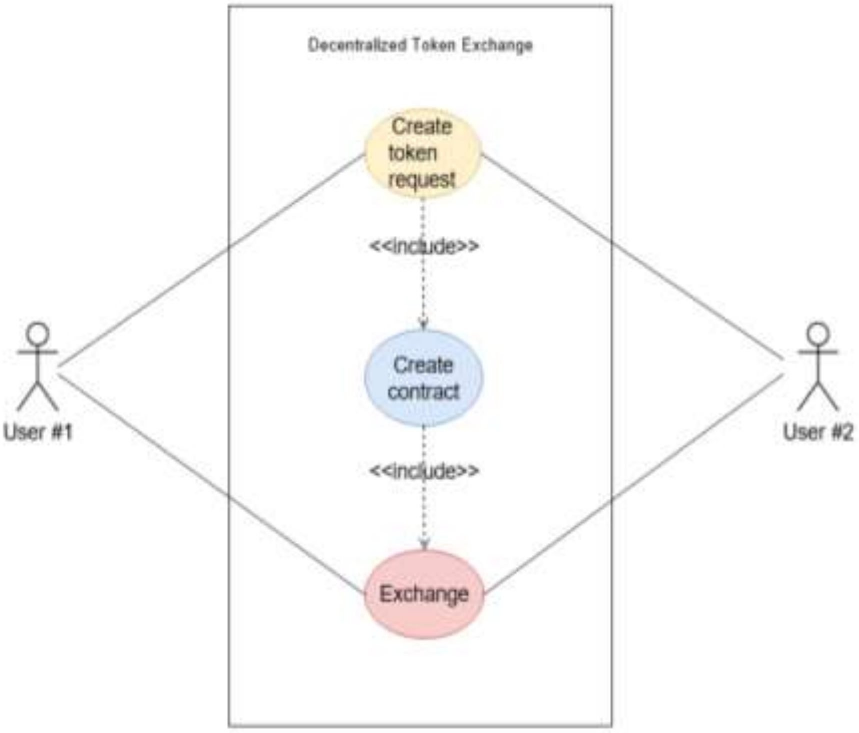

Fig. 3. Use Case Diagram

D. ER Diagram

An Entity Relationship (ER) Diagram is a form of flowchart that shows the relationships between ”entities” like people, things, or concepts within a system. ER Diagrams are most frequently used in the disciplines of software engineering, business information systems, education, and research to build or troubleshoot relational databases.

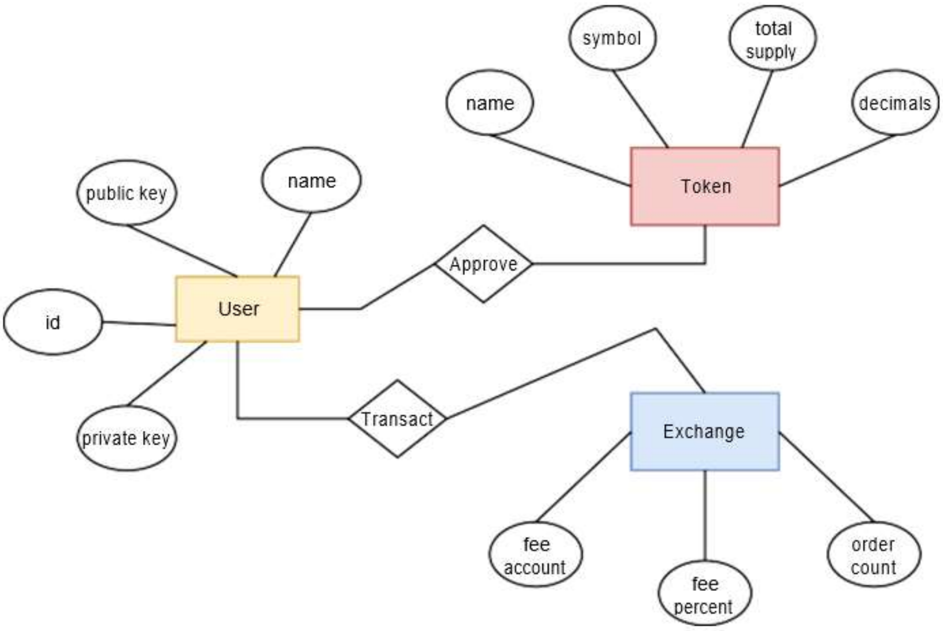

Fig. 4. ER Diagram

E. Class diagram

One of the most helpful forms of diagrams in UML are class diagrams, which accurately depict a system’s structure by modelling its classes, properties, operations, and relationships among objects.

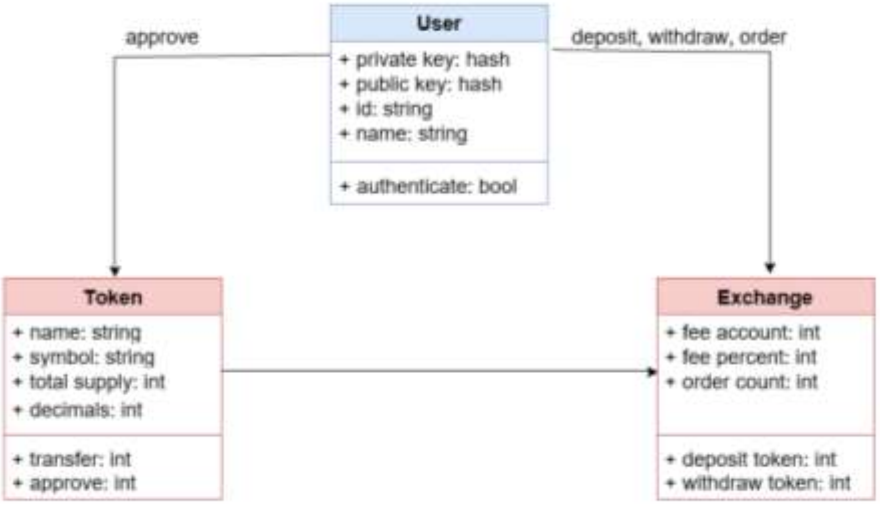

Fig. 5. Class diagram

ACKNOWLEDGMENT

We like to sincerely express our heartfelt gratitude to our mentor Prof. Shweta Shah for providing us with all the support and advice we required. We are incredibly grateful of her wonderful support. We are also grateful to Dr. G.V. Kale, Head of Computer Engineering, Pune Institute of Computer Technology for her valuable suggestions and support.

REFERENCES

[1]. Bhuvana, R., Aithal, P. S. (2020). RBI Distributed Ledger Technology and Blockchain. A Future of Decentralized India. International Journal of Management, Technology and Social Sciences (IJMTS), 5(1), 227- 237.

[2]. Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L.,Brooks, R., 2016. A brief survey of cryptocurrency systems, in:2016 14th annual conference on privacy, security and trust (PST),IEEE. pp. 745–752.

[3]. Chaum, D.: Blind Signatures for Untraceable Payments. In Chaum, D., Rivest,R.L., Sherman, A.T., eds.: Advances in Cryptology, Boston, MA, Springer US(1983) 199–203.

[4]. Pop Claudia, Tudor Cioara, Marcel Antal, Ionut Anghel, Ioan Salomie, and Massimo Bertoncini. ”Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids.

[5]. Pop et al., ”Decentralizing the Stock Exchange using Blockchain An Ethereumbased implementation of the Bucharest Stock Exchange”, 2018 IEEE 14th International Conference on Intelligent Computer Communication and Processing (ICCP), pp. 459- 466, 2018.

[6]. Chris Dannen, “Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners”, Published by Springer Science+Business Media New York, ISBN: 978-1-4842- 2534-9.

[7]. V. Y. Kemmoe, W. Stone, J. Kim, D. Kim and J. Son, ”Recent Advances in Smart Contracts: A Technical Overview and State of the Art”, IEEE Access, vol. 8, pp. 117782- 117801, 2020.

[8]. R. Nair and A. Bhagat, ”An Application of Blockchain in Stock Mar- ket” in Transforming Businesses With Bitcoin Mining and Blockchain Applications, IGI Global Publisher, pp. 103-118, 2020.

[9]. M. Pincheira, M. Vecchio, and R. Giaffreda, “Rationale and practical as- sessment of a fully distributed blockchain-based marketplace of fog/edge computing resources,” in Proc. 7th Int. Conf. Softw. Defined Syst. (SDS), Apr. 2020, pp. 165–170, doi: 10.1109/SDS49854.2020.9143892.

[10]. Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho, and H. Y. Lam, “Blockchain-driven IoT for food traceability with an integrated consen- sus mechanism,” IEEE Access, vol. 7, pp. 129000–129017, 2019, doi: 10.1109/ACCESS.2019.2940227.

[11]. Ethereum. What is Ethereum? The Foundation for Our Digital Fu- ture. Accessed: Aug. 30, 2020. [Online]. Available: https://ethereum. org/en/what-is-ethereum.