

Jerry Token Farm - A Blockchain Based Decentralized Finance Application

Shivam Sunil Bhosale¹

¹UG Student, Department of Computer Science Engineering, SRM Institute of Science and Technology, Chennai, Tamil Nadu

Abstract - The current money lending system is based on exchange of fiat or cash currency wherein the lender gets back their money along with the added interest after agreed duration of time period. In this paper, using the Ethereum based solidity programming language, I created a cryptocurrency lending application over blockchain network, where the user can stake 'mDAI' token for a particular period of time. After the stipulated time period ends the user can un-stake their 'mDAI' tokens and can earn 'Jerry Token' - which is a token created using Ethereum smart contract, as a reward for staking.

Key Words: Cryptocurrency, Blockchain, Ethereum, DeFi, DAI, Tokens.

1. INTRODUCTION

The present financial institutional network is a centralized system consisting of middlemen such as brokerage firms and banks. There are many problems with the current state of the system such as the number of people using it has increased tremendously in the recent years which in turn has delayed the decision making process due to presence of the hierarchy in the system. Also as the system is centralized the decision making power is limited to a few thereby allowing them to abuse the same in their own favour whilst crippling the weaker sections of the strata. The centralized financial system provides an illusion of being more secure wherein in reality is been dented with frauds. A Decentralized financial system would get rid of the hierarchical ladder in the financial system and would distributed the power amongst those who are engaging in it thereby eliminating any threat associated with the financial system. The Decentralized financial system is based on blockchain network and is called as DeFi.

1.1 Cryptocurrency

Cryptocurrencies are a form of a digital currencies which are built over blockchain technology which makes them decentralized and therefore unlike any traditional currency like USD or INR they are not issued by any central governing body or authority. This feature makes them immune to manipulation. The transfer of cryptocurrency relies on P2P network, and therefore

could be transfer for one wallet to another without the third party interference.

1.2 Distributed P2P Network

In a distributed P2P system, there are many computers which are interconnected and the blockchain is copied in every device in the system. If any change is made in the block chain for example: If a block is added in the block chain using any device in the system, all the other connected devices in the system would be notified about the change and then the exact change is ben made in those devices. The devices in the system constantly check its peers blockchain to see whether its same to there's and therefore if anyone hacks any of the device to make any change in the block of the blockchain it would be caught by the other devices in the system and a message would be sent to the hacked system to restore itself in its original state.

1.3 Decentralized Finance (DeFi)

Decentralized Finance or DeFi is a system where the financial services and products are welcoming to anyone with Ethereum and a proper internet connection. The centralized system is absent in this therefore problems such as payments getting denied or blocked can be eliminated, the DeFi system also ensures that the services are fast and safer.

1.4 DAI

The DAI coin is a decentralized cryptocurrency which is built on Ethereum (ERC-20 token) and is fixed against the USD, it is a overcollateralized token , which means if we have \$1 worth of ETH locked up we can borrow \$0.66 worth of DAI, when the borrowed DAI is payed back the ETH is released automatically. There are many exchanges where we can directly buy the DAI coin. In the project we will be using mock DAI or 'mDAI' which is an exact replica of actual DAI token.

2. LITERATURE SURVEY

In [1], the authors have discussed about time-stamping any digital document such as Image, video, audio, text, which servers as a basic idea behind the concept of a

blockchain. The features discussed in the paper match with those of the current blockchain system. The paper states a method which could be used to maintain a complete digital privacy of the documents without any intervention of a time-stamping service.

The authors in [2], have analysed the requirements for the security properties needed to build blocks for the bitcoin-like cryptocurrency system. The authors have also reviewed privacy tactics for to accomplish the proposed system requirements. The focus of the paper is to evoke the people with the in-depth understanding of security and privacy related to the blockchain.

Vitalik Buterin, the creator of Ethereum cryptocurrency talks about the establishing a next-gen smart contract and a Decentralized Application (Dapps) platform in his Ethereum white paper [3]. Unlike Bitcoin which can just be used as a form of currency. Ethereum provides a larger functionality allowing users to create smart contracts and Daaps. It should be noted that the Ethereum uses Keccak-256 hashing algorithm instead of traditional SHA-256 hashing algorithm, predominantly used in Bitcoin blockchain.

In [4], the author have talked about creating a peer-to-peer system which would be used to carry out online transaction without the intervention of a third party such like the current financial institutions. The author has created a digital currency known as 'Bitcoin', which could be used to do the above mentioned process.

The author in [5], highlights the opportunities and risk associated with the DeFi system and proposes to built a multilayered framework which could be used to analyse DeFi based services such as Decentralized exchanges and debt markets.

The paper [6], explores the Decentralized finance primitives and have classified different DeFi protocols with respect to the operations provided by them. The authors have also talked about technical and economical security of the DeFi protocols. The authors have covered a broader challenges with regards to the compatibility risks, governance and anonymity.

3. PROPOSED SYSTEM

The decentralized finance app created uses two tokens 'mDAI', where m stands for mock which is similar to that of the existing 'DAI' token and 'Jerry Token' which would be a reward to be given for staking. The Jerry Token is been created using the Ethereum smart contract. This decentralized finance platform allows the person staking to stake the 'mDAI' token for a stipulated period of time. The deposited amount could be then used to be loaned out

to others. After the period ends the admin of the DeFi application could issue 'Jerry Token' once the user unstakes their 'mDAI' token. This way of loaning out money will skip the traditional banking centralized banking process thereby making it more faster and easier to await flash loans. This is known as yield farming in the world of cryptocurrency.

4. METHODOLOGY

Like any other conventional web application, the first step to this would be creating a website. The user interface of website is created using the HTML, CSS and JS. The whole system is deployed on a third smart contract which will handle all the transaction between the users and the interface. Now instead of accessing any backend server the website will communicate to the blockchain where all the data for the processing will be stored. The code for the blockchain is stored in smart contracts created using the solidity programming language, the smart contracts are immutable which means once deployed the contracts cannot be tampered or changed in any way. Any new data added to the blockchain would be stored permanently.

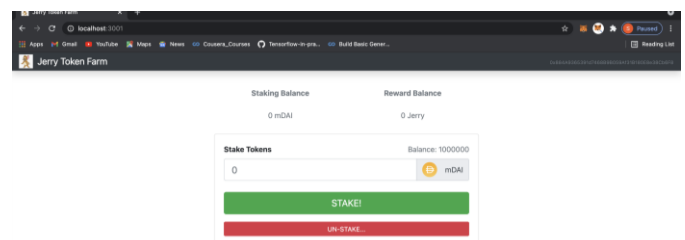


Fig -1: Jerry Token Farm Interface

Now, the user who is the lender will stake a particular amount of 'mDAI' token from his wallet into the DeFi application. To do so the user will have to connect the wallet to a third party application such as MetaMask. The user will have to deposit some Ethereum in the MetaMask wallet which would be used as a gas fee to carry out the transactions. Once this is done, the amount staked will be displayed above.

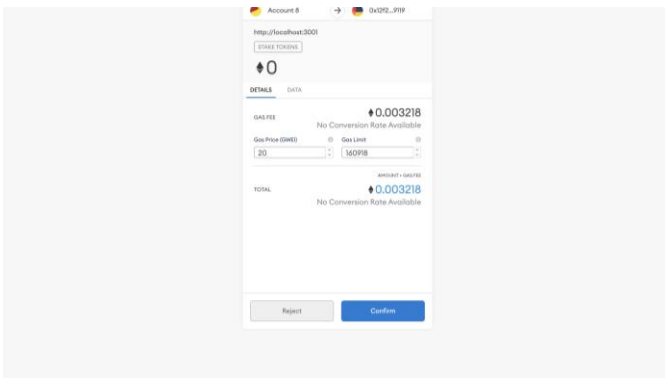


Fig -2: MetaMask interface used to carry out gas fee

Since we are using a mock currencies instead of the actual cryptocurrency, we will be connecting our MetaMask wallet to Ganache Ethereum wallet using the private key and connecting the MetaMask to the localhost of the Ganache system which is usually port 7545. Ganache provides mock Ethereum which could be used to test the application in the productions.

The admin can now run a script which would issue Jerry tokens are reward to those who have staked their mDAI tokens. Once the reward is received the user can un-stake their mDAI token and to do so they will again have to pay the gas fee via their MetaMask wallet.

In an actual scenario the gas fee goes towards the network of miners who monitored and verify every transaction which is made in the blockchain network.

5. TOOLS USED

Given below are the major tools used to built the DeFi application.

5.1 MetaMask

Developed by ConsenSys Software Inc, it is cryptocurrency wallet which is used to store different tokens as well as it provides a medium where these tokens can be exchanged. MetaMask installed in the web browser and in mobile application.

5.2 Ganache

It is a tools which contains mock Ethereum that could be used to test decentralized application in their entire development cycle. The Ganache contains different wallets with 100 mock ETH in each of them which can be accessed using the private key.

5.3 Solidity

Solidity is a programming language made specifically to carry out smart contracts. The languages is highly inspired by JavaScript and Python. Being an object-oriented language it supports all the features like inheritance and has many pre-built libraries.

5.4 Truffle

Truffle is an open-source development environment which is used to test blockchains using the EVM - Ethereum Virtual Machines

6. CONCLUSIONS

The blockchain technology is certainly a newer concept and has a tremendous potential in future when it comes to decentralisation of major systems. It can be said that at this point of time blockchain could be easily compared to the internet of 90s in terms of popularity and development.

At this stage, centralized finance still maintains a major chunk in the market shares when compared to the decentralized finance. But with the growth of the cryptocurrencies in the future decentralized finance is catching up with the existing system.

Decentralized financial systems come with the promise of dividing the power from one single authority to its users and focuses on idea to create an automated, open-source and transparent ecosystem. To overcome the current bureaucratic centralized system, the DeFi crypto based system is certainly one of the most potential alternative.

REFERENCES

- [1] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no2, pages 99-111, 1991.
- [2] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2019.
- [3] Vitalik Buterin, Ethereum White Paper-A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM, 2013.
- [4] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," ACM Computing Surveys (CSUR), vol. 52, no. 3, pp. 1-34, 2019.
- [5] Fabian Schär, Decentralized Finance: On Blockchain-and Smart Contract-based Financial Markets. 2020.
- [6] Sam M. Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, William J. Knottenbelt, SoK: Decentralized Finance (DeFi), 2021.