



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CATENA DECENTRALIZED BANK

Sibi Charavarthy P, Jeevithan S, Sidharthan J Supervisor : Mr. R. Muralidharan

Department of Computer Science and Technology, Dr.Mahalingam College of Engineering and Technology, Pollachi

Abstract : Decentralized financial applications enable users to perform financial transactions in a peer-to-peer fashion. Thus, it eliminates the risk of single point of failure and various other cyber threats such as Man in the middle attack. However, till date only the fundamental transactions and staking have been widely used in the crypto field when it comes to actual crypto banks. Hence, the proposed system aims at developing a stimulation of bank with extended functionality to make it as close to a real time bank as possible. The proposed system makes use of digital assets for this purpose rather than real world objects. It also supports user auctions. To demonstrate the use of the custom tokens of the bank, a course platform is introduced where the user can access the courses for free, but have to pay a certain amount of tokens to obtain certificate on course completion.

Key Words: Decentralized Finance, Non-Fungible Tokens, Decentralized Lending System

1. INTRODUCTION

Blockchain network is a distributed ledger which is shared among all the node in the network. When a new transaction takes place in the blockchain network that transaction get recorded in a block then the block id validated by the miner either in proof of stake or proof of work method, In proof of stake the validator will validate the transaction, In proof of work miner solve the complex mathematical puzzle and validate the hash in order to add the block to the network. Once the block is added to network then the data in the block cannot be changed this makes the blockchain network more secure and reliable. But in some cases if a hacker has more than 51% of total hash power of the network then the hacker can modify the data, but in

major networks like bitcoin, ethereum or ravencion acquiring 51% hash power is merely impossible

Digital assets and crypto currency have become a major topic of internet interest in the past years. The main reason for this huge increase in popularity is that Block chain technology allows for seamless peer-to-peer exchange between users. This eliminates the risk of being de-banked, or being restricted from withdrawing/using the bank funds due to some national crisis, sanctions, etc. Decentralized finance is a modern banking paradigm that utilizes crypto currency for its transactions. The main difference between DeFi and CeFi is that DeFi is fully automated by smart contract, hence is secure, decentralized, whereas CeFi is centrally controlled by some authority and not as much secure as DeFi. DeFi stock exchange has grown up to 47% in the past year. Decentralized finance applications secure their public ledgers by distributed consensus and radical transparency.

Non-fungible tokens or NFTs are digital assets which are used to represent real world items like artwork, music, videos or in-game assets like unique avatars. NFTs are unique, tamper-proof and cannot be duplicated in the block chain network.

These block chain technology has the ability lay path to new business models that were previously not viable. Platforms utilizing decentralized finance are borderless and can be used worldwide while the centralized finance applications / processes are restricted to specific geographic locations.

2. KEY TECHNOLOGIES

2.1 Decentralized finance

Decentralized finance or DeFi uses blockchain technology as a core technology like other crypto currencies. This allows users to conduct business without any organization in middle this helps in eliminating the service fee which is charged by banks, users can hold their assets more secure than centralized finance, users can use their money/assets from any part of the world

2.2 ERC-20

The ERC 20 standard interface has been implemented in this project for creating a custom token. The ERC tokens exist on the ethereum platform. The ethereum platform consists of,

- Blockchain capable of running transactions
- Virtual machine capable of running smart contracts

Tokens live on ethereum blockchain which benefit from this technology. They aren't independent and depend on ethereum's blockchain and platform. Ethereum network can support other custom tokens. These tokens can represent and can be exchanged for currency.

They can also represent,

- Shares of a company
- Loyalty points
- Gold Certificates

A token can be created by a smart contract. These contracts are responsible not solely for the token creation but also for,

- Handling transactions
- Keeping track of balance of each token holder

Some amount of ether has to be sent to the smart contract which will then provide with some amount of tokens in return. So to create a token, a smart contract is created which can create tokens, transfer them and keep track of balances of the token holders. The token creation and deployment also does involve some risks since it cannot be changed anymore once it is deployed to the network.

2.2 DIGITAL ASSETS

In recent days the use of internet and blockchain technology have raised so much in this era the digital assets like NFTs had grown tremendously leading to high demand in digital asset market

This digital can be any thing like artwork, painting, music or video which represent the real life entity.

2.3 DEVELOPMENT PLATFORM

“Truffle and ganache” is used as the local development platform. It comes the test account with which we can test the smart contract locally. The mocha and chai frame work are used to test the smart contract.

2.3 TESTING PLATFORM

Here mocha and chai a javascript based testing framework is used to test the smart contract. These frameworks use test driven development in this process the code gets tested quickly

3. IMPLEMENTATION

The implementation of this project is divided into

- Project planning
- Developing and testing the smart contract
 - Migration
 - Token
 - Bank
- Modules
 - Bank
 - Deposit
 - Withdraw
 - Transfer
 - Barrow
 - Image asset
 - My asset
 - Auction
 - Asset loan
 - Online course platform
 - Learning
- Developing and testing the react app

3.1 BANK

3.1.1 DEPOSIT

In this module the users can deposit their crypto holding in the bank this will be get stored in the address of smart contract. In this the deposit function is invoked on completion of the validation process the crypto transferred from users wallet to banks smart contract address

3.1.2 WITHDRAW

Here the users of bank who deposited crypto can withdraw. The withdrawal amount either equal or less than the amount that user have deposited in the bank. On the successful validation the crypto from the bank will be transferred to user's wallet.

3.1.3 TRANSFER

In this module the user can transfer their crypto holding in bank to other users inside the bank for this both users must use the bank and the sender must posses equal or less amount in his account to make a transfer

3.1.4 BORROW

With this module the users of ban can get tokens as loan from bank by giving the crypto as collateral with the tokens the users can avail the service of the platform like online education portal. The users must pay off the loan on time in order to get back their crypto collateral back

3.2 IMAGE ASSET

3.2.1 MY ASSET

In this interplanetary file system is used. ipfs is a distributed file system which helps in peer-to-peer file sharing. In this the user can upload their assets such as artwork this get store in Interplanetary File System. In which the asset is hashed with unique hash and stored and retrieved with hash generated

3.2.2 AUCTION

In auction module the user can host auction for the asset which they hold. While auction any one can bid for the asset, on completion of the auction the highest bidder will get the rights of the asset and the crypto from the bidders account will be transferred to the hosts account and rest of the bidder will get back their crypto on end of the auction

3.2.3 ASSET LOAN

Here the users can get loan based on the value of their asset which the user willing to give as collateral. Here the bank will provide up to 60% of the value of the asset as loan upon successful validation. The user needs to pay back the loan to get their asset back. If the user fails to pay off the loan the asset will be auctioned with base price as the value of the asset this will help the bank to recover the loss made by the user

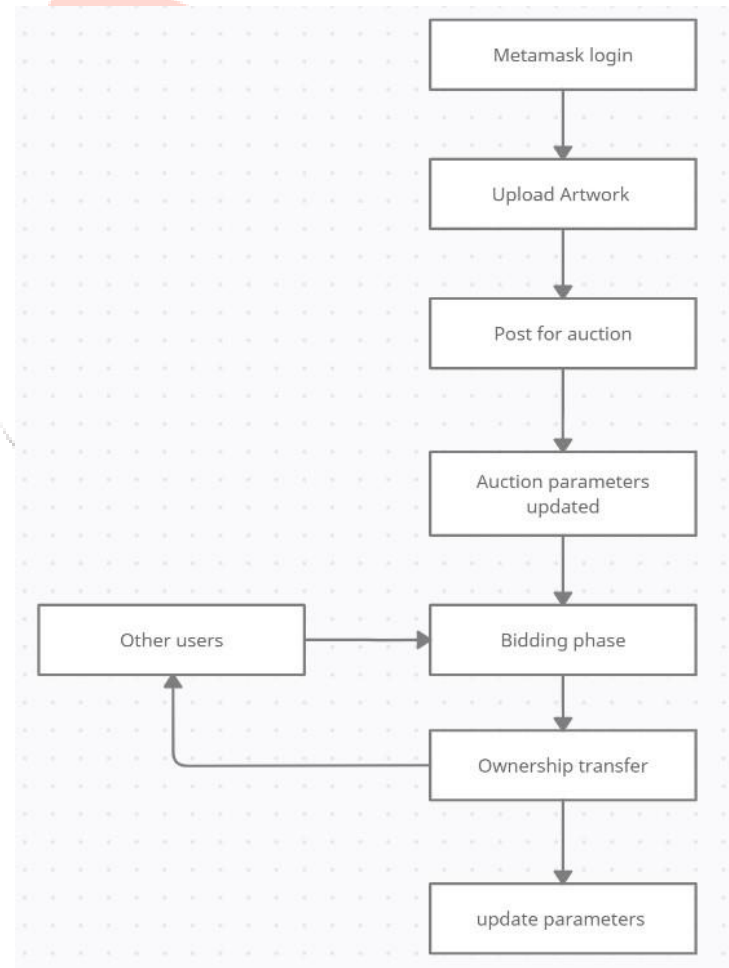


Fig 5.1 Auction system flow diagram

3.3 ONLINE COURSE PLATFORM

3.3.1 LEARNING

In the learning module the user is provided with tutorial videos, which the user can watch for free any number of times. If the user needs certificate as a proof of his knowledge the user must buy the token from the bank and pay with token to get the certificate this certificate will be stored in the interplanetary file system which is the distributed file system the file is splitted into small chunks which is then hashed and stored in the network.

Users can view their certificates in the certificates tab these certificates are retrieved from the network by generated hash

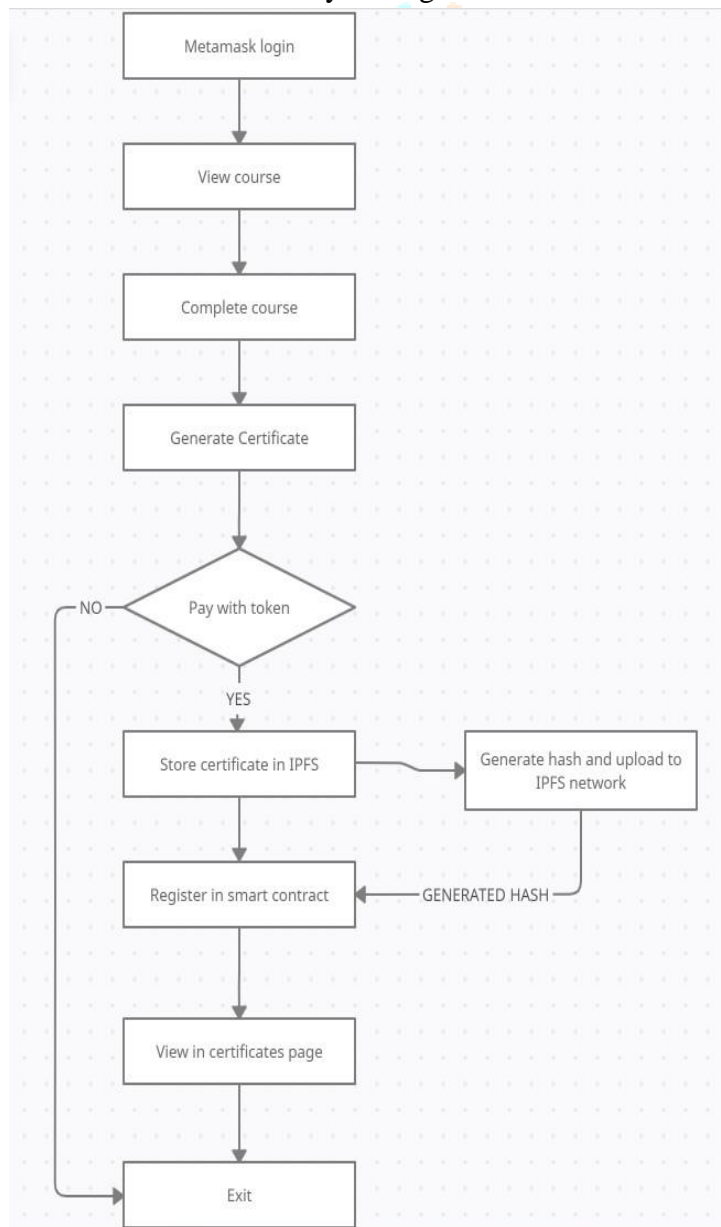


Fig 5.2 Online tutorial platform flow diagram

3.4 MIGRATION

The migration smart contract is used to change the owner of the bank smart contract so that bank smart contract will have bank address as its owner because of this the bank only can mint the token

3.5 TOKEN

This smart contract is based on the ERC-20 Token standards proposed by Fabian Vogelsteller in November 2015. This smart contract contains all the ERC-20 standard methods and events such as

- Methods
 - name()
 - symbol()
 - decimal()
 - totalSupply()
 - balanceOf()
 - transfer()
 - transferFrom()
- Events
 - Transfer()
 - Approval()

. This contract can mint new token based on the requirement, track the total supply of the token

3.6 BANK

This smart contract is core of our project this smart contract handles all the basic functionalities like deposit, withdraw, transfer, receive, upload image, barrow, payoff, swap, record maintain

CONCLUSION

“In banks, we distrust”, was the voice raised in various cypherpunk movements, which has served as the main inspiration for the development of user-friendly, secure decentralized banks using the blockchain technology. The proposed system has been successful in creating a banking system with extended functionality and very close resemblance to the major financial activities in a regular banking system. Hence, this model proves decentralized banks could be the next step in evolving the present day baking systems in security enhancement, better, easy, faster, flexible international exchange, a new

platform of exchange using digital assets. The global financial system serves billions of individuals and businesses, bringing in trillions of dollars in circulation every day. With more popularization of this concept, more number of intermediary nodes would grow, and the benefits of using a decentralized bank would eventually surpass the fee associated with the transactions by a wide margin. Thus, introduction of decentralized banks as a normal means of banking and a more secure equivalent to the traditional banking system could be imminent in the near future.

REFERENCE

- [1] Dirk A Zetsche, Douglas W Arner, Ross P Buckley ,”Decentralized Finance”,Journal of Financial Regulation, Volume 6, Issue 2, 20 September 2020
- [2] YanChenaCristianoBellavitis,” Blockchain disruption and decentralized finance: The rise of decentralized business models”, Journal of Business Venturing Insights Volume 13, June 2020
- [3] Usman W. Chohan,” Non-Fungible Tokens: Blockchains, Scarcity, and Value”,Critical Blockchain Research Initiative (CBRI) Working Papers, 2021
- [4] Lawrence J. Trautman,” Virtual Art and Non-fungible Tokens”,Prairie View A&M University - College of Business Date Written: April 11, 2021
- [5] Jei YoungLee,” A decentralized token economy: How blockchain and cryptocurrency can revolutionize business”,Science and Technology Policy Institute (STEPI), Republic of Korea 25 September 2019.
- [6] Elli Androulaki,Jan Camenisch,Angelo De Caro,Maria Dubovitskaya,Kaoutar Elkhiyaoui,Björn Tackmann,” Privacy-preserving auditable token payments in a

permissioned blockchain system”,ACM Conference on Advances in Financial Technologies October 2020

- [7] Guohua Gan, E. Chen, Zhiyuan Zhou, Yan Zhu,” Token-Based Access Control”, IEEE Access (Volume: 8) 10 March 2020
- [8] Andrei-Dragos Popescu,” Non-Fungible Tokens (NFT) -Innovation beyond the craze”, Proceedings of Engineering & Technology Journal - IBEM 2021

