DECENTRALIZED FINANCE SYSTEM

Shruti Anandas, Anagha Deshmukh, Janvi Singhal,
Final year B.Tech IT, Final year B.Tech IT, Final year B.Tech IT,
Dept. of Information Technology,
UMIT SNDTWU, Mumbai-49, India

Under the guidance of
Prof. Rajesh Kolte

Abstract: Decentralized finance (DeFi) is an emerging financial technology based on secure distributed ledgers similar to those used by cryptocurrencies. In the U.S., the Federal Reserve and Securities and Exchange Commission (SEC), likewise in India we have RBI that define the rules for centralized financial institutions like banks and brokerages, which consumers rely on to access capital and financial services directly. DeFi challenges this centralized financial system by empowering individuals with peer-to-peer digital exchanges. DeFi eliminates the fees that banks and other financial companies charge for using their services. Individuals hold money in a secure digital wallet, can transfer funds in minutes, and anyone with an internet connection can use Defi.

Index Terms- **Defi, Centralization, Decentralization, funds, peer-to-peer, transport, exchanges cryptocurrencies.**

I. INTRODUCTION

The phenomenal rise of cryptocurrencies and decentralized finance have prominently featured "staking": Besides offering a convenience yield for transactions as digital media of exchange, tokens are frequently staked (and slashed) for base-layer consensus generation or for incentivizing economic activities and platform development, and consequently earn stakers rewards in the same tokens. To provide insights into the economics of staking and its asset pricing implications, we build a continuous time model of a token-based economy where agents heterogeneous in wealth dynamically solve their wealth allocation (stake-transact-consume) problem.

Emerging cryptocurrencies like Bitcoin to make a peer to-peer exchange of value without relying on a third party. A blockchain is an immutable, distributed, and append-only data structure created by a sequence of blocks which are chronologically and cryptographically tied

together. Typically, blockchain is a network composed of a set of nodes, named miners or validators, which are responsible for keeping trustworthy records of all transactions using a consensus algorithm in a trust-less environment. More importantly, blockchain enables the essence of smart contracts which can be defined as programs that every blockchain node runs and updates their local replicas according to the execution results without any intervention from a third party. We are Developing Defi application.

This application creates a pool of money, where lenders can stake their money on which they get a Fixed Return with APRs upto 30%, something similar to FDs (Fixed Deposit) but better returns. Now Borrowers can come on our platform and can borrow according to their limits. How do we calculate the limits? Since the data on the blockchain is public, we can traverse through their previous transactions to verify their credibility. Moreover we are using Smart Contracts as an agreement which eliminates the Middleman and directly makes Lender and Borrower the POC.

II. LITERATURE SURVEY

Proof-of-Stake is becoming the prevalent way of securing decentralized networks [1]. Proof-of-Stake has many advantages over the battle-tested Proof-of-Work, including faster block times and finality, lower operational costs, higher throughput, and a lower ecological impact. As a result, the vast majority of new blockchains rely on Proof-of-Stake for their security.

In Proof-of-Stake networks, virtual assets are used as collateral to determine participants ("validators") in the consensus process ("staking"). Since these assets serve to incentivize and enforce the correct behavior of validators, protocols may need to be able to confiscate or destroy them in case of misbehavior [2]. So, Proof-of-Stake protocols escrow staked assets, which prevents them from being transferred or used in decentralized finance applications. Also, a delay ("unbonding period") is often enforced by protocols when one wants to stop participating to recover staked assets.

In the paper presented by Lin William Cong, Zhiheng He, Ke Tang, J, they examined the first study relating various utility-based functions tokens provide to users (e.g., transaction convenience via medium of exchange and rewards via staking) to token prices, from both theoretical and empirical angles [3]. We start by building a continuous time model of an economy with token-based digital networks, where agents heterogeneous in wealth optimally conduct transactions on a (blockchain) platform subject to endogenous productivity shocks, stake tokens to earn rewards from both newly minted tokens and fees, and consume offline. Tokens derive value by enabling users to complete economic transactions on the digital platform, making them a hybrid of money and investable assets. Stakable tokens further serve as collateral and represent claims to rewards. Our model captures the following two distinguishing features of Proof-of-Stake consensus protocols and stakable projects. First, such tokens are used on platforms that support specific economic transactions or broader use in on-chain-based projects.

In the paper presented by Lin William Cong, Zhiheng He, Ke Tang, method they have developed a continuous-time model of a token-based economy where agents heterogeneous in wealth dynamically solve their wealth allocation (staketransact-consume) problems. We cast the interactions as a mean field game with stochastic control and systematic shocks, which underscores aggregate staking ratio as a key variable linking staking to token pricing and equilibrium reward rate [4].

In the paper presented by Calvin, Jonas, & Etienne, it presents a novel and effective method for utilizing staking rewards as an incentive mechanism to encourage users to participate in the consensus finding of the chain actively [5]. In practice, rational users are expected to be profit- seeking and therefore, must assess the potential rewards of participating in the ecosystem of each coin. However, staking rewards are typically denominated in a non-fiat pegged cryptocurrency, carrying potential volatility risks.

In the paper presented by Chris McCoy and Rag Bhagavatha, they designed to offer token holders competitive returns in the growing, multi-billion dollar staking market and to redesign the dynamics of the $266B public cloud computing market through a radically new design that provides value to all stakeholders (users, miners and developers) [6].

III. PROBLEM STATEMENT

A decentralized financial system is a network of financial transactions and services that operate without intermediaries, such as banks or other financial institutions. Its objective is to enable direct peer-to-peer transactions, which can reduce costs and increase efficiency. The system uses blockchain technology to provide transparency, security, and immutability of transactions. It aims to empower individuals and communities by giving them control over their finances and eliminating the need for centralized authorities. In summary, the goal of a decentralized financial system is to provide a transparent, secure, and efficient financial infrastructure that operates without intermediaries.

IV. EXISTING SYSTEM

Understanding DeFi protocols requires understanding the definition of decentralized finance. Peer-to-peer financing, also known as decentralized finance, refers to the transition from conventional, centralized financial systems to peer-to peer funding. In addition to tokenized digital currency and stablecoins, the DeFi ecosystem has successfully created a lending and borrowing platform. Over time, the DeFi landscape has :-

A. AAVE: In the DeFi landscape, Ave is one of the most popular and leading lending protocols. Besides providing security for the protocol, it also enables users to participate in its governance with the native token AAVE. Users can stake AAVE tokens through the Safety Module to achieve AAVE rewards.

B. yEarn: Another top mention goes to yEarn, among the best DeFi protocols. There are several options for yield farming available through this automated liquidity aggregator. YFI, yEarn's native token, handles governance of the protocol. Users could stake YFI tokens to participate in the protocol governance and to claim a pro-rata share of the protocol fees.

C. Uniswap: The UniSwap protocol is also one of the leading DeFi protocols today. As of right now, it is the most popular decentralized exchange in the DeFi space. Offering liquidity to certain pools allows users to earn UNI, the native token. Uniswap will offer 15starting in September 2020 by introducing the "Universal Basic Income" program.

V. PROPOSED SYSTEM

This system explores the different modules involved along with the various models through which this system is understood and represented. Analysis/Framework/ Algorithm Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding).

Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved. Staking is when you lock crypto assets for a set period of time to help support the operation of a blockchain. In return for staking your crypto, you earn more cryptocurrency. Many blockchains use a proof of stake consensus mechanism. Under this system, network participants who want to support the blockchain by validating new transactions and adding new blocks must "stake" set sums of cryptocurrency. Staking helps ensure that only legitimate data and transactions are added to a blockchain. Participants trying to earn a chance to validate new transactions offer to lock up sums of cryptocurrency in staking as a form of insurance.

Popular cryptocurrencies Solana (SOL) and Ethereum (ETH) use staking as part of their consensus mechanisms. Ethereum is a technology that's home to digital money, global payments, and applications. The community has built a booming digital economy, bold new ways for creators to earn online, and so much more. It's open to everyone, wherever you are in the world – all you need is the internet.

VI. METHODOLOGY

Several proof-of-stake blockchains allow for "staking pools", i.e. agents interested in validating transactions can open a pool to which others can delegate their stake [7]. We develop a first game- theoretic model of staking pool formation in the presence of malicious agents who want to disrupt the blockchain. We establish the existence and uniqueness of equilibria. Moreover, we identify the potential and risk of staking pools [8]. First, staking pools can never increase current blockchain security over a system in which such pools are not allowed. Yet, by optimally selecting the distribution of the validation returns, honest stakeholders obtain higher returns, which may be beneficial for future blockchain operations. Second, by choosing welfare optimal distribution rewards, staking pools prevent from allocating large rewards to malicious agents. Third, when pool owners can freely distribute the returns from validation to delegators, staking pools disrupt blockchain operations, since malicious agents attract all delegators by distributing most of the returns to them.

VII. SYSTEM ARCHITECHTURE

In Defi, we have a very open system architecture where the Users can be of mainly two types and the user can exist in both Categories, which are as followed, Lender & Borrow [9].

Both will first Connect their Hot wallet (Meta mask) with our application which gives our platform the ability to communicate with the blockchain using their wallet, Once that is done, User can Stake their tokens for a specific period of time for which they will receive a fixed reward and Same goes for the lenders they come on the platform and connect their Hot Wallet so our Defi has access to the Blockchain and can communicate with other Wallets on the EVM, [10] All the tokens staked by the Lenders are collected in a pool and Borrowers can take their share from it, on which they will be charged an Interest like a

normal traditional Banking system with the key difference being, Instead of the profits going to Greedy Banks it goes to the actual owner.
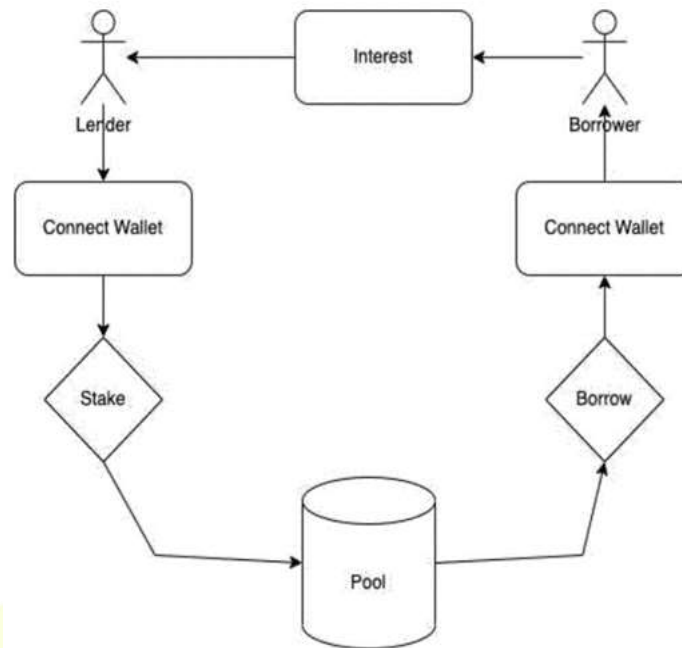

fig.1- system architecture

The modules are:
1)   Authentication
2)   Staking (Lending)
3)   Borrowing

A. Connect Wallet:- Blockchain authentication refers to the system developed for increasing the security of the users and verifying user identity and allows users to connect to the resources found on technologies of digital currency, transactions, cryptocurrencies, etc.

B. Staking Pools:- Users can Stake their tokens for a specific period of time for which they will receive a fixed reward.
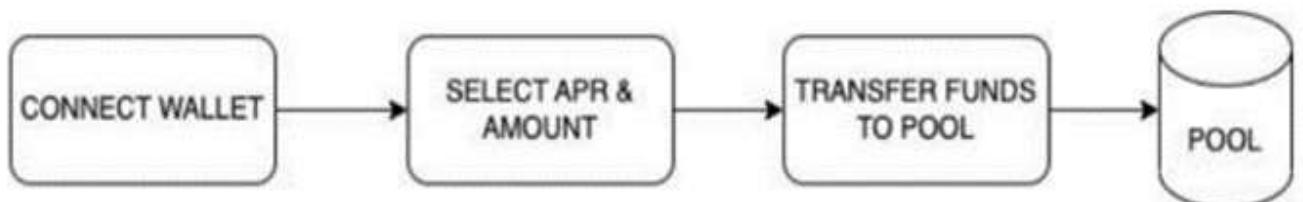

fig.2- staking pools

C. Borrowing Mechanism:- Blockchain technology can help eradicate all the key issues in mortgage origination by means of distributed ledger framework, which provides a list of benefits and capabilities: Multi-party transactions with decentralization capabilities. No intermediaries. Security assurance.
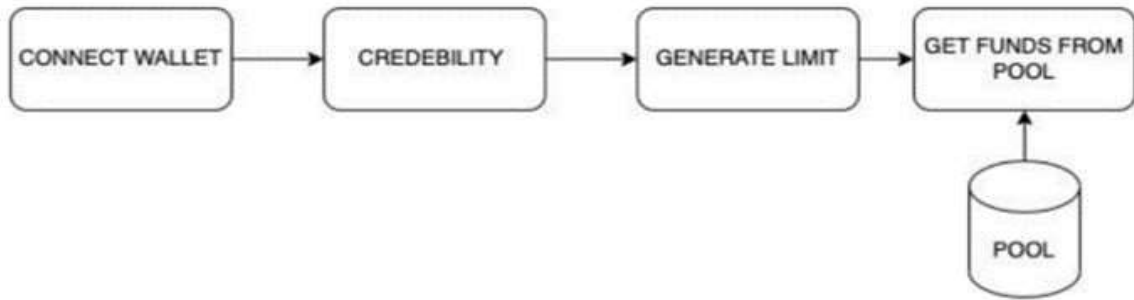

fig.3- lending mechanism

VIII. RESULT

The existing system that is implemented will help the common prople participate in Decentralized Online well as having an option of Lending and Borrowing while eliminating the middleman to earn more profits.
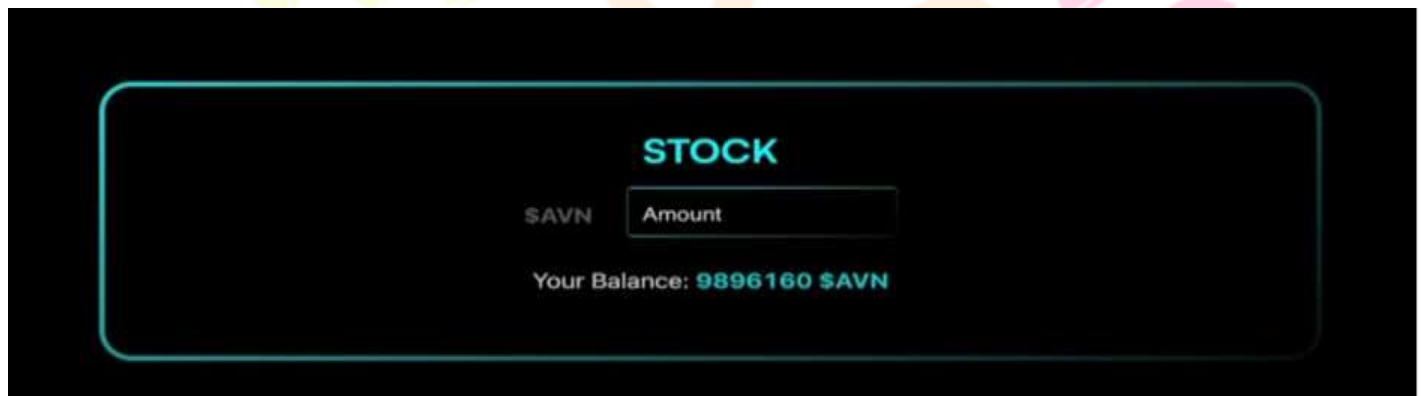

fig.4- enter amount to stake

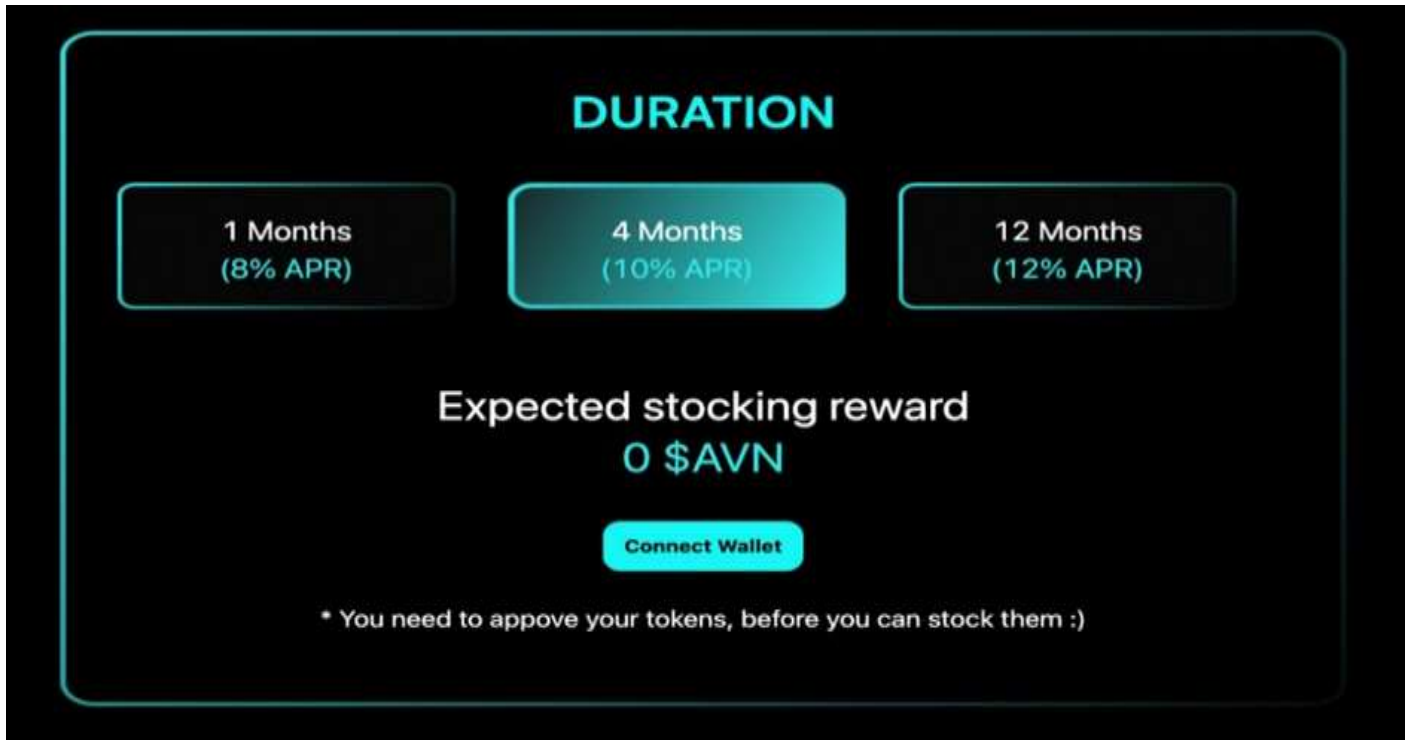fig.5- overview of the amount staked/rewards generated

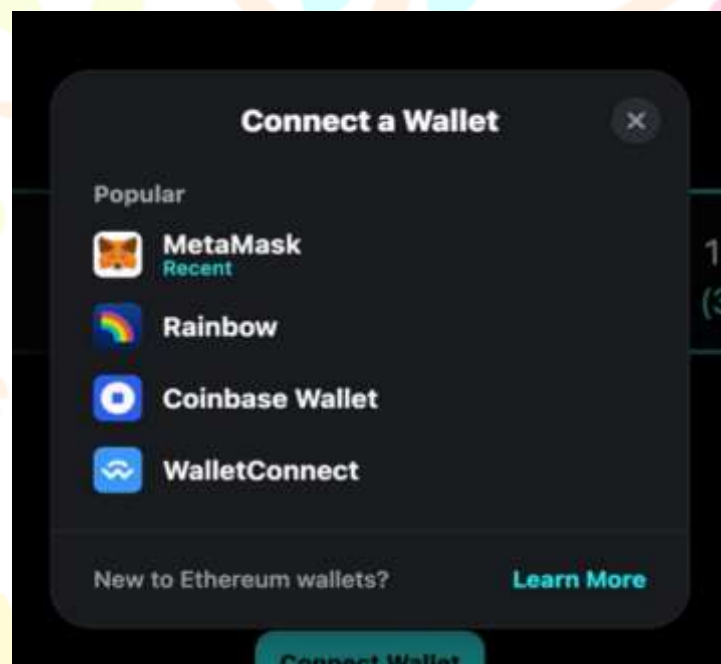fig.6- select APR/duration to lock the tokens for duration

Fig.7- hot wallet options

The dashboard is an Initial Page that enables users to keep track of their financial accounts, transactions, and budgets. It also allows payments to be made using QR codes and DefiId. The design of the dashboard is modern and visually appealing, while also being easy to use and navigate.

Making a payment using QR code or Defi ID through a mobile app involves scanning a QR code or entering Defi ID on a mobile device to initiate a payment transaction. Users can enter their payment details within the app and confirm the payment. This method of payment is becoming increasingly popular as it offers a quick and convenient way to make payments without the need for physical cash or credit cards. The payment has been processed and confirmed as successful. This means that the funds have been transferred to the intended recipient's account.

The transaction history shows a record of both credited and debited payments. It provides a detailed account of all the payments that have been made or received by an individual or organization over a specific period of time. By reviewing the transaction history, one can keep track of their finances and ensure that all payments have been accurately recorded.

IX. CONCLUSION

Lending and borrowing platforms have become a tremen dous part of the DeFi ecosystem. Users are able to lock crypto positions into a smart contract and borrow against their position. Other users are able to lock crypto positions into a smart contract and generate yield by allowing their coins to be lent out to borrowers.

An interesting thing to note is the yields generated by lenders in the DeFi ecosystem are substantially higher than the traditional financial system. Running a smart contract is much more cost-effective than running a traditional bank; therefore, nearly all of the yield generated from lending money is passed directly back to the lender via the smart contract. Many people place their trust in these transparent smart contracts and are able to generate a significant income from their utilization. In a world of ultra-low interest rates, the cost-effective smart contracts are providing a technological solution to this problem.

Many people are upset with central bankers for allowing interest rates to be so low, and a solution isn't found by political persuasion but rather through technology, which has yet again created an opportunity for borrowers and savers alike. Perhaps it would be wise to hedge your bets on the traditional banking system through building a robust DeFi portfolio.

X. REFERENCES

[1] M. R. Baviskar, "Consensus in Blockchain: PoW V/S PoS," Interna tional Journal of Advance Research in Computer Science and Manage ment Studies (IJARCSMS), 2020.

[2] A. Shah, K. Shah, V. Shah, and C. Shah, "Built-in Face Recognition for Smart Phone Devices," International Research Journal of Engineering and Technology (IRJET), 2019.

[3] H. Wiese, J. Komes, S. T¨uttenberg, J. Leidinger, and S. R. Schwein berger, "Staking, Token Pricing, and Crypto Carry," 2018.

[4] Calvin, Jonas, and Etienne, "The Rise of Staking: From Theory to Building Large Infrastructure," 2020.

[5] C. McCoy and R. Bhagavatha, "The Staking Paper," Governed by fault tolerant democracy (one-entity, one-vote), 2022.

[6] "Decentralized finance — Wikipedia, the free encyclopedia," https:// en.wikipedia.org/wiki/Decentralized finance, 2024, https://en.wikipedia. org/wiki/Decentralized finance.

[7] S. B. Conference, "The economics of defi: A gentle introduction to decentralized finance," https://youtu.be/SZXwDhcx9uY?si=LX-yJgq9 Fm3IN5 , 2020.

[8] S. C. Academy, "What are staking pools?" https://www.skrill.com/en/ crypto/the-skrill-crypto-academy/intermediate/what-are-staking-pools/, Year Unknown.

[9] CoinPaper, ing to "Walletconnect dapps and explained: wallets," Secure link https://coinpaper.com/3021/ wallet-connect-explained-secure-linking-to-dapps-and-wallets, Unknown.

[10]   Blocktorch, cations "Architecture (dapps)," of decentralized Year appli https://medium.com/@blocktorch/   architecture-of-decentralized-applications-dapps-d583db198a6f, Unknown.