International Journal of Research Publication and Reviews

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

DeFi using Blockchain

Prof. Punashri Patil [1], Ramchandra Mahesh Warang [2]

[1]Assistant Professor, Department of Information Technology, AISSMS's Institute of Information Technology, Pune-411001, INDIA
[2]TE. BE (Information Technology), AISSMS's Institute of Information Technology, Pune-411001, INDIA

A B S T R A C T

Decentralized finance will dominate the industry in the future because its applications are already transforming it. This article explains the Decentralized Finance concept and how a blockchain is implemented for the Defi. We have already witnessed the revolution that the rise of cryptocurrencies and other blockchain-based tools has sped up. We have looked at the characteristics, how a blockchain works, and the many uses it has. We have studied different types of Blockchain in existence and implemented and future implementation of Blockchain technology in future.

Keywords: Decentralized Finance , DeFi , Smart Contract , CBDC , Dapps

Introduction

Defi is acronym for Decentralized Finance that is a financial system wherein there's no requirement of an central monitoring party to overlook all of the finance elements like transaction between two individuals or corporations.

Digital assets, protocols, smart contracts, and decentralized application platforms all fall under the category of decentralized finance.[3]

Centralized Finance, or CeFi, is the general term for carrying out a transaction through an intermediary like a bank or other numerous services tracking and monitoring the transaction.

The currency that fuels our economy is issued by central authorities, and the government and banks use that same currency in all of their transactions. [3].

Blockchain technology is used to achieve decentralization in the financial sector. As a result of the applications' rapid rise in popularity, the total value of the assets locked in DeFi applications (TVL) increased from $675 million at the beginning of 2020 to more than $40 billion by the end of the first quarter of the following year. [1]

2. Blockchain Technology

2.1 What is Blockchain Technology ?

Blockchain is a distributed ledger system which can be accessed by all the nodes (connected computers) within the network, transaction performed on the Blockchain records are immutable and easily trackable if the records are tampered with.

It allows flow of direct transaction from sender to receiver which stands as the base of Decentralized finance.

Cryptography and the Blockchain hashing process makes sure that the data is immutable. Cryptocurrency are the tokens in an Blockchain network provided for proof of stake or proof of work for maintaining the Ledger of the network.

Proof of work (PoW) is a decentralized consensus mechanism that forbids system-gaming by requiring network participants to spend time and effort resolving an arbitrary mathematical puzzle.

In order to process transactions and add new blocks to a blockchain, cryptocurrencies use the Proof-of-Stake (PoS) consensus mechanism.

Crypto-Assets are ownership stake in an underlying Network, Examples of Crypto-assets is Cryptocurrency or an NFT.

2.2 Features / Characteristics of Blockchain Technology

In Traditional Finance performing a transaction acts like Rube Goldberg machine.

You tap your card in the corner store, and a bitstream goes through a dozen companies, each with their own computer system, some of them being 1970s mainframes and three days later, a settlement occurs. [4]

Well, with a blockchain financial industry, there would be no settlement, because the payment and the settlement is the same activity, it's just a change in the ledger. [4]

2.3 Hashing in Blockchain

Using a mathematical function, hashing is the process of producing a value or values from a string of text. [6].

When a message is only intended for a specific recipient, hashing is one method for enabling security during the transmission process. The hash is created using a formula, which aids in preventing tampering with the transmission's security. [6]

A unique class of hash functions called a cryptographic hash function has several characteristics that make it perfect for use in cryptography. A cryptographic hash function must possess a number of characteristics in order to be deemed secure, including determinism, speed of computation, pre-image resistance, collision resistance, and small changes in the input cause the hash to change. [6]

2.4 Bitcoin

Online payments could be made using only peer-to-peer electronic cash. transferring money without going through a bank or other financial institution directly from one party to another.

Digital signatures provide a part of the solution, but the main benefits are lost if a trustworthy third party is still required to prevent double spending.

To address the double-spending issue, we advise using a peer-to-peer network. The network timestamps transactions by hashing them into a continuous chain of hash-based proof-of-work, establishing a record that cannot be altered without re-doing the proof-of-work. [7].

The longest chain provides evidence of the events as they were observed as well as evidence that it originated from the largest CPU resource.

They will produce the longest chain and outperform attackers as long as nodes in control of the majority of the CPU power are not working together to attack the network. [7]

The network itself doesn't really require much structure. Nodes have the freedom to join and leave the network whenever they want, accepting the longest proof-of-work chain as proof of what happened while they were gone. All reasonable efforts are made to broadcast messages. [7]

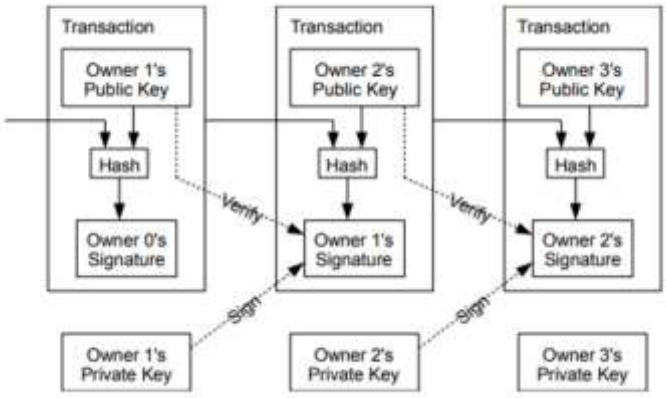

Fig – Chaining the Block [7]

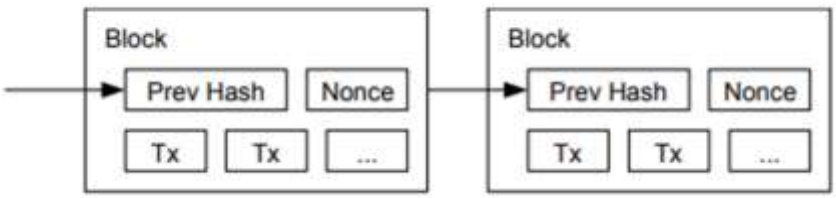

Fig - Blockchain [7]

Digital signatures provide part of the solution, but if a trustworthy third party is still required to prevent double spending, the main benefits are lost.

The following are the steps to running the network:.

1. All nodes receive a broadcast when a new transaction is created.
2. New transactions are compiled into blocks by each node.
3. Each node strives to come up with a challenging proof-of-work for its block.
4. A node broadcasts the block to all other nodes when it discovers a proof-of-work.
5. Only valid transactions that have not already been spent in the block are accepted by nodes.
6. By putting effort into creation, nodes show that they accept the block.

2.5 Ethereum

With Ethereum, you can create decentralized apps and businesses that can hold assets, conduct transactions, and communicate with one another. [8]

You retain control over your own data and what is shared, so using Ethereum does not require you to give up all of your personal information. Ether, Ethereum's own cryptocurrency, is used to fund specific network transactions. [8]

Decentralized programming is done on the Ethereum platform, which is DeFi. You can use Ethereum to build smart contracts that specify a set of requirements or guidelines that must be met before an agreement can be made. It is impossible to change a smart contract once it has been put into use.

The cryptographic hash function Keccak-256 is widely used in Ethereum. As a potential replacement for the SHA-3 cryptographic hash function, Keccak-256 was developed. [8]

With a focus on scenarios where rapid development time, security for small and infrequently used applications, and the ability for various applications to interact very efficiently are important, Ethereum aims to develop an alternative protocol for creating decentralized applications. This protocol will offer a different set of tradeoffs that we believe will be very useful for a large class of decentralized applications. [8].

Ethereum achieves this by creating a blockchain with a built-in Turing-complete programming language that enables anyone to create smart contracts and decentralized applications with their own arbitrary rules for ownership, transaction formats, and state transition functions. This is essentially the ultimate abstract foundational layer. [8].

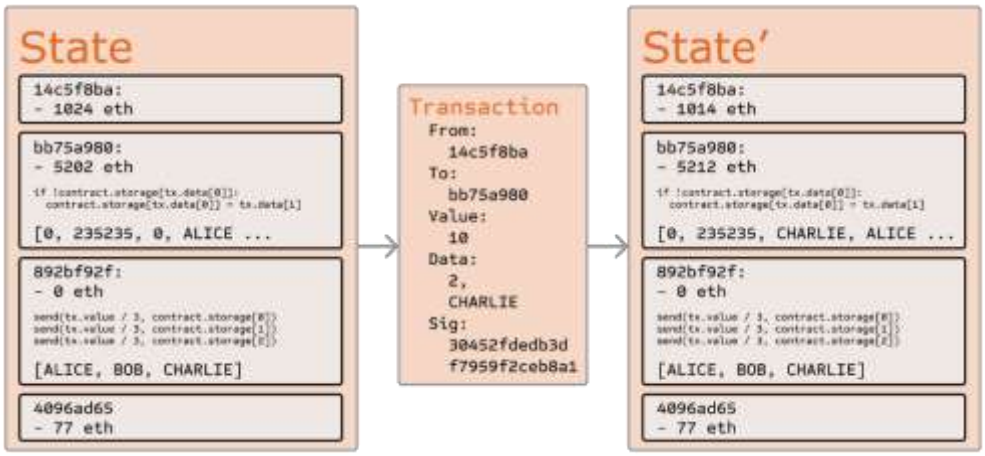

Fig - Block containing transaction [8]

The "Ethereum virtual machine code" or "EVM code" used in Ethereum contracts is a low-level, stack-based bytecode language. The code is made up of a string of bytes, each of which stands for a different operation. [8].

In general, code execution is a never-ending loop that involves repeatedly performing the operation at the current program counter (which starts at zero) and then increasing the program counter by one, up until the end of the code or the detection of an error, STOP, or RETURN instruction. [8].

The code can also output a byte array of data and access the value, sender, and data of the incoming message in addition to block header data. [8]

2.6 Smart Contracts

On the Ethereum blockchain, smart contracts are merely computer programs. They only take action when a transaction from a user (or another contract) initiates it. [8].

They set Ethereum apart from other cryptocurrencies and give it a lot of flexibility. These applications are what are now referred to as decentralized apps, or dapps. [8]

Simple addition and subtraction are requested in digital currency transfers. Transactions using Ethereum are possible and can perform more complicated operations.

Ethereum supports smart contracts and virtual machines on which smart contracts run. Decentralized applications that achieve goals other than a value transfer are made possible by smart contracts. efficient automation of decentralized applications like supply chains.

A smart contract is structurally similar to a class definition in an object-oriented design. It includes data, getter, a set of functions, and functions or methods with the public or private modifier.

For creating smart contracts, particular programming languages have been created. Solidity is one of these words.

3. Advantages of Decentralized Finance over Traditional Finance

The majority of bank-provided features, such as lending, borrowing, earning interest, trading derivatives, purchasing insurance, and trading assets, are also available in decentralized finance.

One of the DeFi market segments with the fastest growth rate is blockchain-based financial contracts, which eliminate the risk associated with relying on middlemen to carry out the transaction and keep track of the contract and transaction records.

All DeFi system transactions carried out on a specific Blockchain network are done so using a specific cryptocurrency.

A transaction may take several business days to settle in a centrally managed system, and there may be multiple charges. There would be no settlement under a decentralized financial system because making payments and settling disputes are the same thing.

The ledger is only changed by a blockchain network transaction. A "DeFi application" is a collection of smart contracts with user interfaces that execute predefined business logic in a transparent and deterministic computing environment made possible by permissionless blockchain technology.

4. Analytical Studies

Liquidity is measured by the total capital locked in DeFi services, which has increased by more than 1,700% to $247 billion over the past year. Over the past year, trading volume on decentralized exchanges (DEXs) has increased by more than 1,500%, reaching more than $300 billion each month. DeFi lending protocols have resulted in an increase of $23 billion in outstanding loans at an annual rate of more than 800%.

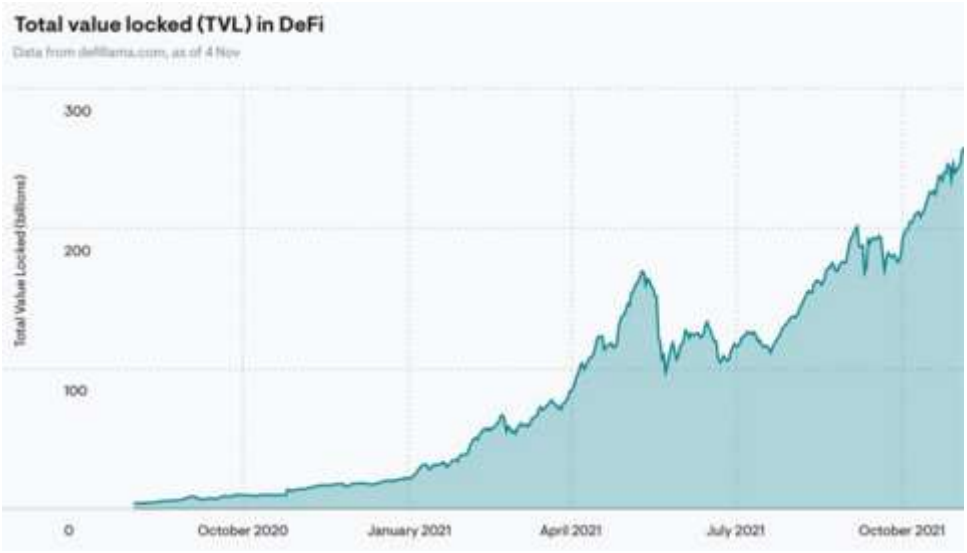

Fig – TVL in DeFi

Fig - Ethereum used [8]

Fig - Growth in Blockchain Wallet user[5]

5. Application of Blockchain in Finance –

5.1 Decentralized Finance Apps

A Dapp, or decentralized application, solves a problem that needs blockchain infrastructure and services in order to function.

A Dapp typically has a blockchain back end, a web front end, and the code connecting the two.

With this architecture, a Dapp's front end sends any external input from users to the blockchain infrastructure and receives any responses back from it.

It starts transactions to call the smart contract's functions. This then logs the transactions, state changes, and receipts on the blockchain. A command line interface can serve as a Dapp's front end.

It could also be an intuitive mobile app or a sophisticated web application. As part of the front-end development, a web client may be created using HTML, JavaScript, CSS, and other web assets, or a web app framework, like Express. In this case, the E-node on the supporting infrastructure is the blockchain server. And a web client with embedded web3 serves as the front-end. JSON over RPC pipeline is being used by a JS script to communicate.

Examples of Decentralized Finance Apps –

MetaMask: MetaMask provides the security and usability required for a runaway to blockchain applications. But in addition to connecting anyone to the blockchain, it also functions as a wallet and can handle account management. In addition, it even provides hardware wallets that are completely independent from the website. [9].

Gnosis Safe : You can fully personalize and manage all of your cryptocurrency assets with the help of the app Gnosis Safe. Even storing them on different devices is possible. It provides, as an illustration, hardware wallets, paper wallets, EOA-based wallets, and even a mix of these. [9].

Codefi Compliance: This program offers KYT procedures that assist companies in identifying potentially risky behaviors right away. As a result, it can provide CFT and AML checks to find any fraudulent activities, including terrorism. [9].

KYC-Chain: Another application that provides you with a wide range of features is KYC-Chain. You will receive access to the Selfkey network, identity and verification checks, crypto wallet AML, a scalable and secure network, and KYC and AML checks. [9].

AirSwap: AirSwap is a fantastic decentralized peer-to-peer trading application for finance. Actually, the technology that powers it is Ethereum. Furthermore, there are no fees, deposits, or sign-ups necessary to trade. Additionally, it provides a safe and user-friendly interface to encourage asset liquidity. [9].

Uniswap : This Ethereum-based Exchange provides an automated liquidity protocol. They employ non-upgradable smart contracts for their formula because it is quite special. As a result, using this gives you access to trusted intermediaries, excellent security, censor resistance, and decentralization as a priority. [9]

5.2 Concept of CBDC

Central Bank Digital Currency (CBDC) is a digital version of currency notes that are issued by a central bank. The majority of central banks worldwide are investigating the issuance of CBDC, but the main drivers behind it depend on the particular needs of each nation. [10]

The legal tender issued in digital form by a central bank is known as CBDC, according to Reserve Bank. It has parity (1:1) exchange rates with the fiat currency and functions exactly like a sovereign currency. [10].

Although India has a large amount of digital money, such as bank accounts that are recorded as book entries on the ledgers of commercial banks, a CBDC would be different from other digital currencies because it would be a liability of the Reserve Bank rather than a commercial bank. [10]

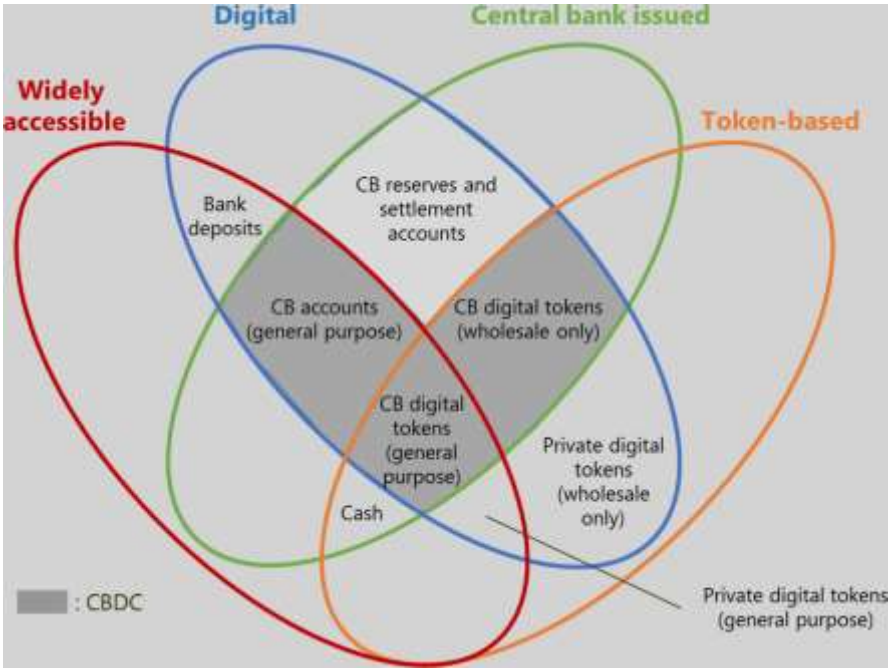

Fig – CBDC [10]

Features of CBDC:

1. CBDC is a form of sovereign currency that central banks have issued in accordance with their monetary policies.
2. On the balance sheet of the central bank, it appears as a liability.
3. All individuals, businesses, and governmental organizations must recognize it as a form of payment, legal tender, and a secure place to store value.
4. Freely convertible into cash and money from commercial banks.
5. Holders are not required to have a bank account and are given fungible legal tender.

6. Hoped to reduce the cost of issuing money and conducting transactions. [10]

6. Conclusion

We have looked at the potential effects, difficulties, and dangers brought on by the expansion of consumer-facing DeFi applications. Although DeFi applications running on permissionless blockchains have the radical potential to transform consumer-facing financial services, there are still significant risks involved in using these applications.

Decentralized finance system has already start replacing some of the factors of a centralized system.

Recently the increasing interest in Blockchain and cryptocurrency has got many people to invest and learn blockchain development which has lead to amazing innovation and applications of Decentralized finance using Blockchain Technology Decentralized finance is the future as most of the value is shifting to Blockchain technology and its implementations.

References

Van der Geer, J., Hanraads, J. A. J., & Lupton, R. A. (2000). The art of writing a scientific article.*Journal of Science Communication, 163*, 51–59.

Strunk, W., Jr., & White, E. B. (1979).*The elements of style* (3rd ed.). New York: MacMillan.

Mettam, G. R., & Adams, L. B. (1999).How to prepare an electronic version of your article. In B. S. Jones & R. Z. Smith (Eds.), *Introduction to the electronic age* (pp. 281–304). New York: E-Publishing Inc.

Fachinger, J., den Exter, M., Grambow, B., Holgerson, S., Landesmann, C., Titov, M., et al. (2004).Behavior of spent HTR fuel elements in aquatic phases of repository host rock formations, 2nd International Topical Meeting on High Temperature Reactor Technology. Beijing, China, paper #B08.

Fachinger, J. (2006). Behavior of HTR fuel elements in aquatic phases of repository host rock formations.*Nuclear Engineering & Design,236*, 54.

[1] Johannes Rude Jensen , Victor von Wachter , and Omri Ross, "*An Introduction to Decentralized Finance (DeFi)*", Complex Systems Informatics and Modeling Quarterly (CSIMQ) eISSN: 2255-9922 , Article 150, Issue 26 , 2020

[2] Dirk A. Zetzsche , Douglas W. Arner , and Ross P. Buckley, "*Decentralized Finance*", Journal of Financial Regulation, 2020, 6, 172–203 doi: 10.1093/jfr/fjaa010, 2021

[3] Decentralized finance explained, accessed on 2022 Sept 21, *https://dappradar.com/blog/decentralized-finance-explained*

[4] "*How the blockchain is changing money and business*" YouTube, uploaded by TED, Sep 16, 2016, *https://www.youtube.com/watch?v=Pl8OlkkwRpc*

[5] *The Future is Decentralised*, accessed on 2022 Sept 21, *https://www.blockchain.com/static/pdf/TheFutureisDecentralised.pdf*

[6] *What Is Hashing?* [Step-by-Step Guide-Under Hood Of Blockchain], accessed on 2022 Sept 21, *https://blockgeeks.com/guides/what-is-hashing/*

[7] *Bitcoin: A Peer-to-Peer Electronic Cash System*, accessed on 2022 Sept 21, *https://bitcoin.org/bitcoin.pdf*

[8] *Ethereum.org Website*, accessed on 2022 Sept 21, *https://ethereum.org/en/*

[9] *30+ Best Decentralized Finance Applications*, accessed on 2022 Sept 21, *https://101blockchains.com/decentralized-finance-applications/*

[10] FinTech Department Reserve Bank of India, *Concept Note on Central Bank Digital Currency*, 2022 October