International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 04 | April - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Decentralized Finance: An Innovative Approach to Money Transactions

Praveen Lachheta[1] , Ramanarayan Singh[2] , Ritul Yadav[3], Assis . Prof. Varsha Kothari[4]

[1] Student, B. Tech, Department of Computer Science and Engineering, Medi-Caps University, Indore, Madhya Pradesh, India

[2] Student, B. Tech, Department of Computer Science and Engineering, Medi-Caps University, Indore, Madhya Pradesh, India

[3]Student, B. Tech, Department of Computer Science and Engineering, Medi-Caps University, Indore, Madhya Pradesh, India

[4]Assistant Professor, Department of Computer Science & Engineering , Medi-Caps University, Madhya Pradesh , India

---

Abstract: *Decentralized finance (DeFi) is a rapidly growing sector of the cryptocurrency industry that aims to provide financial services and applications on a decentralized and open-source network. DeFi platforms utilize blockchain technology to enable peer-to-peer transactions, lending and borrowing, staking and yield farming, and other financial services without the need for traditional financial intermediaries such as banks.*

Blockchain is a technology that makes it possible for parties to transact securely and openly without the use of middlemen like banks, governments, or other reliable third parties.

Keywords: Blockchain, Cryptocurrency, Bitcoin, Peer-to-Peer Network, Decentralized Ledger, Nodes, Tokens

1. Introduction:

Decentralized Finance (DeFi) has become a major focus of innovation within the blockchain industry, and its potential impact on traditional financial systems is gaining more attention every day. DeFi promises to democratize finance, making financial services more accessible and less costly to users. In the DeFi ecosystem, decentralized applications (dApps) are built on blockchain networks such as Ethereum, and they allow users to access a range of financial services such as lending, borrowing, trading, and investing.

One of the key advantages of DeFi is that it eliminates intermediaries such as banks and other financial institutions, which can reduce costs and provide greater access to financial services. DeFi also offers greater transparency, as all transactions are publicly auditable and traceable. This transparency can help to reduce the risk of fraud and increase trust in financial systems [20].

Another advantage of DeFi is its potential to promote financial inclusion. According to the World Bank, there are an estimated 1.7 billion people who are unbanked or underbanked, and DeFi has the potential to provide them with access to financial services. DeFi protocols can be accessed from anywhere in the world, and they do not require users to have a bank account or a credit score [21].

DeFi also offers users greater control over their funds, as they can manage their assets directly without the need for intermediaries. Smart contracts enable users to automate transactions, manage collateral, and ensure compliance with predetermined rules. Additionally, DeFi protocols are highly secure, and they use cryptography to protect users' funds from theft and other forms of fraud.

Despite its potential benefits, DeFi also faces some challenges. One of the key challenges is the lack of regulation in the space. While DeFi protocols are highly transparent, they are not subject to the same level of regulation as traditional financial institutions. This lack of regulation can lead to potential risks for investors, and it may make it difficult for DeFi to gain mainstream adoption [20].

Another challenge is the high volatility of cryptocurrencies, which are often used as the underlying asset in DeFi protocols. This volatility can make it difficult to predict returns and can lead to significant losses for users. Additionally, the DeFi ecosystem is still in its early stages, and there are many technical and scalability issues that need to be addressed.

2. Literature Review:

Decentralised Finance (DeFi), a new trend in the financial sector, uses blockchain technology to build a network of open, transparent, and widely available financial applications. Smart contracts, the foundation of the DeFi ecosystem, automate financial transactions and make it possible to create financial products and services including lending, borrowing, trading, and insurance without the use of middlemen.

One of the earliest DeFi projects is MakerDAO, which was launched in 2017 and enables users to borrow stablecoins (DAI) by locking up their cryptocurrency holdings as collateral [1]. The system is governed by a decentralized autonomous organization (DAO) that ensures the stability of the DAI stablecoin, and the collateralization ratio of the system.

Another noteworthy DeFi initiative is Uniswap, a decentralised exchange that was introduced in 2018 and allows users to trade cryptocurrencies without the involvement of middlemen [2]. Based on the ratio of the assets in the liquidity pool, the automated market maker (AMM) algorithm that powers the exchange determines prices. With its trading volume surpassing that of numerous centralised exchanges, Uniswap has experienced tremendous growth in popularity in recent years.

Other DeFi projects have emerged in recent years, such as Compound, Aave, and Curve, which offer lending, borrowing, and trading services on a decentralized platform [3][4][5]. These projects have introduced new financial instruments such as flash loans, which enable users to borrow and repay loans within a single transaction, and yield farming, which enables users to earn rewards by providing liquidity to the platform.

The growth of the DeFi ecosystem has led to several challenges, such as scalability, interoperability, and security. The scalability challenge is related to the high gas fees on the Ethereum network, which can make DeFi transactions costly and slow [6]. The interoperability challenge is related to the fragmentation of the DeFi ecosystem, with different protocols and platforms using different standards and architectures. The security challenge is related to the potential vulnerabilities in the smart contracts and the potential for hacks and exploits.

To address these challenges, several initiatives have been proposed, such as the use of layer 2 solutions to increase scalability, the development of cross-chain protocols to increase interoperability, and the use of formal verification and audits to increase security [7][8][9].

In conclusion, the DeFi ecosystem has emerged as a new trend in the financial industry, offering open, transparent, and accessible financial services to everyone. The ecosystem is based on smart contracts that automate financial transactions, and has introduced new financial instruments and services. However, the growth of the DeFi ecosystem has also led to several challenges that need to be addressed to ensure scalability, interoperability, and security.

A. DeFi Overview: -

Decentralized Finance (DeFi) can be referred to as an alternative financial instrument that is built on top of blockchain technology - a tamper-proof and immutable data recording platform [3]. As DeFi does not rely on intermediaries and centralized parties for its transactions, agreements are enforced using self-executing code called smart contracts. This approach has several advantages over conventional centralized financial systems and can work in a more transparent way without the need for central clearing houses or escrow services as DeFi protocols are implemented using decentralized applications (dApps) where many of the roles are by agreements written into lines of code [4].

Decentralized Finance is an architecture with many layers, and each of these layers has specific functions to perform. The layers of a typical DeFi framework are (1) Aggregation Layer, (2) Application Layer, (3) Protocol Layer, (4) Asset Layer, and (5) Settlement Layer. The detailed functionalities of each of these layers are outlined as follows

- The Aggregation Layer: The duty of the aggregation layer is to work as an intermediate layer connecting user applications and different protocols or applications. This layer helps users easily consume the application's protocols simultaneously and reduce the burden of complex procedures to use the protocols [5]. In addition, this layer will collect and aggregate relevant information in a concise manner for the users.

- The Application Layer: The application layer acts as a container for creating user applications that can connect with individual protocols in the DeFi stack [6]. The users may be presented with a browser extension for using the application easily. One example of an application layer is Metamask, which is a browser extension for token wallets and token exchanges.

- The Protocol Layer: The protocol layer provides templates and standards for specific applications such as decentralized exchanges (DEXs), asset management, and debt market-based activities [7]. Smart contracts play a vital role in the protocol layer as the protocol standards are primarily implemented using smart contracts.

- The Asset layer: The asset layer contains all of the assets such as fungible tokens - such as Ethereum ERC20 tokens - and non-fungible tokens - Ethereum ERC721 tokens [8]. These assets are issued on a blockchain platform and include digital art, bonds, real estate, venture capital funds, and commodities.

- The Settlement Layer: The settlement layer holds the blockchain and its corresponding native assets [9]. Figure 2 depicts the typical architecture for a DeFi platform and identifies ETH as the native asset of the Ethereum blockchain.

B. Blockchain architecture: -

Blockchain technology is based on the idea of a decentralised database, where identical copies of the data are stored across multiple computers.

Organisations keep their data in centralised databases, making them an obvious target for hackers. In contrast, the decentralised structure of the blockchain has made it a technology that is hacker-proof. One way to think of blockchain is as a peer-to-peer network that runs on top of the internet.

The three primary levels of the blockchain architecture are applications, decentralised ledgers, and peer-to-peer networks. The top layer of the network is Applications, followed by the Decentralised Ledger and the Peer-to-Peer Network at its base.

The Blockchain application software is contained in the application layer. For instance, the private and public keys are created and stored by Bitcoin wallet software, which enables users to maintain control over their unspent bitcoins. Users can trace their transactions using an interface provided by the application layer that is human understandable.

The Decentralised Ledger layer, which sits in the midst of a blockchain architecture, confirms a reliable and consistent global ledger. In this layer, transactions can be organised into blocks that are connected cryptographically. Tokens can be exchanged between two participants in a transaction, and each transaction must first pass a validation process before being accepted as a valid transaction.

Gathering transactions into a block and adding it to the end of the current blockchain is the process of mining. A proof-of-work method is used by blockchain to identify the chain that has needed the most overall effort to construct it and to ensure consensus among all nodes on the blockchain's legitimacy. Peer-to-Peer networks, which perform diverse functions for different sorts of nodes and exchange different kinds of messages to run the Decentralised Ledger, are the foundation of the blockchain architecture.[14]

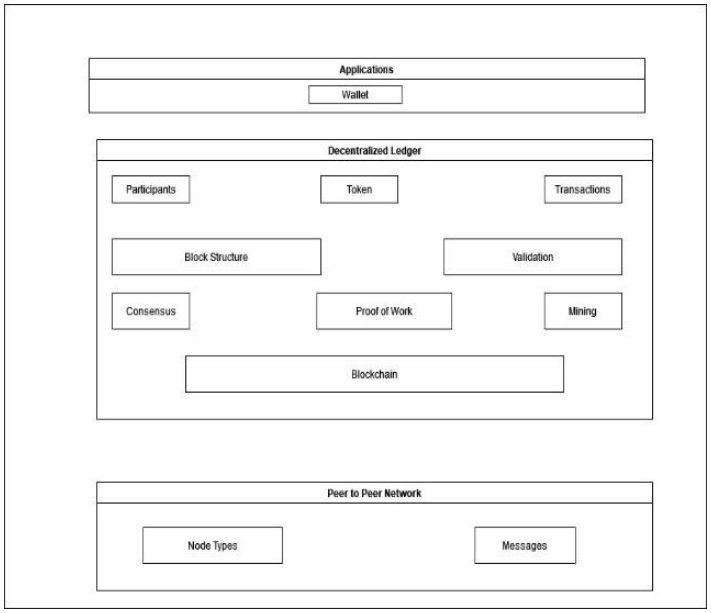

Figure 1: Layers of blockchain architecture

i. Applications:

It offers interfaces for applications on top of the blockchain and is used to protect coins. This programme can be hosted on a third-party site, installed on your PC or mobile devices, or both.[15]

ii. Decentralized Ledger:

A decentralised ledger is a shared and duplicated set of data that keeps network participants in sync. It keeps track of all transactions between network participants. The ledger is in charge of documenting all interactions between the participants. Blockchain shares many characteristics like databases, with the exception that data is kept as tokens or cryptocurrencies rather than in the header of a database.

As the first step in entering transactions into the ledger, it is necessary to arrange the recently validated transactions into blocks. Any user of the blockchain has the ability to compile fresh transactions and build blocks that can be added to the blockchain. Transactions, the hash pointer, timestamps, and the nonce are the main components of a block.

Nodes carry out a variety of tasks according to their position in the blockchain network. When a node proposes and approves transactions as well as engages in mining to create consensus and safeguard the blockchain, it is referred to as a miner. It can carry out tasks like basic payment verification and others, depending on the blockchain being utilised.

A consensus algorithm that confirms the accuracy of data is known as proof of work. Hashcash, for instance, is used by Bitcoin as a proof of work for bitcoin transactions. To ensure that the transactions in the block are legitimate, miners must complete a proof of work before the network will accept the block. The blockchain network is secure and has consensus thanks to proof of work. A hash (id) is given to a block during the verification process. This hash is appended to the most recent block of transactions in order to verify the following block. Add a nonce, which is a random number that may only be used once, to the end of the subsequent block in the following step. This random number is altered using the hash function to create a string that has a number of zeros in front of it.

Because it always depends on the incentives of the miners, proof of work can have scalability and security problems in the future. It is also expensive to maintain. It is profitable to enforce a sophisticated solution known as "proof-of-stake," which defines who gets to update the consensus and prevents unintended forking of the underlying blockchain.

In a blockchain network, no private information is exchanged, and every transaction is public to every node. Peer-to-peer networks can be constructed on any physical infrastructure and do not need additional security.[15]

3. Pros and Cons:

- **Benefits of DeFi: -**

1. Decentralization: DeFi eliminates the need for intermediaries such as banks, making the financial system more decentralized [10].

2. Transparency: Transactions on DeFi platforms are transparent and publicly available on the blockchain, increasing trust in the system [11].

3. Accessibility: Anyone with an internet connection can participate in DeFi, regardless of geographic location or socio-economic status [12].

4. Security: The use of blockchain technology in DeFi provides security against fraud and tampering with the ledger [13].

5. Interoperability: DeFi protocols can be easily integrated with one another, allowing for the creation of complex financial products and services [12].

6. Cost-efficiency: DeFi eliminates the need for intermediaries, reducing transaction costs and fees [10].

- **Cons of DeFi:**

1. Security vulnerabilities: Smart contracts, which are used extensively in DeFi, can have security vulnerabilities that can be exploited by attackers [16].

2. Lack of regulation: The DeFi space is largely unregulated, which can lead to potential risks for investors [18].

3. High volatility: The value of cryptocurrencies, which are used as collateral in many DeFi protocols, is highly volatile, leading to potential risks for borrowers and lenders [19].

4. Limited adoption: Despite the growth of the DeFi space, it still has limited adoption compared to traditional finance [17].

5. Limited scalability: Some DeFi protocols may face scalability issues, limiting the number of users that can participate in the system [17].

4. Discussion:

Decentralized Finance (DeFi) has gained significant attention in recent years as it promises to democratize financial services and provide greater financial inclusion. DeFi has the potential to disrupt traditional financial systems by providing an alternative to centralized financial intermediaries such as banks and other financial institutions.

One of the key advantages of DeFi is the transparency it provides. All transactions on a blockchain network are publicly visible, and anyone can audit the transactions and smart contracts to ensure that everything is working as

intended. This transparency is a significant advantage over traditional financial systems, which are often opaque and difficult to audit.

Another advantage of DeFi is that it is accessible to anyone with an internet connection. Traditional financial systems often exclude those who are unbanked or underbanked, but with DeFi, anyone with a smartphone or computer can access financial services. This accessibility has the potential to drive financial inclusion and help to reduce global poverty.

Furthermore, DeFi has the potential to reduce transaction costs and increase transaction speeds. By eliminating intermediaries, DeFi can reduce the fees associated with traditional financial systems, making financial services more affordable for everyone. Additionally, DeFi transactions can be
settled in a matter of seconds, as opposed to days or even weeks for traditional financial systems.

However, DeFi is not without its challenges. One of the main challenges is the lack of regulation, which can lead to potential risks for investors. Additionally, DeFi is still in its early stages, and there are many technical and scalability issues that need to be addressed.

Furthermore, the use of cryptocurrencies in DeFi protocols can be highly volatile, leading to potential risks for borrowers and lenders. Additionally, smart contracts, which are used extensively in DeFi, can have security vulnerabilities that can be exploited by attackers [16].

In conclusion, while DeFi has the potential to disrupt traditional financial systems and provide greater financial inclusion, it still faces significant challenges that need to be addressed. With careful regulation and development, DeFi has the potential

References:

[1]. MakerDAO. (2021). MakerDAO. Retrieved from https://makerdao.com/

[2]. Uniswap. (2021). Uniswap. Retrieved from https://uniswap.org/

[3]. Compound. (2021). Compound. Retrieved from https://compound.finance/

[4]. Aave. (2021). Aave. Retrieved from https://aave.com/

[5]. Curve. (2021). Curve. Retrieved from https://curve.fi/

[6]. Ethereum. (2021). Ethereum. Retrieved from https://ethereum.org/

[7]. Ethereum. (2021). Ethereum 2.0. Retrieved from https://ethereum.org/eth2/

[8]. Polkadot. (2021). Polkadot. Retrieved from https://polkadot.network/

[9]. OpenZeppelin. (2021). OpenZeppelin. Retrieved from https://openzeppelin.com/

[10]. Global Digital Finance, "Decentralized Finance: Scaling Public Infrastructure," 2020. Available:

[11]. D. Cohen and E. W. Felten, "Designing Secure Systems That Encourage User Participation," Communications of the ACM, vol. 58, no. 4, pp. 42-44, 2015.

[12]. C. M. Ivan and A. N. Nistor, "Blockchain-Based Decentralized Finance: Current State and Opportunities," Sustainability, vol. 13, no. 6, p. 3258, 2021.

[13]. D. R. K. Chaitanya and D. M. Kumar, "A Comprehensive Review of Decentralized Finance (DeFi)," IEEE Access, vol. 9, pp. 18883-18897, 2021.

[14]. Decentralized finance research and developments around the world. https://www.researchgate.net/publication/362861920_Decentralized_finance_research_and_developments_around_the_world

[15]. Simanta S (2018) Understanding Blockchain Technology. https://www.researchgate.net/publication/336130918_Understanding_Blockchain_Technology

[16]. E. Kharaz, A. Shafiei, and A. G. Voyiatzis, "Coinbugs: Enumerating Common Blockchain Implementation-Level Vulnerabilities," in Proceedings of the 27th USENIX Security Symposium, 2018, pp. 1103-1118.

[17]. L. Li and A. M. C. So, "Security and Privacy in Decentralized Finance," in Proceedings of the 2021 IEEE

International Conference on Blockchain and Cryptocurrency (ICBC), 2021, pp. 1-6.

[18]. B. Donnelly, "Decentralized Finance (DeFi) Is Booming, But There Are Serious Risks Involved," Forbes, 2021. Available: https://www.forbes.com/advisor/investing/decentralized-finance-defi-risk/.

[19]. R. T. McInerney, "Why Decentralized Finance Is a Double-Edged Sword," Harvard Business Review, 2021. Available: https://hbr.org/2021/02/why-decentralized-finance-is-a-double-edged-sword.

[20]. ConsenSys. (n.d.). Decentralized Finance (DeFi). Retrieved September 14, 2021, from https://consensys.net/defi/

[21]. World Bank. (2018). The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution. Retrieved September 14, 2021, from