DOI: 10.21917/ijsc.2023.0438
SPECIAL ISSUE ON INNOVATIONS AND TECHNOLOGY IN FINTECH (ITFT-2023)

CHALLENGES, OPPORTUNITIES AND RISK ANALYSIS OF ADOPTION OF DECENTRALIZED FINANCE APPLICATIONS

Rupali Ahuja, Janhavi Khandelwal and Anjali
Department of Computer Science, Maitreyi College, India

Abstract

Decentralised Finance or DeFi has emerged as a transformative and disruptive force within the financial industry, offering innovative financial services powered by blockchain technology and smart contracts. This paper provides in-depth knowledge of DeFi, its evolution, applications, and their adoption. It identifies the opportunities brought about by DeFi, comparing it with the traditional CeFi (Centralized Financial) system, including financial inclusion, transparency, and programmable money. It highlights the potential of applications of DeFi for decentralized lending, decentralized exchanges, and yield farming as innovative and promising avenues within the DeFi space. A SWOT analysis comparing DeFi and CeFi was performed to delve into the strengths, weaknesses, opportunities, and threats associated with DeFi. This study explored the intricate challenges and inherent risks involved in the adoption of DeFi applications, offering insights into the hype, fear, and apprehensions among governments and the masses regarding its adoption. The findings offer a nuanced understanding of the current state of DeFi, providing valuable insights for researchers, policymakers, and industry practitioners.

Keywords:

Decentralised Finance, Smart Contracts, CeFi, DeFi Risks, DeFi Adoption, SWOT Analysis

1. INTRODUCTION

Finance deals with managing money, investments, and financial assets. Our modern economy depends a lot on investing money. Many organizations around the world gather and distribute money invested by people. Financial information is mostly digital nowadays. The financial services industry is experiencing a significant impact due to the process of digitization. DeFi (Decentralized Finance) is a new way of handling financial transactions based on blockchain technology. It allows the creation of financial infrastructure that eliminates centralized authority and offers financial services in a decentralized manner [1].

Traditional financial systems have existed for centuries. The initial type of market exchange can be traced back to peer-to-peer transactions, commonly referred to as barter. However, barter systems have limitations, such as the requirement of a double coincidence of wants and difficulties in establishing a standardized value for different goods. To overcome these challenges, societies gradually transitioned to using money as a medium of exchange. With the establishment of money as a medium of exchange, centralized financial systems evolved. In its financial institutions play an important role as intermediaries in controlling financial transactions. These intermediaries assist in lowering transaction costs, facilitating the smooth flow of financial transactions, and ultimately dominating economic activities [2]. Centralized financial institutions such as Central Banks, Financial Regulators, Brokers, and Asset Management Companies hold dominant market power and earn profits. These systems have relied on trust in centralized entities, regulatory frameworks, and physical infrastructure to operate.

CeFi (Centralized Finance) emerged as a response to the limitations and inefficiencies of traditional financial systems. It involved the digitization and automation of financial processes, bringing convenience and speed to transactions and services. CeFi entities, such as online banks and payment processors, acted as intermediaries, controlling users' funds and executing transactions on their behalf [3]. The global unbanked population stands at approximately 1.7 billion people, while small businesses face exclusion from traditional banking services and resort to expensive financing options like credit cards. This leads to significant costs for both small businesses and retailers, with the latter losing 3% on each credit card sales transaction. As a consequence, there is a reduction in investment and economic growth [4].

The term “Fintech”, which emerged by combining the words “financial” and “technology”, refers to the application of technology and innovation to improve and enhance financial service and is believed to have been introduced in the early 1990s by John Reed, the chairman of Citicorp [5]. Fintech seeks to enhance efficiency, accessibility, and convenience in traditional financial systems using various technological advancements. Fintech encompasses innovations such as mobile banking, digital payments, online lending platforms, robo-advisors, and more. Fintech’s impact extends beyond traditional banking and finance, with its influence expanding into areas such as insurance, wealth management, regulatory compliance, and financial inclusion [6].

According to Saulo Dos Santos et al. [7], Innovative technologies in the finance field have the potential to revolutionize the financial ecosystem, posing competitive risks to established firms and creating opportunities for new entrants.

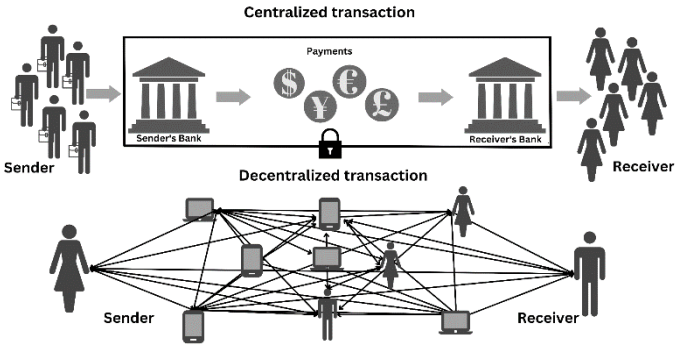

Fig.1. Working of the Centralized vs Decentralized transactions [7]

The advent of blockchain technology and cryptocurrencies has further propelled the fintech industry, giving rise to DeFi. DeFi is a financial system that is fundamentally different from traditional

finance as it doesn't have a single authority governing the entire financial ecosystem. The Fig.1 contrasts the working of centralized and decentralized transactions.

A variety of protocols associated with DeFi make use of advanced software programs called "smart contracts" that enable the execution of traditional financial activities on top of the blockchain framework. Smart contacts [8] is a self-executing contract with the terms of the agreement directly written into lines of code. These contracts run on a blockchain network, such as Ethereum [9], and automatically execute when predefined conditions are met.

Blockchain employs multiple replicated immutable and secure copies of each transaction. If one version of the copy is modified, all of the remaining copies will be modified as well. Each message is encrypted before it is sent to the blockchain. Blockchain technology allows anyone to assess transactions, but due to clever design and being supplemented by cryptography and consensus mechanisms, the way data is recorded in the blockchain makes it extremely difficult to modify one piece of data without requiring changes to all subsequent data records. Distributed payment systems, like blockchain-based money transfers, seem to be more secure than CeFi.

DeFi plays a significant role within the broader realm of fintech. It represents a specific area of innovation and disruption within the financial technology landscape. Ethereum [9], as a decentralized blockchain platform, played a crucial and influential role in the evolution of DeFi. By introducing the concept of smart contracts, Ethereum enabled the creation of autonomous and self-executing financial agreements. This breakthrough empowered developers to construct decentralized applications (dApps) on the Ethereum network, thereby facilitating a diverse array of financial services like lending, borrowing, decentralized exchanges, and yield farming [9].

In DeFi, transactions are based on cryptographically secured digital currency. Satoshi Nakamoto in 2008 proposed the first decentralized digital cryptocurrency called bitcoin [10]. China declared all cryptocurrencies illegal in September 2021[11]. Many nations have outrightly banned cryptocurrency as of 2023. Bangladesh, Nepal, Qatar, and Ghana are among them. Forty-two nations have an implicit ban on the asset, typically by prohibiting local financial institutions from doing business with cryptocurrency companies. In contrast, 103 countries like Canada, Slovenia, and Germany have taken up initiatives to develop crypto regulations alongside their objectives for organizations dealing with cryptocurrencies [12]. El Salvador was the first nation to adopt bitcoin cryptocurrency as a legal tender on 9 June 2021 followed by the Central African Republic on 27 April 2022 [13], [14].

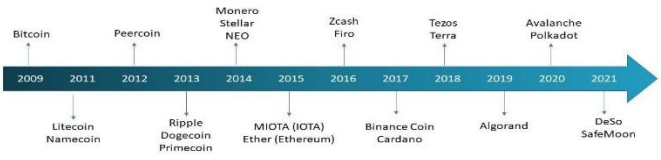

Fig.2. Timeline of the introduction of the most famous cryptocurrencies from 2009 – 2021 [12]

The Indian Government recently banned the use of cryptocurrencies in India as cryptocurrencies would lead to the dollarization of the Indian economy if they are legalized [15]. According to the KuCoin report [16], 115 million people in India own cryptocurrencies as of the year 2021. In the next section, we discuss some popular digital currencies.

1.1 DIGITAL CURRENCIES

Bitcoin introduced the concept of decentralized digital currency and addressed the need for a trustworthy electronic cash system without relying on a central authority. Since then, many Decentralized digital currencies have come up with their own features and applications. These cryptocurrencies have the potential for future adoption and use in DeFi applications. Fig.2 represents the timeline of the introduction of the most popular cryptocurrencies introduced between 2009 to 2021.

Bitcoin [17] was created by Satoshi Nakamoto, as a peer-to-peer electronic cash system that revolutionized the financial environment as the first decentralized cryptocurrency and payment system. It operates as a digital currency exchanged directly between parties, eliminating the need for intermediaries like banks or financial institutions.

Litecoin [18] was introduced as a faster and lighter alternative to Bitcoin. It functions on a distributed network and utilizes the Scrypt algorithm to expedite the creation of blocks. Litecoin, which has a limited supply of 84 million coins, stands out for its reduced transaction fees and broad acceptance in various transactions.

Namecoin [19] is a digital currency that serves as a decentralized name and censorship resistant domain registry service that allows for data storage on its dedicated blockchain. It is capable of registering bit domain names and storing associated values.

Peercoin [20] launched in 2012, is an alternative cryptocurrency based on the Bitcoin framework. It offers value storage, anonymity, and decentralized transactions. Peercoin pioneered the use of a hybrid proof-of-stake (PoS) and proof-of-work (PoW) consensus, combining energy efficiency with network security.

Ripple [21] is a cryptocurrency introduced by Ripple Labs Inc in 2013. The native XRP participates as a bridge currency on the Ripple network and facilitates exchanges of cryptocurrencies across borders, serving as an ecosystem medium for value transfer. It uses a consensus mechanism instead of mining to confirm transactions quickly. Ripple transactions are energy-efficient, fast, and cost-effective compared to Bitcoin.

Dogecoin [22] introduced in 2013, was introduced by Billy Markus and Jackson Palmer as an alternative to Bitcoin. Dogecoin utilizes the Proof of Work consensus mechanism, boasts a larger supply cap and has a faster block time of one minute, ensuring faster transaction confirmations in comparison to Bitcoin's ten-minute block time.

Primecoin [23] is a cryptocurrency launched in 2013 by Sunny King, the creator of Peercoin. It is an innovative digital currency that utilizes cryptography and decentralized mining. Inspired by Bitcoin, Primecoin introduces a novel proof-of-work mechanism centred around prime numbers. It is the first cryptocurrency designed to incorporate scientific computing as its primary function

Stellar [24] launched in 2014 by Jed McCaleb, is a decentralized ledger for transmitting digital currencies. Its native token is Stellar Lumens (XLM). Stellar utilizes a consensus algorithm that is faster, cheaper, and more energy-efficient compared to Bitcoin. However, critics argue that the Stellar blockchain is centralized due to the influence of the Stellar Development Foundation, which holds a significant portion of lumens tokens.

Monero [25] is an open-source cryptocurrency that prioritizes privacy by concealing transaction details and addresses. It offers CPU mining, eliminating the need for specialized hardware. While its privacy features have led to associations with illicit activities and the dark web, Monero also appeals to individuals seeking enhanced transaction confidentiality.

NEO [26] is a cryptocurrency and blockchain platform known as the "Chinese Ethereum." Initially launched as AntShares in 2014 and later rebranded as NEO in 2017, it aims to create a smart economy by digitizing real-world assets and implementing features like digital identity and smart contracts.

MIOTA (Mega Internet of Things Application) [27] is a cryptocurrency that operates on an open-source smart contract platform called IOTA designed specifically for seamless transactions among internet connected devices. The platform utilizes the MIOTA cryptocurrency tokens to facilitate transactions. It aims to enable frictionless value and data transfer between humans and machines within the Internet of Everything, a concept for the next generation of the digital revolution. With feeless transactions, tamper-proof data, and low resource requirements, IOTA provides a scalable distributed ledger suitable for powering the Internet of Things (IoT) without extensive infrastructure investments.

Ether [28] is the primary digital currency of the Ethereum blockchain, a decentralized and open-source platform recognized for its smart contract functionality. With a powerful market presence as the second largest cryptocurrency, Ethereum operates independently, facilitating the automatic execution of smart contracts based on predetermined conditions within its blockchain.

Zcash [29] is a cryptocurrency launched in 2016 by Zooko Wilcox which focuses on privacy, built upon the codebase of Bitcoin. It follows Bitcoin's model of a fixed total supply of 21 million units. Zcash transactions can either be transparent, resembling Bitcoin, or shielded, utilizing zero-knowledge proofs for enhanced anonymity. The option of "selective disclosure" allows users to prove payment for auditing purposes, aiding compliance with anti-money laundering and tax regulations for private transactors.

Firo [30], previously known as Zcoin, is a privacy-focused cryptocurrency launched in 2016 by Poramin Insom. It emphasizes user privacy and transaction anonymity, employing the Zerocoin protocol for encrypted transactions. With ongoing advancements, including the adoption of the Sigma protocol and preparations for a transition to Lelantus, Firo provides a privacy-centric alternative to other cryptocurrencies.

Cardono [31], also known as ADA, is a cryptocurrency utilized for digital transactions. It was developed by Charles Hoskinson and distinguishes itself through its "Scientific philosophy and research-driven approach." This means that the coin undergoes rigorous examination by scientists and programmers to ensure its reliability and integrity.

Binance coin [32] is the proprietary cryptocurrency of Binance, a renowned and widely used crypto exchange established in 2017. With a view to improving transactions and reducing fees, BNB was created exclusively on the Binance platform. It is finding extensive use in the Binance ecosystem for selling fees, coin sales and a variety of transactions on the BNBChain blockchain. BNB's value and popularity have soared, establishing it as a prominent cryptocurrency based on market capitalization.

Tezos [33] is a cryptocurrency and blockchain network that operates with its native digital token called Tez (XTZ). It enables user involvement in decentralized finance (DeFi), decentralized applications, and non-fungible token (NFT) initiatives. What distinguishes Tezos from other blockchains is its unique governance mechanism that eliminates the need for disruptive hard forks. Instead, Tezos employs a blockchain-based voting system where users can propose and adopt protocol upgrades based on their economic stake in the network. This approach ensures a more inclusive and streamlined development process for the Tezos ecosystem.

Terra [34] is a cryptocurrency that operates on the Terra blockchain network. It is a decentralized payment platform and blockchain protocol known for its algorithmic stablecoins. Terra's objective is to provide users with a stable and efficient medium of exchange, achieved through its ecosystem of stablecoins. These stablecoins, like TerraUSD (UST), maintain a steady value by dynamically adjusting their supply based on market demand. LUNA, the governance and staking token, enables users to engage in network governance and earn rewards by participating in network security through staking.

Algorand [35] is a cryptocurrency and decentralized blockchain network designed to support various applications, offering security, scalability, and efficiency. It enables computations with reliable performance guarantees, fostering new levels of trust.

Avalanche [36] is a prominent cryptocurrency known for its exceptional transaction speed of 4,500 TPS and scalability. It operates on a proof-of-stake mechanism and employs a unique three-layered blockchain system, making it a prime example for Web 3.0 applications. The platform's native token, AVAX, is extensively utilized for payments, security, and network connectivity within the Avalanche ecosystem.

Polkadot [37] is a cryptocurrency and blockchain project that seeks to provide a strong foundation for the development and integration of decentralized applications (dApps). Unlike focusing on specific applications, Polkadot aims to enable seamless communication between different blockchain ecosystems. It achieves this by acting as a network of networks, allowing diverse blockchain architectures to interact through specialized blockchains called parachains. The network utilizes a nominated proof-of-stake (PoS) consensus algorithm, drawing inspiration from the Ouroboros protocol.

DeSo [38] formerly known as BitClout, is a blockchain-driven social media platform and cryptocurrency. Its mission is to transform the landscape of social media by granting users direct ownership and authority over their content and influence. DeSo

functions as the intrinsic cryptocurrency of the DeSo blockchain, enabling users to engage in transactions such as buying, selling, and supporting creators and their content. The platform presents an opportunity for individuals to invest in public profiles and reap the benefits of their growth, effectively establishing a decentralized social economy. DeSo aspires to challenge conventional social media models by empowering users and offering them the means to monetize their online presence.

SafeMoon [39] is a recently introduced cryptocurrency that operates on the Binance Smart Chain (BSC) and offers distinctive tokenomics. One notable feature is an automatic liquidity generation and reflection system, where a portion of transaction fees is distributed to current token holders, encouraging them to retain their tokens. SafeMoon also implements static rewards and the automatic burning of tokens. The project has gained attention due to its community-oriented approach, but it is essential to exercise caution and conduct thorough research before considering any investments in cryptocurrencies.

2. LITERATURE REVIEW

In [1], P. K. Ozili conducted a global review of DeFi research and development, revealing the advantages and risks including smart contract execution and the potential for illicit activities. According to them, observations show rising interest in DeFi in Europe, US, Asia, and Oceania, but regulatory apprehensions prevail, especially in Asia and African nations with cryptocurrency limitations.

Y. Chen and C. Bellavitis [2] examined the advantages of decentralized finance, identified current business models, obstacles and constraints and showcased the potential of decentralization as a foundation for new business models. S. D. Santos et al. [7] provide an overview of key financial services in DeFi, comparing them to centralized counterparts, and discussed associated technical and economic risks.

In [8], F. Schär spotlighted the possibilities and potential hazards within DeFi ecosystem and introduced a comprehensive framework for assessing the underlying architecture and diverse components of DeFi, encompassing token standards, decentralized exchanges, decentralized debt markets, blockchain derivatives, and on-chain asset management protocols.

Huang et al. [9] discussed applications of DeFi like supply chain management, crowdfunding, lending, and stable currency, which are implemented on the Ethereum platform, and how they will significantly revolutionize these industries.

In [40], Spinoglio discussed the idea of restructuring the banking system, with a new monetary policy to address macroeconomic concerns and enhance the traditional banking system. The proposed solution utilizes blockchain technology and decentralized DeFi 2.0 protocols to establish a sustainable and liberated banking model.

In [41] Auer et al. discussed the evolution and the current state of DeFi markets, the risks and benefits of DeFi including key risks such as regulation and compliance, and challenges around the governance of DeFi. In [42], a comparative analysis of the acceptance of cryptocurrencies in China and India was conducted. While China has invested in blockchain and created its own centrally-issued digital currency. India's stance on cryptocurrencies and blockchain was found to be intricate.

In [43] Daniel Ramos et al. conducted a comprehensive analysis of the evolving landscape of decentralized finance and its crucial elements, recent historical developments, significant project categories, present status, future prospects, and its responsiveness to cryptocurrency market trends. In [44] Amler et al. examine the challenges and potential of DeFi, emphasizing its ability to create an inclusive and transparent financial system. The authors propose pathways for DeFi's growth, emphasizing lending, payments, and insurance. They emphasize the need for interoperability among DeFi applications and better user interfaces for DeFi to revolutionize finance and fulfil its potential.

In [45] Jensen et al. highlight the significance of understanding the potential consequences, complexities, and risks associated with the widespread adoption of consumer oriented DeFi applications. F. Carapella et al. [59] explored a broad range of risk implications of DeFi and stability challenges that emerge when offering financial services through blockchain technology. Additionally, it underscores specific issues that stem from the evolution of DeFi, particularly those related to managing the code governing decentralized applications.

In [60] U. W. Chohan conducts a rigorous assessment of significant aspects like market manipulation, distortionary incentives, excess short-termism, Ponzi schemes, and money-laundering challenges to counter DeFi's experimental and disintermediated financial practice.

The Table.1 provides a comparative study of similar work done by others. This study highlights the promising avenues of the applications of decentralized finance and the role of smart contracts and blockchain in its implementation. It examines the features, architecture, challenges and opportunities presented by DeFi, compares it to the traditional financial system through SWOT analysis and delves into the intricacies of the potential risks inherent in this domain. It provides a complete summary of the DeFi landscape for researchers, academicians and corporates who want to invest in it.

Section 3, provides a comprehensive explanation regarding decentralized finance encompassing its features, architecture, and the pivotal role played by smart contracts and blockchain. In section 4, we conducted a SWOT analysis comparing DeFi and CeFi applications. Section 5 explores several well-known dApps that are utilized in financial services. In section 6, we delve into the global adoption of decentralized finance in diverse countries. In section 7, we discuss the current status of adoption of DeFi applications across the world. In section 8, we list various types of risks and potential security considerations associated with decentralized finance. In section 9, we discuss the future of DeFi landscape.

Table.1. Comparative study of Related works

References	Features	Challenges	Opportunities	Architecture	Applications	Adoption	Threats/ risks
[1]			✓		✓	✓	✓
[2]	✓	✓					
[4]			✓		✓		✓
[7]			✓		✓		✓
[8]			✓	✓	✓		✓
[9]	✓				✓		
[40]	✓						✓
[41]				✓	✓		
[42]						✓	
[43]					✓		
[44]	✓	✓	✓		✓		
[45]				✓	✓		✓
[47]		✓			✓		✓
[59]					✓		✓
[60]					✓		✓
This Work	✓	✓	✓	✓	✓	✓	✓

3. METHODOLOGY

The research methodology employed in this study is qualitative and exploratory in nature, utilizing a comprehensive review of existing literature. The study analyzed data gathered from diverse secondary sources like financial reports, government websites, reputable commercial platforms, scholarly articles, and academic journals. Extensive examination and thorough analysis were performed on this data to shed light on the Challenges, opportunities, and threats within the decentralized finance industry.

4. DECENTRALIZED FINANCE (DEFI)

DeFi, is an incredibly dynamic and diverse sector that thrives on the revolutionary power of blockchain technology and financial systems. Blockchain is a decentralized and distributed digital ledger technology that records transactions across multiple computers in a secure and immutable manner. A decentralized ledger is a type of digital record-keeping system that operates in a distributed and decentralized manner. Blockchain consists of a chain of blocks, where each block contains a list of transactions, and each block is linked to the previous one using cryptographic principles. This design ensures that once data is added to the blockchain, it cannot be altered or deleted retroactively without altering all subsequent blocks, making it highly resistant to tampering and fraud. Within the realm of DeFi, an assortment of innovative financial instruments, protocols, and systems merge together, all fuelled by distributed, consensus-driven blockchains. In decentralized finance, consensus algorithms play a crucial role in achieving agreement among network participants on the validity of transactions and the state of the blockchain or decentralized ledger. Consensus algorithms ensure that all nodes in the network come to a common understanding and maintain a consistent and immutable record of transactions without the need for a central authority.

4.1 FEATURES OF DEFI

A collection of fundamental values that define DeFi's essence and set it apart from conventional financial systems serve as its guiding features. The following is a description of the features that serve as the foundation of the DeFi ecosystem. The Fig.3 represents some popular features of DeFi.

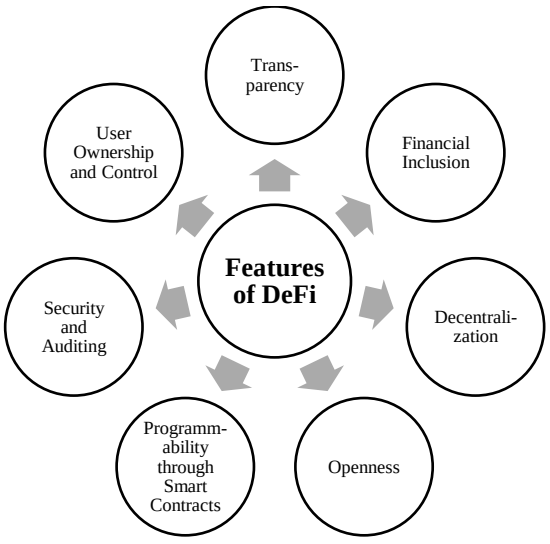

Fig.3. Features of DeFi

4.1.1 Decentralization:

DeFi operates on decentralized networks, utilizing blockchain systems. Its aim is to eliminate the need for trusted intermediaries,

in contrast to traditional finance which heavily relies on centralized entities such as banks and financial institutions. Decentralization [2], [9] in DeFi fosters autonomy and reduces dependence on centralized entities, eliminating concerns like single points of failure, censorship, and control over user funds. Participants have complete control over their assets, making decisions and conducting transactions without requiring approval from a central authority.

4.1.2 Openness:

DeFi promotes transparency, collaboration, and community-driven development [2]. The accessibility of DeFi protocols, codebases, and infrastructure allows anyone to investigate, contribute, and enhance the ecosystem. This transparency enables programmers, auditors, and researchers to evaluate the logic, security, and fairness of the protocols.

4.1.3 Transparency:

It is a fundamental principle in DeFi, made possible by the inherent advantages of blockchain technology. All financial transactions, smart contract codes, and protocol specifications are publicly documented on an open and immutable blockchain ledger. This openness promotes accountability, and trust, and addresses information asymmetry. Users can review smart contract codes, verify transaction history, and assess the integrity of the system. It enables individuals to evaluate risks in DeFi and make informed decisions. Transparency [2] also encourages auditability and community involvement, allowing participants to examine protocols, identify weaknesses, and propose improvements. This cooperative approach enhances the security and reliability of the DeFi ecosystem.

4.1.4 Programmability through Smart Contracts:

The programmability of smart contracts is a central aspect of DeFi, enabling the automation and execution of predefined conditions and actions. DeFi platforms can offer cutting-edge financial instruments and protocols because of these self-executing agreements built on blockchain platforms. Smart contracts enable a wide range of financial operations, including sophisticated transactions, lending, borrowing, and decentralized exchanges, without the need for intermediaries. DeFi reduces reliance on centralized institutions and promotes peer-to-peer interactions by ensuring efficient and transparent execution of financial procedures through smart contracts.

4.1.5 Financial Inclusion:

DeFi aims to address the exclusivity inherent in traditional financial systems by providing open and unrestricted access to financial services. With DeFi protocols operating on public blockchains, anyone with internet access can participate, conduct transactions, and utilize financial tools. The inclusive nature of DeFi's services allows individuals who are unbanked, underbanked or have limited access to financial services to benefit from its offerings. DeFi promotes economic growth, empowers marginalized communities, and bridges the global financial divide by fostering financial inclusion.

4.1.6 Security and Auditing:

Security and auditing are crucial in DeFi to ensure reliability, integrity, and trust. Robust security measures mainly based on cryptography, hashing algorithms, and digital signatures are implemented in DeFi protocols to safeguard user assets and data. Independent third-party firms conduct audits to identify vulnerabilities and potential exploits in smart contracts, which serve as the foundation of DeFi applications. Through these audits, risks are mitigated, and the overall security of DeFi platforms is enhanced, ensuring the protection of user funds from malicious activities.

4.1.7 User Ownership and Control:

User ownership and control are fundamental principles in DeFi, setting it apart from traditional financial systems that rely on centralized intermediaries. In DeFi, users have complete ownership and control over all their assets during financial transactions. They interact directly with protocols using blockchain technology and smart contracts, eliminating the need for intermediaries. Users retain ownership of their private keys, ensuring the confidentiality of their funds. They actively participate in decision-making processes through voting or consensus mechanisms. DeFi platforms offer consumers the flexibility to engage in various financial activities without stringent eligibility requirements or intermediaries' permission. User ownership and control in DeFi encourage financial independence, personal empowerment, and a superior user experience.

These guiding principles form the foundation for the creation and management of DeFi projects, shaping the decentralized financial ecosystem and advancing the goal of establishing a more accessible, inclusive, and transparent financial system.

4.2 DEFI ARCHITECTURE

DeFi protocols are divided into a number of layers according to their functionalities within the ecosystem. The DeFi layering system is not precisely defined, and there may be overlap or variation in the classification of various layers and protocols deployed. There are 5 recognized layers in DeFi [8] as shown in Fig.4.

4.2.1 Settlement Layer:

The settlement layer, also known as the infrastructure layer or base layer, embodies the underlying blockchain network that establishes the fundamental framework for decentralized finance. This layer comprises the blockchain itself and its native protocol asset like ETH on the Ethereum blockchain. It enables the secure storage of ownership information within the network and ensures the adherence of any changes in the system state to its predefined ruleset. The blockchain functions as the cornerstone for trustless execution, operating as a settlement and dispute resolution layer. It facilitates robust and decentralized transaction processing, consensus mechanisms, and the execution of smart contracts.

4.2.2 Asset Layer:

The asset layer comprises all the assets that are generated on the settlement layer. This encompasses the native protocol asset and any supplementary assets issued on the blockchain, commonly known as tokens. Tokenization protocols facilitate the representation of real-world assets (such as real estate, art, and commodities) as digital tokens on the blockchain. Synthetic asset protocols create assets that emulate the value or performance of other assets, enabling users to attain exposure without possessing the underlying asset directly. Stablecoin protocols are responsible

for furnishing price-stable cryptocurrencies, often pegged to a fiat currency or maintained through algorithmic mechanisms.

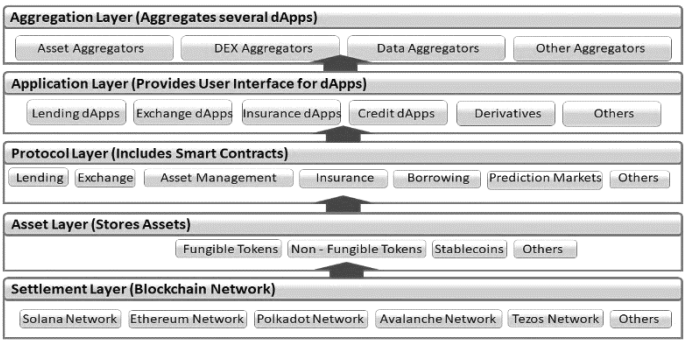

Fig.4. DeFi Stack [8]

4.2.3 Protocol Layer:

The protocol layer forms the foundational bedrock of DeFi, encompassing a multitude of decentralized protocols and smart contracts that facilitate precise financial functionalities. It establishes standardized frameworks for distinct use cases, such as decentralized exchanges, debt markets, derivatives, and on-chain asset management. These standards are typically implemented as a collection of smart contracts and are accessible to all users and DeFi applications. Consequently, these protocols exhibit a high degree of interoperability, enabling seamless integration and interaction across the DeFi ecosystem.

4.2.4 Application Layer:

The application layer of DeFi encompasses the user interfaces, applications, and decentralized applications (dApps) that enable users to interact with and leverage the functionalities offered by the underlying DeFi protocols. This layer facilitates the provision of user-friendly interfaces, often in the form of web-based interfaces, mobile apps, or dedicated dApps, which grant users access to features such as asset management, trading, lending, borrowing, yield farming, and more. The application layer creates user-centric applications that establish connections with individual protocols, while abstracting the smart contract interaction through web browser-based front ends, thereby enhancing the usability of the protocols

4.2.5 Aggregation Layer:

The aggregation layer focuses on platforms or aggregators that consolidate and integrate various DeFi protocols and services, extending the capabilities of the application layer. Aggregators construct user-centric platforms that establish connections with multiple applications and protocols. They typically offer tools to compare and rate services, enabling users to execute complex tasks by simultaneously interacting with several protocols, while presenting pertinent information in a concise and easily understandable manner. These platforms streamline the user experience by amalgamating liquidity, data, and services from multiple protocols into a unified interface. Aggregators assist users in identifying the optimal prices, routes, and opportunities across diverse protocols.

4.3 SMART CONTRACTS

The decentralized finance (DeFi) landscape has been significantly impacted by the revolutionary power of blockchain technology and smart contracts. DeFi, powered by the potential of smart contracts, aspires to upend conventional financial services by promoting inclusivity and creating solutions for their customers, regardless of their asset holdings. In order to understand how DeFi uses smart contracts, here is a step-by-step explanation:

4.3.1 Smart Contract Creation:

Programmers use blockchain programming languages to create smart contracts, such as Solidity for Ethereum. Specific financial operations, rules, conditions, logics, or protocols are defined by smart contracts.

4.3.2 Deployment on the Blockchain:

Smart contracts are deployed to blockchains once they have been written. A contract address is created on the blockchain corresponding to the contract's code. The contract address identifies the smart contract.

4.3.3 Interacting with the Smart Contract:

Smart contracts can be accessed by sending transactions to their blockchain addresses. Wallets that support blockchain transactions or web interfaces can be used for these types of interactions

4.3.4 Validation and Execution:

Blockchain networks verify the authenticity of transactions sent to smart contracts. The sender is verified to have the necessary funds and permissions. Based on the parameters of the transaction and the contract's code, a smart contract executes its predefined instructions.

Financial transactions are transparent, immutable, and automated using smart contracts on the blockchain powered by DeFi. With these characteristics, individual access to decentralized financial services is wide open, permissionless financial systems can be investigated, and assets can be managed without intermediaries.

4.4 BENEFITS OF SMART CONTRACTS AND BLOCKCHAIN TECHNOLOGY IN DEFI

Smart contracts and blockchain technology play crucial roles in the functioning of DeFi. The Fig.5 displays the benefits of using smart contracts and blockchain technology.

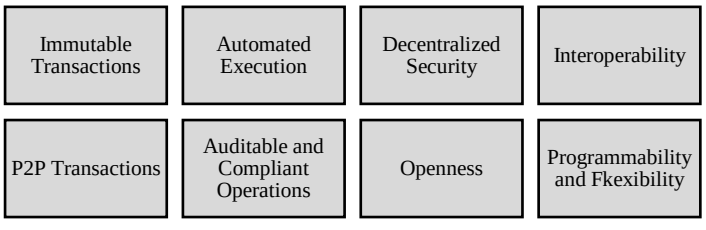

Fig.5. Benefits of Smart contracts and blockchain

4.4.1 Immutable Transactions:

Once recorded data cannot be easily corrupted as blockchain-based financial transactions are linked and secured through hashing algorithms which make sure that data cannot be altered once deployed. Immutability not only increases transparency and confidence but also makes it possible to audit and verify transactions and lowers the risk of fraud.

4.4.2 Automated Execution:

When certain circumstances are met, smart contracts completely execute themselves and carry out a prescribed set of operations. The efficiency of financial transactions and operations is increased because of this automation, which also decreases human involvement and eliminates potential errors.

4.4.3 Decentralized Security:

Smart contracts enforce the agreed-upon rules and enhance security and reduce the risk of malicious activity.

4.4.4 Interoperability:

With the help of smart contracts based on blockchain technology, different protocols, and applications can interoperate seamlessly. As a result of DeFi's platform's composability, financial products, and services can be created using multiple building blocks that are integrated and complex.

4.4.5 P2P Transactions:

P2P transactions are facilitated using smart contracts without the need for any intermediaries, unlike centralized finance. They eliminate counterparty risk. Using trustless transactions, users will be able to lend, borrow, trade, or provide liquidity directly to one another.

4.4.6 Auditable and Compliant Operations:

Smart contracts on the blockchain provide a transparent and auditable record of financial operations. Regulations and standards can be monitored and audited using this feature, which is especially useful for compliance purposes.

4.4.7 Openness:

Smart contracts and blockchain technology are open and accessible and provide a permissionless infrastructure. Any individual can participate in the DeFi ecosystem, create or use DeFi protocols, and access financial services, regardless of geographical location or centralized financial system limitations with a good internet connection.

4.4.8 Programmability and Flexibility:

Smart contacts are very flexible & programmable in nature, allowing developers to create sophisticated financial logic and customize the behaviour of DeFi applications. This flexibility enables the creation of various financial instruments and tools, lending protocols, decentralized exchanges, and other DeFi functionalities.

5. SWOT ANALYSIS

In this section we provide a comparative SWOT analysis of CeFi and DeFi applications. The Fig.6 provides a SWOT analysis of Centralized Finance applications and Fig.7 provides a SWOT analysis of Decentralized Finance applications.

Strengths	Weaknesses
• Provide Seamless customer services • Supports cross-chain services • Reduces excessive processing	• More Expensive • KYC is mandatory to access the Cefi Service • Less secure • Vulnerable • Monopolistic behaviour
Opportunities	**Threats**
• More Transparent financial transactions • Assist in the process of conducting audits • Established Regulatory framework and infrastructure	• Unpredictability and Inefficiencies • Higher security risk • Restricted financial freedom and autonomy

Fig.6. SWOT analysis of Centralized Finance applications

Strengths	Weaknesses
• Eliminates the need for intermediaries • More secure and permissionless • The user has sole control over the fund • Less expensive • Reduces inefficiency • DeFI data is tamper-proof, secure and auditable	• Lack of privacy • Delays in transaction due to higher complexity • Time and money consuming • Does not provide customer service • No centralized authority, volatility may be a problem
Opportunities	**Threats**
• Faster Transactions • Globally accessible through the internet • Provides transparency and the ability to track transactions • Promotes cross-chain interoperability • Greater Acceptability	• High-security risk and higher volatility • Smart contract risks • User error problem • No consumer protection • Privacy issue • DeFI's energy-intensive nature threatens environmental sustainability

Fig.7. SWOT analysis of Decentralized Finance applications

5.1 STRENGTH

The weaknesses of Centralized Finance (CeFi) lie in its higher costs due to intermediary fees, mandatory KYC requirements, security vulnerabilities, potential fraud and data corruption, and the risk of monopolistic behaviour. However, these weaknesses were resolved in DeFi. DeFi eliminates the need for intermediaries, resulting in lower costs and increased accessibility. It operates on a decentralized network, enhancing security through cryptographic protocols and providing a tamper proof and auditable system. Unlike CeFi, DeFi does not mandate KYC, ensuring greater privacy and inclusivity.

Users have complete control over their funds in DeFi, mitigating the risk of third-party mismanagement or fraud. Thus, the weaknesses of CeFi act as catalysts for the strengths exhibited in DeFi, including cost-efficiency, enhanced security, privacy, user control, and a more competitive and inclusive financial ecosystem [46]-[47].

5.2 WEAKNESS

The strengths of Centralized Finance (CeFi), such as providing seamless customer services, supporting cross-chain transactions, facilitating fiat-to-cryptocurrency exchanges, and reducing excessive processing, can transform into weaknesses

when compared to Decentralized Finance. DeFi does not have centralized authority and customer service in place, which makes it more difficult for users to use. The complexity of decentralized protocols can result in delays in transactions, posing a challenge to efficiency. Privacy concerns may also arise from DeFi's decentralized nature, as transactions are recorded on the blockchain. Furthermore, while DeFi aims to streamline operations, it may require a certain degree of time and further steps in some cases. Moreover, participants may risk their own security by being exposed to the intrinsic volatility of decentralized systems. As a result, the strengths of CeFi have become weaknesses of DeFi, highlighting the drawbacks of the decentralized model in terms of convenience, speed, privacy, complexity, and volatility.

5.3 OPPORTUNITY

The threat of centralized finance arises from higher security risks, limited financial freedom, and dependence on central authorities, despite being globally accessible through the Internet. However, these threats become opportunities for decentralized finance to address and provide alternative solutions. DeFi offers faster transactions compared to CeFi, leveraging blockchain technology. It provides transparency and traceability of transactions through immutable records on the blockchain. Furthermore, DeFi offers greater acceptability as it does not require a traditional bank account, expanding access to financial services and promoting financial inclusion. By addressing the limitations and inefficiencies of CeFi, DeFi creates an opportunity for a more efficient, transparent, and accessible financial ecosystem. Cross-chain interoperability in DeFi refers to the ability of different blockchain networks to seamlessly communicate, share data, and interact with one another. Cross-chain interoperability presents significant opportunities in the DeFi space. It refers to the seamless interaction and exchange of assets and data between different blockchain networks. It allows users to access and utilize decentralized finance applications and services across multiple blockchains, enhancing liquidity, expanding opportunities, and unlocking the potential for diverse financial activities. It's important to remember that attaining cross-chain interoperability is a challenging technological task. Numerous projects and protocols are currently creating ways to successfully connect various blockchains while upholding security and decentralization [48], [49].

5.4 THREATS

The opportunities presented by centralized finance, including more transparent financial transactions, assistance in conducting audits, and an established regulatory framework and infrastructure, can become threats for implementing decentralized finance. The lack of centralized control in DeFi introduces higher security risks, as the absence of a central authority increases the potential for vulnerabilities and attacks. Higher volatility in DeFi can lead to significant losses for investors, as price fluctuations can occur rapidly and without centralized interventions. The use of smart contracts in DeFi introduces the risk of coding errors or vulnerabilities that could be exploited. Additionally, the absence of consumer protection mechanisms and the potential for user errors pose risks to participants in DeFi. Privacy issues can also arise in DeFi, as blockchain transactions are generally transparent and visible to all participants. The energy-intensive mechanism in DeFi poses a significant environmental threat due to its larger carbon footprint compared to centralized systems. Neglecting sustainability concerns may lead to negative public perception, increased regulatory scrutiny, and hinder the growth of DeFi networks. Proactive measures, such as exploring energy-efficient consensus algorithms, are essential to address this issue. Therefore, while CeFi opportunities initially attract users, they also create concerns and threats when transitioning to the decentralized model of DeFi.

SWOT analysis of DeFi reveals its immense potential for transforming the financial landscape. Its strengths in accessibility, transparency, and empowerment make it an attractive alternative to traditional systems. However, it must address weaknesses related to scalability and regulatory uncertainty. By capitalizing on opportunities like decentralized lending and asset management, DeFi can shape the future of finance. Nevertheless, it must navigate threats such as regulatory challenges, security vulnerabilities, and market volatility. With continued innovation, collaboration, and adaptation, DeFi has the potential to revolutionize the way we think about and interact with finance.

6. DECENTRALIZED FINANCIAL APPLICATIONS

Decentralized applications, also known as dApps, refer to software applications that operate on blockchain technology or peer-to-peer platforms. Financial applications are software programs specifically created to access, facilitate, and secure personal or business financial data. Its purpose is to effectively manage, analyze, process, and store financial records and information. The Fig.8 shows some of the popular dApps used in financial services.

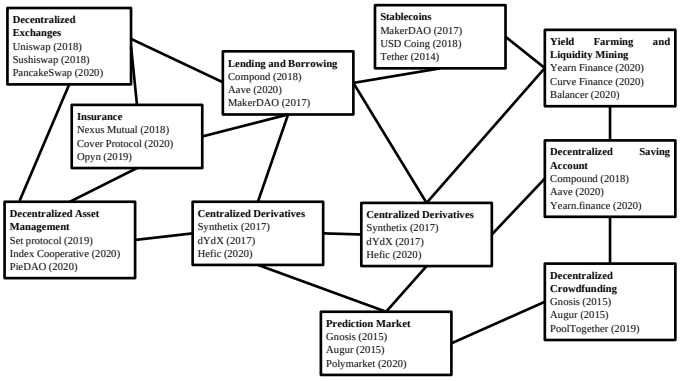

Fig.8. dApps based on DeFi

6.1 DECENTRALIZED EXCHANGES

DEXs (decentralized exchanges) [50]-[51] are trading platforms that improve the exchange of digital assets without a centralized authority. Instead of relying on traditional exchanges, they use a robust algorithm to dynamically update prices and execute trades based on available liquidity. These platforms typically use automated market makers (AMMs) to efficiently execute orders. Users can trade one cryptocurrency or token for another on these exchanges while maintaining full ownership and control of their crypto assets. Those who provide liquidity to token pools on these platforms will be rewarded.

Uniswap [52] operating on the Ethereum blockchain, holds the position of being the most extensive decentralized exchange (DEX). It enables global users to engage in cryptocurrency trading directly, eliminating the need for intermediaries or middlemen.

6.2 INSURANCE

DeFi insurance offers policyholders the opportunity to receive a significant compensation for covered events by paying a fixed premium. In this type of insurance, the entire life cycle, including risk assessment and management, for specific risks like smart contract attacks, is managed and coordinated using decentralized transaction and governance systems. Currently, there are decentralized insurance protocols operating on blockchain networks that provide on-chain coverage for various risks, allowing users to purchase protection against unintended use of code in any smart contract listed on the protocol.

Nexus Mutual [53] is a decentralized insurance application that offers individuals the opportunity to join and collectively bear risks. It offers various insurance products to its members, safeguarding them against different types of risks. Built on the Ethereum blockchain, the Nexus Mutual protocol serves as the foundation for members to acquire coverage, evaluate risks, process claims, and even establish risk management enterprises.

6.3 DECENTRALISED ASSET MANAGEMENT

Decentralized Asset Management [8], [43] in DeFi involves the management of digital assets through blockchain based protocols and smart contracts, bypassing conventional financial intermediaries. It gives individuals direct control over their assets, enabling them to invest in diverse financial products using self-executing smart contracts. These decentralized platforms ensure transparency and efficiency, automating investment choices without the need for banks or centralized entities.

6.4 STABLECOINS

Stablecoin plays a vital role in DeFi applications by providing stability and reducing the volatility commonly seen in cryptocurrencies such as Bitcoin and Ethereum. These digital assets are specifically designed to maintain a constant value by pegging themselves to specific assets or a combination of assets, ensuring a 1:1 value ratio with traditional currencies like the US Dollar. As a result, stablecoins are favoured in DeFi for enhancing liquidity in various aspects, including liquidity pools. Their steady value also makes them appealing to investors seeking consistent yields and a reliable choice for participating in DeFi.

USD Coin (USDC) [54] is a stablecoin that maintains a fixed value, always equivalent to one U.S. Dollar. This ensures that the worth of one USDC remains constant and equal to one dollar at all times.

6.5 LENDING AND BORROWING

In DeFi lending and borrowing play crucial roles within the rapidly expanding decentralized financial ecosystem [7], [8], [47]. These innovative applications utilize blockchain technology and smart contracts, allowing users to lend their cryptocurrencies and earn interest or borrow assets with collateral. Users deposit digital assets into lending protocols, contributing to liquidity pools accessible by borrowers. Borrowers can then obtain loans by providing collateral from these pools, and lenders earn interest on their deposited assets. Smart contracts efficiently manage interest payments, collateral requirements, and other aspects, ensuring transparency and effectiveness without intermediaries. These DeFi lending and borrowing platforms foster financial inclusion and empower users to access loans and generate passive income while retaining control over their assets. Nonetheless, users must be cautious of associated risks with DeFi protocols and conduct thorough research before engaging in these activities.

MakerDAO [55] is one of the pioneering DeFi protocols that holds the distinction of being the first Ethereum based project to provide secure and dependable lending services. With its peer-to-peer structure, MakerDAO leverages blockchain technology for creating innovative solutions in cryptocurrency borrowing, saving, and lending. Through its platform, users can access a robust ecosystem that facilitates decentralized financial transactions while promoting transparency and trust.

6.6 DECENTRALIZED DERIVATIVES

DeFi brought a revolutionary change to the financial world by introducing tokenized derivatives on the Ethereum blockchain. These derivatives [8] are usually linked to an underlying asset, and their value fluctuates based on the performance of that asset. DeFi derivatives offer the flexibility to represent a wide range of real-world assets, including bonds, currencies, commodities, and cryptocurrencies. Through the use of DeFi derivatives, people can securely gain exposure to various financial instruments and assets.

6.7 YIELD FARMING & LIQUIDITY IN DEFI

Yield farming, also known as liquidity mining, involves users supplying liquidity to DeFi protocols by depositing funds into liquidity pools. As compensation, they receive rewards in the form of additional tokens or fees generated by the protocol. This practice enables individuals to generate passive income by actively participating in the DeFi ecosystem and contributing to the liquidity of diverse protocols Liquidity in DeFi refers to the ample availability and extensive variety of tradable assets within a market. In the context of decentralized exchanges (DEXs) and lending platforms, liquidity plays a critical role in ensuring the efficient operation of these protocols. Users have the opportunity to provide liquidity by depositing their digital assets into liquidity pools, where others can access them for trading or borrowing purposes. In return for their contribution, liquidity providers receive rewards or fees. Liquidity serves as a fundamental element for promoting smooth market operations, establishing price stability, and facilitating the provision of various financial services within the DeFi ecosystem.

6.8 DECENTRALIZED SAVING ACCOUNT

In DeFi, a decentralized savings account enables users to securely store and earn interest on digital assets through blockchain and smart contracts. By depositing cryptocurrencies into a smart contract, users can automatically earn interest based on predefined rules, with interest rates determined algorithmically by the platform's supply and demand factors. This decentralized method offers enhanced control, transparency, and accessibility compared to traditional bank-provided savings accounts.

6.9 DECENTRALIZED CROWDFUNDING

Decentralised crowdfunding, also known as blockchain based fundraising, is an innovative method of generating money that uses cryptocurrencies and blockchain technology to enable direct communication between project creators and backers. By using smart contracts, creators can specify their project details and funding objectives, while backers can make contributions directly to the project's smart contract address. This transparent and secure process eliminates the involvement of middlemen, resulting in lower fees and increased accountability. By embracing decentralized crowdfunding, creators gain the ability to reach a global audience and foster community participation.

6.10 DECENTRALIZED IDENTITY

Decentralized identity is a concept that seeks to give individuals greater control over their digital identities and personal data through the use of decentralized systems and blockchain technology. Decentralized identity enables individuals to determine their own identities, unlike the conventional identification systems that depend on centralized databases and trusted intermediaries. Through the use of cryptographic keys and blockchain, users can establish unique and verifiable digital identities, known as self-sovereign identities. These self-sovereign identities, represented by Decentralized Identifiers, offer users complete ownership and authority over their identity information, ensuring advanced security and the ability to selectively share data.

6.11 PREDICTION MARKET

The advent of prediction markets has profoundly impacted the realm of decentralized finance, ushering in a new era of speculation where participants can engage in a wide array of events, ranging from elections and sports outcomes to cryptocurrency price movements. These markets operate on the robust foundation of blockchain technology, employing smart contracts to create decentralized and transparent platforms. Within these platforms, users can trade prediction tokens that signify the probability of specific outcomes. This innovative approach empowers users to contribute real-time information, thereby fostering a collective intelligence that informs decision making. As a result, DeFi prediction markets facilitate more precise forecasts and risk evaluations, leading to heightened efficiency and liquidity within the ecosystem. In effect, participants are now equipped with novel financial instruments and opportunities to leverage the power of these prediction markets.

Augur [56] is one of the earliest and most well-known decentralized prediction market platforms. It enables users to create and participate in prediction markets on various events using the Ethereum blockchain.

Polymarket [57] is a prediction market platform that gained popularity in 2020. It allows users to speculate on various topics, including political events, sports outcomes, and more, using blockchain technology.

7. ADOPTION OF DEFI

The adoption of DeFi has been growing rapidly in recent years. One of the main driving forces behind its adoption is the potential for greater financial inclusivity which leads to a greater level of accessibility to the financial services. It has been observed that the total value locked in DeFi protocols has increased significantly over the past few years. An indicator of adoption is how many cryptocurrency assets are locked into DeFi applications, which is called TVL. Users are increasingly recognizing the opportunity in DeFi and investing their assets in a variety of protocols, including decentralized exchanges, yield farming, and liquidity providers. In developing countries, individuals without access to banking services may find traditional financial systems to be out of reach. Many countries are not allowing decentralized finance to mature in their country and have banned it despite having a good banking system.

Cryptocurrency, a type of digital or virtual currency that relies on cryptography for security and operates independently of a central bank, has garnered substantial global attention and popularity. Many jurisdictions are still debating or are in the process of changing the legal status of cryptocurrencies. While cryptocurrency usage is not illegal in most countries, its status and usability as a means of payment (or as a commodity) varies greatly, with differing regulatory implications. The legal status of cryptocurrency varies across countries and is subject to continuous regulatory developments [58].

In numerous nations like the United States and Canada, cryptocurrency is generally acknowledged as a legal form of currency, accompanied by regulations that govern its use and trade. These regulations primarily concentrate on concerns such as money laundering, taxation, and safeguarding consumers. In the United States, for example, there exists a comprehensive framework for cryptocurrency, overseen by regulatory bodies such as the Securities and Exchange Commission (SEC) and the Financial Crimes Enforcement Network (FinCEN). In contrast, Canada has embraced a more progressive stance by recognizing cryptocurrency as a legitimate method of payment and implementing regulations to ensure its proper operation [58].

In Europe, countries such as Germany and the United Kingdom have acknowledged the legality of cryptocurrency and have put in place regulatory measures to enable its utilization. Germany treats cryptocurrency as a recognized unit of account, permitting individuals and businesses to conduct transactions using digital currencies like Bitcoin. Similarly, the United Kingdom has implemented regulatory guidelines specifically targeting cryptocurrency exchanges and custodian wallet providers to counteract money laundering and prevent terrorist financing [58].

In Asia, Japan has emerged as a significant participant in the cryptocurrency realm by officially recognizing it as a legal form of tender. The country has established a comprehensive regulatory framework to oversee cryptocurrency exchanges, implement measures for consumer protection, and ensure appropriate governance. On the other hand, South Korea, while legalizing cryptocurrency, has imposed stringent regulations to combat illegal activities and safeguard investors. These regulations include requirements such as Know Your Customer (KYC) procedures and the use of real-name banking accounts.

Nevertheless, there are countries that have not embraced cryptocurrency. Bolivia has completely prohibited cryptocurrency, deeming it illegal and forbidding its usage in any way. Similarly, Nepal has implemented a blanket ban on cryptocurrency transactions. Certain countries, such as China and India, have adopted restrictive measures and taken strong actions against cryptocurrency trading and initial coin offerings (ICOs) due to concerns surrounding financial stability and the potential for illicit activities.

Several countries find themselves in a grey area regarding cryptocurrency, where its legal status is neither explicitly permitted nor prohibited. These countries, such as Australia, Brazil, France, and Russia, have issued cautionary warnings concerning the risks associated with cryptocurrency transactions and encourage individuals to exercise prudence. Additionally, they are currently in the process of formulating regulatory frameworks to tackle the challenges and capitalize on the opportunities presented by cryptocurrencies [58].

It is important to highlight that the legal status of cryptocurrency can undergo rapid changes as governments and regulatory bodies frequently reassess their positions in light of the increasing impact of this digital asset. Consequently, it is vital for individuals and businesses involved in the cryptocurrency industry to remain informed about the most recent legal developments in their specific jurisdictions.

Overall, the legality of cryptocurrency varies worldwide, ranging from acceptance and regulation to complete prohibition, reflecting the diverse approaches taken by different countries and territories in adapting to this emerging form of currency. The landscape of cryptocurrency regulations is dynamic and constantly evolving, shaping the future of this digital financial ecosystem.

8. RISK ANALYSIS

DeFi presents a multitude of advantages, but it is imperative to acknowledge the accompanying uncertainties and potential security concerns. The Fig.9 displays the different types of risks and potential security considerations related to decentralized finance.

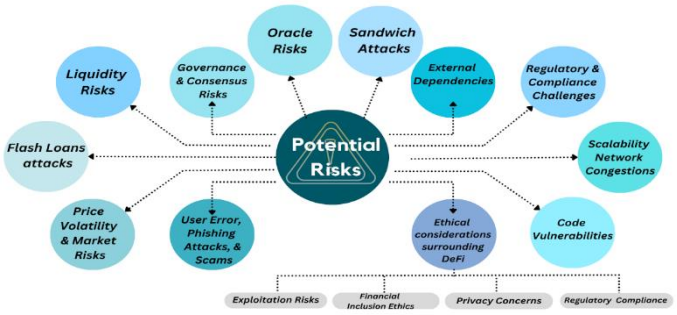

Fig.9. Risk and Security Considerations of DeFi

8.1 CODE VULNERABILITIES AND SMART CONTRACTS VULNERABILITIES

Smart contracts [8], [47] are intricate pieces of code, and if they are not meticulously audited or tested, they may harbour vulnerabilities that could be exploited. Flaws or loopholes in the code have the potential to result in financial losses or hacking incidents. These risks stem from coding errors, design flaws, and malicious intent, leading to potential exploits such as re-entrance attacks, where a contract can be called repeatedly before it completes previous executions, enabling attackers to drain funds. Other threats include arithmetic overflows, improper input validation, and weak access controls, allowing unauthorized access to sensitive functions.

DeFi's interconnected nature exacerbates the impact of any smart contract breach, highlighting the need for thorough audits, formal verification, and continuous monitoring to bolster the robustness of smart contracts and fortify the security of DeFi platforms. To mitigate these risks, extensive code auditing, formal verification, and rigorous testing are indispensable.

8.2 SCALABILITY AND NETWORK CONGESTION

As the popularity of DeFi surges, the surge in network congestion and scalability issues could ensue, leading to increased transaction fees & slower confirmation times. These challenges can affect the usability & cost-effectiveness of DeFi applications. Blockchain networks, particularly those experiencing high levels of activity like Ethereum, may encounter scalability obstacles. Continuous efforts are being made to enhance blockchain scalability [8].

8.3 REGULATORY AND COMPLIANCE CHALLENGES

The regulatory landscape surrounding DeFi is still evolving, with different jurisdictions adopting varying approaches [7]. As the industry matures, the possibility of heightened scrutiny, regulatory interventions, or changes in regulations that may impact the operation of DeFi protocols and applications increases. Compliance with existing regulations and adaptation to new regulatory requirements which will be crucial for ensuring the long-term viability of DeFi projects. In a decentralized environment, compliance with existing financial regulations like KYC (Know Your Customer) and AML (Anti-Money Laundering) can be arduous [7]. Striking a balance between innovation and regulatory compliance remains an ongoing consideration.

8.4 EXTERNAL DEPENDENCIES

While smart contracts are self-executing, they often interact with external data oracles to access off-chain information [8]. Relying on these oracles introduces potential security risks if they are compromised or manipulated. Efforts are underway to develop secure and decentralized oracle solutions to mitigate these risks.

8.5 USER ERROR, PHISHING ATTACKS, AND SCAMS

DeFi platforms frequently require users to manage their private keys, navigate unfamiliar interfaces, and make complex financial decisions. This elevates the risk of user error, including inadvertent loss of funds or falling prey to scams. Addressing these challenges necessitates robust education and user-friendly interfaces. User errors such as typographical errors in addresses or improper security practices can result in irretrievable loss of funds. Phishing attacks, fraudulent websites, and fake token

offerings also pose risks that users must remain vigilant about [7]. Adequate education, appropriate security measures, and user-friendly interfaces can help mitigate these risks.

8.6 PRICE VOLATILITY AND MARKET RISK

DeFi tokens and assets can exhibit high volatility, subject to rapid price fluctuations. This volatility introduces risks for investors and users alike. Price manipulation, pump-and-dump schemes, and market speculation can impact the value and stability of DeFi assets. Before engaging in DeFi activities, investors and users must carefully evaluate and manage these risks, taking into account factors such as market liquidity, token supply, and project fundamentals. Diversification and risk management strategies can help mitigate the impact of price volatility.

8.7 GOVERNANCE AND CONSENSUS RISKS

Many DeFi protocols rely on decentralized governance mechanisms, involving token holders in decision-making processes [8]. However, this presents risks related to governance attacks, manipulation of voting systems, or the concentration of power among influential stakeholders. Malicious actors could amass a significant number of tokens to influence decisions or manipulate protocol parameters. Mitigating these risks and ensuring fair decision-making processes in DeFi protocols necessitates effective governance frameworks, transparent voting mechanisms, and strong community engagement.

8.8 LIQUIDITY RISKS

DeFi protocols heavily depend on liquidity providers to facilitate trading and maintain efficient markets. Insufficient liquidity or sudden withdrawal of liquidity can lead to price slippage, reduced trading opportunities, and potential losses for users. Additionally, low liquidity can hinder users from entering or exiting positions without significantly impacting market prices [8]. Well-designed tokenomics, incentivization mechanisms, and liquidity management strategies are essential to maintain adequate liquidity and mitigate risks associated with liquidity fluctuations in DeFi protocols.

8.9 ORACLE RISKS

In the dynamic landscape of DeFi, the term "oracle risk" highlights a critical concern rooted in the dependence on external data sources to initiate automated smart contract actions [3], [59]. Within DeFi ecosystems, smart contracts play a pivotal role in executing transactions based on real-world data, such as asset prices. However, the susceptibility arises when these Oracle data streams are compromised or tampered with, potentially enabling malicious entities to exploit this vulnerability and manipulate contract outcomes to their advantage. The resulting financial losses for users emphasize the utmost importance of making judicious choices in adopting robust and reliable Oracle solutions. Doing so becomes instrumental in upholding the integrity of DeFi protocols, thwarting potential disruptions, and fortifying the overall stability of the DeFi space.

8.10 SANDWICH ATTACKS

A sandwich attack exploits token price volatility by swiftly conducting transactions on both sides of a targeted trade. Some DeFi platforms attract potential participants with the promise of high-interest rate instruments. Nevertheless, it's crucial to view these offerings within a risk-adjusted framework. Despite their appealing high interest rates, especially in today's low-inflation and low-interest rate environment, they also come with questionable risks. [60] Sandwich attack is a form of price manipulation attack that occurs in a short period around a transaction, particularly in the context of Automated Market-Making (AMM) platforms [61]. In this manoeuvre, a malicious actor strategically places substantial buy and sell orders around a legitimate trader's transaction, seeking to profit from the price fluctuations triggered by the trader's move. By essentially "sandwiching" the genuine trade, the attacker induces the trader to buy or sell at an unfavourable rate due to the momentary price distortion arising from the attacker's rapid manoeuvres. This technique has the potential to lead to financial setbacks for the unsuspecting trader, underscoring the imperative for robust strategies that counter such susceptibilities within DeFi ecosystems.

8.11 FLASH LOANS ATTACKS

Flash loans [47] pose a serious threat to the DeFi ecosystem as they lack collateral and offer borrowers the means to exploit price disparities and manipulate markets within a single transaction block. These loans are a type of price manipulation attack [62]. Such loans can pave the way for arbitrage attacks, market manipulation, and oracle exploits, resulting in significant losses for other participants and draining liquidity from the underlying protocols. Furthermore, discovering smart contract vulnerabilities during the loan period opens the door for malicious users to inflict further harm. Although certain platforms attempt to implement limitations, the simplicity of accessing flash loans makes them an alluring instrument for potential attackers, necessitating ongoing security measures and utmost vigilance when engaging with such loans in the DeFi space.

8.12 ETHICAL CONSIDERATIONS SURROUNDING DEFI

DeFi offers numerous advantages, it also raises several ethical considerations, including potential risks of exploitation, financial inclusion ethics, and privacy concerns. Let's delve into each of these aspects:

8.12.1 Exploitation Risks:

DeFi platforms, driven by self-executing smart contracts with predefined rules, facilitate a wide range of financial activities, including lending, borrowing, and trading. The allure of reducing intermediaries and enhancing transparency through smart contracts is tempered by their susceptibility to exploits and attacks. The staggering financial losses witnessed in previous DeFi hacks underscore the gravity of smart contract bugs or vulnerabilities. Especially those users who are less familiar with technology, find themselves unintentionally involved in these risks due to the uncertain nature of these complexities. Minimizing the threat of exploitation necessitates paramount

importance to security audits, comprehensive testing, and robust disclosures by DeFi developers and platform operators.

8.12.2 Financial Inclusion Ethics:

DeFi opens its virtual doors to anyone with an internet connection, it presumes users possessing indispensable technology are aware of how to engage in it meaningfully. Consequently, a digital gap emerges, further marginalizing vulnerable communities. Tackling this issue demands that DeFi platforms embrace user-friendly interfaces, empower with educational resources, and fortify support systems, thereby ensuring genuine accessibility to a diverse populace. Moreover, it is essential to implement strict measures to prevent any exploitative actions aimed at financially vulnerable individuals.

8.12.3 Privacy Concerns:

Every transaction in the realm of decentralized finance is recorded on immutable public blockchains, creating a transparent audit trail [47]. Although this quality is meant to foster confidence and strengthen monitoring, it paradoxically raises concerns about individual privacy. Users are put at risk by free access to financial data since it may reveal their whole financial history and portfolio, making them vulnerable to malicious groups. This dangerous breach of confidentiality seriously affects people living in places with restrictive fiscal laws or oppressive governments. DeFi systems must thus quickly implement cutting-edge privacy-enhancing technology, such as zero-knowledge proofs or anonymity-preserving blockchain networks, in order to protect user data and give them complete control over their financial information.

8.12.4 Regulatory Compliance:

DeFi works in a highly unregulated industry, and this may have positive and negative consequences. On the one hand, it promotes financial inclusiveness and accessibility by enabling quick innovation and experimentation. On the other hand, it can encourage fraudulent individuals to take advantage of the system without being held accountable. An important ethical issue involves figuring out how to strike a balance between innovation and regulatory oversight. Concerns concerning compliance may be addressed without limiting innovation with the support of responsible self-regulation by DeFi initiatives and industry participants and cooperation with regulatory organizations.

Participants in the DeFi ecosystem, including investors, users, and developers, must be aware of these risks and implement appropriate risk management strategies. Diligence, continuous monitoring, security audits, and community engagement are vital for identifying and addressing these risks. Additionally, regulatory frameworks and industry standards are evolving to address some of these concerns and enhance the overall security and stability of the DeFi space.

9. CONCLUSION

Currently, the DeFi industry is in its infancy but is constantly evolving despite many apprehensions regarding its adoption. A lot of research and development work is being done to promote DeFi applications and many such applications are running successfully. In this paper, we analyzed the various fields and applications where DeFi is being currently utilized, in which form, and how it will transform financial transactions of the future. We also did a risk analysis of its adoption and found out the driving reasons such as regulatory challenges, Financial stability concerns, Loss of control and lack of Monetary policy, Tax Evasion, & Illicit Activities, and most importantly customer protection as main reasons why some governments are fearing to adopt it. The risks such as Code Vulnerabilities and Smart Contracts Vulnerabilities, Scalability, Network Congestion, Regulatory and Compliance Challenges, External Dependencies, User Error, Phishing Attacks, and Scams, Price Volatility and Market Risks, Governance Consensus Risks, and Liquidity Risks in the DeFi Ecosystem makes it a cause of threat to privacy. Overcoming these risks and challenges will be crucial for DeFi adoption.

9.1 FUTURE OF DEFI

The future of DeFi is incredibly promising and filled with potential. Its ongoing development positions DeFi to play a pivotal role in reshaping the financial sector, fundamentally transforming conventional financial services. The general public and governments are looking towards its adoption and use in future financial applications with a lot of anticipation and curiosity. Despite the risks involved, the future of DeFi still looks bright, with improved scalability, widespread acceptance, regulatory clarity, and introduction of the new avenues of DeFi. Over time, there will be an increase in DeFi exchange offerings which will accelerate the trend toward alternative protocols, scaling, and infrastructure solutions. Opportunities for DeFi innovation are abundant, opening the door to new and improved methods to serve clients. DeFi has the capacity to democratize finance, granting broader global access to financial offerings, especially for individuals currently underserved by conventional banking systems. However, to reach its full potential and become a more mainstream and inclusive financial ecosystem, it must overcome challenges and obstacles, such as regulatory hurdles, scalability constraints, and requirements for user-friendly interfaces.

ACKNOWLEDGMENT

We extend our sincere thanks to the Centre for Research at Maitreyi College for their unwavering support, guidance, and resources. Their contribution has been invaluable in shaping this work and nurturing our passion for research.

REFERENCES

[1] P. K. Ozili, “Decentralized Finance Research and Developments around the World”, *Journal of Banking and Financial Technology*, Vol. 6, No. 2, pp. 117-133, 2022.

[2] Y. Chen and C. Bellavitis, “Decentralized Finance: Blockchain Technology and the Quest for an Open Financial System”, *Stevens Institute of Technology School of Business Research Paper*, pp. 1-27, 2019.

[3] K. Nath, “ CeFi, Fintech, and DeFi - Understanding the Benefits, Limitations, and Challenges”, Available at https://www.techrxiv.org/articles/preprint/CeFi_Fintech_and_DeFi_Understanding_the_Benefits_Limitations_and_Challenges/22274371, Accessed in 2023.

[4] C.R. Harvey, A. Ramachandran and J. Santoro, "*DeFi and the Future of Finance*", John Wiley and Sons, 2021.
[5] Puschmann, "Fintech", *Business and Information Systems Engineering*, Vol. 59, No. 1, pp. 69-76,2017.
[6] L. Zavolokina, M. Dolata and G. Schwabe, "FinTech - What's in a Name?", *Proceedings of International Conference on Information Systems*, pp.1-6, 2016.
[7] S.D. Santos, J. Singh, R.K. Thulasiram, S. Kamali, L.J. Sirico and L. Loud, "A New Era of Blockchain-Powered Decentralized Finance (DeFi)-A Review", *Proceedings of International Conference on Annual Computers, Software, and Applications*, pp. 1286-1292, 2022.
[8] F. Schar, "Decentralized Finance: on Blockchain- and Smart Contract-Based Financial Markets", *FRB of St. Louis Review*, Vol. 103, No. 2, pp. 1-11, 2021.
[9] H. Teng, W. Tian, H. Wang and Z. Yang, "Applications of the Decentralized Finance (DeFi) on the Ethereum", *Proceedings of IEEE Asia-Pacific Conference on Image Processing, Electronics, and Computers*, pp. 573-578, 2022.
[10] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Available at https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf, Accessed in 2008.
[11] World Economic Forum, "What's Behind China's cryptocurrency Ban? Global Agenda: The Agenda is Weekly", Available at https://www.weforum.org/agenda/2022/01/what-s-behind-china-s-cryptocurrency-ban/, Accessed in 2023.
[12] Cryptonews, "Countries where Bitcoin is Banned or Legal in 2023", Available at https://cryptonews.com/guides/countries-in-which-bitcoin-is-banned-or-legal.htm, Accessed in 2023.
[13] Wikipedia, "Bitcoin in El Salvador", Available at https://en.wikipedia.org/wiki/Bitcoin_in_El_Salvador, Accessed in 2023.
[14] Times of India, "Central African Republic becomes the Second Country to Adopt Bitcoin as Legal Tender", Available at indiatimes.com, Accessed in 2023.
[15] T.R. Sankar, "Cryptocurrencies - An Assessment", Proceedings of Indian Banks Association Conference on Annual Banking Technology Conference and Awards, Reserve Bank of India, pp. 1-12, 2022.
[16] The Indian Express, "FE Digital Currency (2022, August). 115 Million Indians have Invested in Cryptocurrency with a Sentiment to Gain Long-Term Returns: Report", Available at:https://www.financialexpress.com/blockchain/115-million-indians-have-invested-in-cryptocurrency-with-a-sentiment-to-gain-long-term-returns-report/2641525/, Accessed in 2023.
[17] Bitcoin, Available at https://bitcoin.org/en/, Accessed in 2023.
[18] Litecoin, Available at https://litecoin.com/en/, Accessed in 2023.
[19] Namecoin, Available at https://www.namecoin.org/, Accessed in 2023.
[20] Peercoin, Available at https://www.peercoin.net/, Accessed in 2023.
[21] Ripple, Available at: https://crypto.com/price/xrp, Accessed in 2023.
[22] Dogecoin (DOGE), Available at https://dogecoin.com/, Accessed in 2023.
[23] Primecoin (XPM), Available at https://primecoin.io/, Accessed in 2023.
[24] Stellar, Available at https://stellar.org/, Accessed in 2023.
[25] Monero, Available at https://www.getmonero.org/, Accessed in 2023.
[26] NEO, Available at https://neo.org/, Accessed in 2023.
[27] IOTA, Available at https://www.iota.org/, Accessed in 2023.
[28] Ethereum, Available at https://ethereum.org/en/, Accessed at 2023.
[29] Zcash, Available at https://z.cash/, Accessed in 2023.
[30] Firo, Available at https://firo.org/, Accessed in 2023.
[31] Cardono, Available at https://cardano.org/, Accessed in 2023.
[32] Binance Coin, Available at https://accounts.binance.com/e, Accessed in 2023.
[33] Tezos, Available at https://tezos.com/, Accessed in 2023.
[34] Terra, Available at https://www.terra.money/, Accessed in 2023.
[35] Algorand, Available at https://algorand.com/, Accessed in 2023.
[36] Avalanche, Available at https://www.avax.network/, Accessed in 2023.
[37] Polkadot, Available at https://polkadot.network/, Accessed at 2023.
[38] DeSo, Available at https://bitclout.com/, Accessed in 2023.
[39] Safe Moon, Available at https://safemoon.com/, Accessed in 2023.
[40] F. Spinoglio, "Redefining Banking through Defi: A New Proposal for Free Banking based on Blockchain Technology and Defi 2.0 Model", *Journal of New Finance*, Vol. 2, No. 4, pp. 1-12, 2022.
[41] R. Auer, B. Haslhofer, S. Kitzler, P. Saggese and F. Victor, "The Technology of Decentralized Finance (DeFi)", *Bank for International Settlements, Monetary and Economic Department*, Vol. 1066, pp. 1-36, 2023.
[42] V. Shakya, P.P. Kumar, L. Tewari and Pronika, "Blockchain based Cryptocurrency Scope in India", *Proceedings of International Conference on Intelligent Computing and Control Systems*, pp. 361-368, 2021.
[43] D. Ramos and G. Zanko, "A Review of Decentralized Finance as an Application of Increasing Importance of Blockchain Technology", Available at https://static1.squarespace.com/static/553d790de4b08ceb08ab88fd/t/5f5037549883d84929c20ace/1599092566315/DeFi_SciPaper_Final.pdf, Accessed in 2020.
[44] H. Amler, L. Eckey, S. Faust, M. Kaiser, P. Sandner and B. Schlosser, "DEFI-ning DEFI: Challenges and Pathway", *Proceedings of International Conference on Blockchain Research and Applications for Innovative Networks and Services*, pp. 181-184, 2021.
[45] J. R. Jensen, V. Von Wachter and O. Ross, "An Introduction to Decentralized Finance (DEFI)", *Complex Systems Informatics and Modelling Quarterly*, Vol. 26, pp. 46-54, 2021.

[46] Tech Target, "Decentralized Finance vs. Centralized Finance: What's the Difference?", Available at https://www.techtarget.com/whatis/feature/Decentralized-finance-vs-centralized-finance-Whats-the-difference, Accessed in 2023.

[47] K. Qin, L. Zhou, Y. Afonin, L. Lazzaretti and A. Gervais, "CeFi vs. DeFi - Comparing Centralized to Decentralized Finance", *Proceedings of International Conference on General Finance*, pp. 1-18, 2021.

[48] A. Rejeb, K. Rejeb and J.G. Keogh, "Centralized vs. Decentralized Ledgers in the Money Supply Process: A SWOT Analysis", *Quantitative Finance and Economics*, Vol. 5, No. 1, pp. 40-66, 2021.

[49] Analytics Insight, "Top 10 Opportunities and Risks of Decentralized Finance", Available at https://www.analyticsinsight.net/top-10-opportunities-and-risks-of-decentralized-finance/, Accessed in 2023.

[50] D. Jindawattana, "Problems in the Regulation of Decentralized Finance (DeFi) in the EU", Master Thesis, Department of Banking and Finance, University of Zurich, pp. 1-98, 2022.

[51] 101 Blockchain, "30+ Best Decentralized Finance Applications", Available at https://101blockchains.com/decentralized-finance-applications, Accessed in 2023.

[52] Uniswap, Available at https://uniswap.org, Accessed at 2023.

[53] Nexusmutual, Available at https://docs.nexusmutual.io/overview/, Accessed in 2023

[54] USD Coin, Available at https://www.circle.com/en/usdc, Accessed in 2023.

[55] Blockchain Council, "What is maker DAO and How Does it Works?", Available at https://www.blockchain-council.org/dao/makerdao/, Accessed in 2023.

[56] Augur, Available at https://augur.net/, Accessed in 2023.

[57] Polymarket, Available at https://polymarket.com/, Accessed in 2023.

[58] Wikipedia, "List of Cryptocurrencies", Available at https://en.m.wikipedia.org/wiki/List_of_cryptocurrencies, Accessed in 2023.

[59] F. Carapella, E.J. Dumas, J. Gerszten, N. Swem and L.D. Wall, "Decentralized Finance (DeFi): Transformative Potential and Associated Risks", *Finance and Economics Discussion Series*, Vol. 2022, No. 57, pp. 1-33, 2022.

[60] U.W. Chohan, "Decentralized Finance (DEFI): An Emergent Alternative Financial Architecture", *Social Science Research Network*, Vol. 23, No. 2, pp. 1-14, 2021.

[61] Y. Wang, P. Zuest, Y. Yao, Z. Lu and R. Wattenhofer, "Impact and user Perception of Sandwich Attacks in the Defi Ecosystem", *Proceedings of International Conference on Human Factors in Computing Systems*, pp. 1-15,2022.

[62] S. Wu, D. Wang, J. He, Y. Zhou, L. Wu, X. Yuan, Q. He and K. Ren, "DeFiRanger: Detecting Price Manipulation Attacks on DeFi Applications", *Proceedings of International Conference on Cryptography and Security*, pp. 1-22, 2021.