IOSCO DECENTRALIZED FINANCE REPORT

Public Report

The Board
of the
International Organization of Securities Commissions

OR01/2022	**MARCH 2022**

Contents

INTRODUCTION AND EXECUTIVE SUMMARY

"Decentralized Finance" ("DeFi") is an important, evolving and expanding technological innovation.[1] DeFi commonly refers to the provision of financial products, services, arrangements and activities that use distributed ledger technology ("DLT") in an effort to disintermediate and decentralize legacy ecosystems by eliminating the need for some traditional financial intermediaries and centralized institutions. Currently, there is no generally accepted definition of "DeFi," or what makes a product, service, arrangement or activity "decentralized." Regardless of any characterization or assertion of "decentralization," applicable regulatory frameworks still apply to participants and activities. IOSCO and its Fintech Network established the DeFi Working Group[2] to focus on understanding the current state of the DeFi market, its typologies, and policy implications.

DeFi products, services, arrangements and activities rely upon systems built on top of public permissionless smart contract platforms, such as the Ethereum blockchain. DeFi involves a multi-layered technology "stack." In summary, at the base, or settlement layer, is the underlying blockchain.[3] On top of the settlement layer, multiple systems of smart contracts (and auxiliary software) create financial products and services (protocols).[4] As described in more detail in this report, these smart contract and software applications may include, among others, activities that are or are akin to offering, trading, lending, borrowing, and asset management activities. End-user applications, such as web interfaces, are built on top of the smart contract layer. Often, end-user applications may aggregate multiple protocols to provide access and interoperability.

Financial innovation may lead to benefits for investors and others, but it may also present risks. DeFi appears to present many similar risks to investors, market integrity and financial stability as do other

---

1 "DeFi" is a term used in industry and broader discussions. It does not give rise to a unique or different legal arrangement. While this report cites to a number of sources, much of the report represents a compilation of information developed by examining publicly available sources, including websites, white papers, and software code, including smart contract code. Not all these sources have been cited. *See also*, OECD (2022), Why Decentralised Finance (DeFi) Matters and the Policy Implications, available at https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf.

2 The DeFi Working Group is led by the United States Securities and Exchange Commission with members from the Alberta Securities Commission, the Australian Securities and Investment Commission, the Securities Commission of the Bahamas, the British Columbia Securities Commission, the Investment Industry Regulatory Organisation of Canada, the Croatian Financial Services Supervisory Agency, the Dubai Financial Services Authority, the Hong-Kong Securities and Futures Commission, the Ontario Securities Commission, the Polish Financial Supervision Authority, the Commission National de Valores (Spain), the United Kingdom Financial Conduct Authority, the United States Commodity Futures Trading Commission and the United States Financial Industry Regulatory Authority.

3 For a discussion of "blockchain technology," *see* IOSCO Research Report on Financial Technologies (IOSCO FinTech Report), February 2017, pp. 45-64, available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf.

4 For purposes of this document, the term "protocol" is used to describe all the components of a financial product or service using blockchain-based technology at its core—implemented through smart contracts and including potentially a number of related functional components like user interfaces, oracles, governance and voting mechanisms, development grants and foundations, and financial assets such as tokens, treasuries and funds. Some of those components may be automated, and some may be carried out by individuals and entities. This report recognizes that this term may be used differently by others. For purposes of this report, the term is used broadly to reflect that projects offer DeFi products and services that are implemented through multiple layers of technology.

financial products and services, and it also poses specific and unique risks and challenges for regulators to consider.

Understanding the regulatory implications arising from DeFi requires analyzing the totality of a DeFi ecosystem as it exists currently, its interrelationship with centralized crypto-asset trading platforms and service providers and traditional markets and activities, and how it may continue to develop in the future. Developing a comprehensive understanding includes identifying and analyzing, among other things, the structural components of each type of DeFi financial product, service, arrangement and activity; what aspects of these may be "decentralized" and why; what are the roles of each of the components and participants involved at each of the different layers or levels, including their incentives and motivations; how participants engage with the various components and each other; and the roles that centralized crypto-asset trading platforms and service providers play.

Many of the financial products, services, arrangements, and activities in DeFi mirror, and in some cases overlap with, more traditional securities and derivatives products, services, arrangements and activities. In some cases, these may be novel to DeFi. One primary characteristic of DeFi is its peer-to-peer nature and resulting ability to create alternatives to traditional and centralized financial market infrastructures, products or services, and potentially to complicate the application of existing regulatory frameworks to DeFi market participants and activities, including those that govern issuers, offerings, products, intermediaries, and trading markets. As DeFi continues to expand, both a granular and holistic understanding of the DeFi market will improve authorities' ability to understand the regulatory implications of this emergent market with respect to their own jurisdictions.

This report is based on currently available information as of the date of publication. The purpose of this report is to provide a general understanding of DeFi, including some areas of potential regulatory concern. The descriptions contained in this report are meant to describe typical features of DeFi protocols currently available. Actual features of any particular DeFi protocol in existence may vary.

IOSCO welcomes input from the public, including crypto-asset market and DeFi participants and from any other interested party, on the presentation of information in this report, as well as on any other crypto-asset or DeFi related matter. Comments may be submitted to DeFi@iosco.org.

OVERVIEW OF THE DECENTRALIZED FINANCE MARKET

HOW DEFI WORKS TECHNOLOGICALLY

OVERVIEW

DeFi technologies work to create alternatives to traditional financial approaches. A public blockchain forms the base or computational layer on which transactions are recorded and smart contracts (code) operate. A smart contract is code that is deployed on a blockchain. The execution of a smart contract is triggered when that smart contract is "called" by a transaction on the blockchain. If triggered, the smart contract will be executed through the blockchain's network of computers and will produce a change in the blockchain's "state." Smart contracts can be used, for example, to issue and manage tokens, escrow tokens, or carry out any number of "if/then" type computations.[5] While much of the activity in DeFi occurs on a particular base blockchain (on-chain), participants also rely upon and use technologies apart from blockchain (off-chain) to build products and systems and communicate and coordinate activities, such as the internet and its infrastructure, including internet-based software, collaborative tools, online forums and social media.

THE BUILDING BLOCKS OF DEFI

In DeFi, financial products and services are created using smart contracts, which operate in a stack of technologies that interact with each other. Products and services are offered at each level of the stack. For purposes of this report, the DeFi technology stack is presented in four "layers" as well as a grouping of external, off-chain inputs that connect to multiple layers:[6]

- The "settlement layer" – blockchains and "Layer 2"[7] solutions where the consensus state of the blockchain is maintained, i.e., transactions are recorded, and participants and smart contracts have addresses that can hold crypto-assets and interact with other participants and smart contracts.[8]
- The "asset" layer – crypto-assets (coins and tokens) that participants and smart contracts create and transfer on a blockchain.
- The "smart contract" layer – smart contracts (and auxiliary software) used to provide functionality to DeFi products and services.
- The "application" layer – front-end user interfaces, APIs, and other code that allow participants to interact with the smart contracts. Today, these applications are primarily hosted off-chain.
- Key off-chain inputs that make up a "DeFi supply chain" of information, services and assets that can affect the application, smart contract or asset layer.

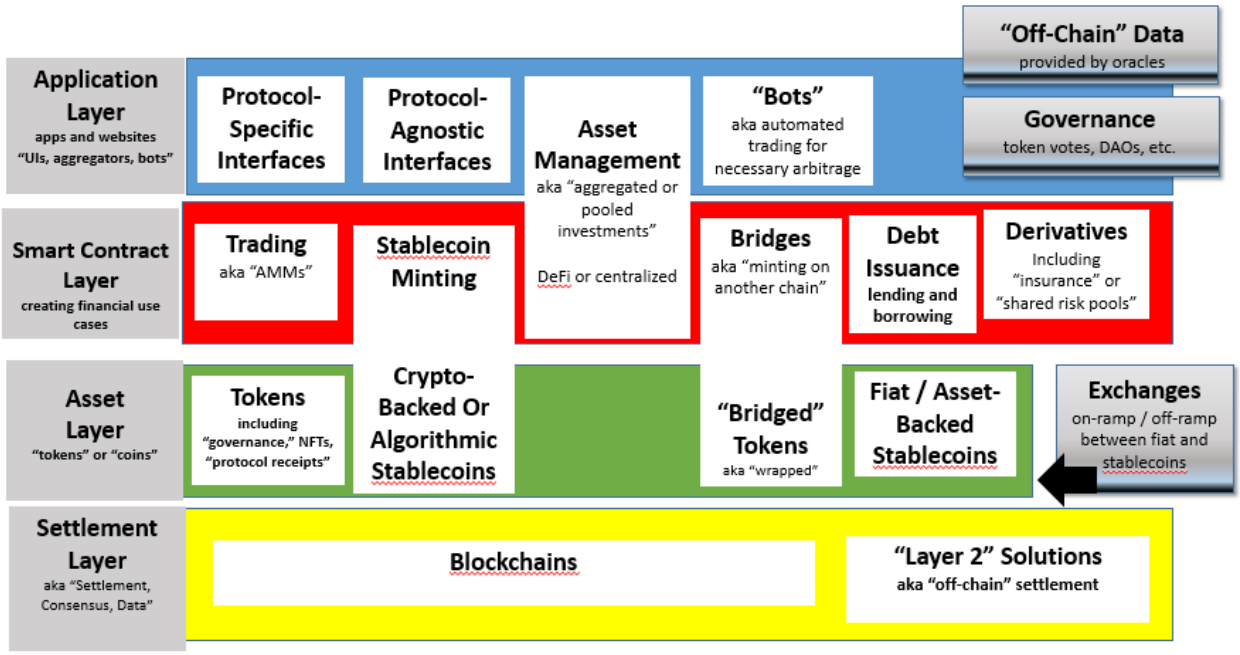
---

5 For a more detailed explanation of smart contracts, *see, e.g.*, https://policyreview.info/glossary/smart-contracts. *See also* https://journals.uic.edu/ojs/index.php/fm/article/view/548.

6 The DeFi "stack" has been presented in different ways. *See, e.g.*, a "DeFi Stack" schematic in Fabian Schär, "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets," Federal Reserve Bank of St. Louis Review, Second Quarter 2021, pp. 153-74, available at https://doi.org/10.20955/r.103.153-74.

7 Layer 2 solutions are software on networks running on top of the settlement-layer blockchain. These Layer 2 solutions allow for transactions to occur off-chain and eventually be recorded on the applicable blockchain. For example, Layer 2 solutions that operate with Ethereum are often marketed as cheaper and faster than on-chain transactions.

8 For a more detailed understanding of blockchain and the role of consensus mechanism, *see* IOSCO FinTech Report, *supra*.



This chart is meant to be a high-level visualization of these layers. No single chart could capture the totality of blockchains, crypto-assets, and applications in use in DeFi, each created with different goals and design choices and often composable (usable together) into novel forms.

SETTLEMENT LAYER: BLOCKCHAINS AND "LAYER 2" SOLUTIONS

In DeFi, blockchains are used as a "settlement" layer for recording transactions. The state of the blockchain ledger can only be changed by adding records to it chronologically and secured cryptographically as "blocks" of transactions in a "chain." Operations such as validating and recording transactions are handled cooperatively by computers organized in a peer-to-peer network structure rather than a server-client network model.[9]

Each blockchain can differ materially in multiple ways, such as: who can participate on the blockchain and how; what kind of data can be stored, and what activity blockchain transactions represent; whether and what kind of custom software code can be run on the blockchain; how to incentivize users to provide the computing and storage resources needed to operate and maintain the blockchain; and how to secure data and discourage attacks. The design choices made by any given blockchain developer about these questions are defined in that blockchain's core code and reinforced by how users follow and/or modify this code over time. The result of these choices will influence outcomes such as how expensive it is to operate and use the blockchain, what kind of transaction speed and throughput can be achieved, and what kind of assets and use cases can be supported.[10]

---

9 *See* IOSCO FinTech Report, *supra*, at 45-64.

10 As described in the IOSCO FinTech Report, *supra*, public blockchains such as Bitcoin and Ethereum are maintained through incentivized contributions, they are typically pseudonymous, and anyone can conduct transactions or contribute resources. For a discussion of certain scalability, security, and decentralization issues involving blockchains, sometimes referred to as the "blockchain trilemma," *see* for example, "Blockchain Trilemma" at https://coinmarketcap.com/.

As an alternative to utilizing a base blockchain layer to process all transactional data, various "layer 2" technologies exist that attempt to scale blockchain usage by enabling faster and/or cheaper transactions with greater throughput. These currently include "lightning" networks, sidechains and roll-ups, to name a few. Essentially, these "layer 2" technologies allow for certain transactional data to be processed off the base blockchain and eventually to be anchored back onto the base blockchain.

The most popular blockchain used currently in DeFi is Ethereum, in part because of its flexible support for smart contracts as a central design goal. Ethereum has used a variety of design choices to successfully incentivize a large, peer-to-peer network of users to contribute the resources needed to operate the network. However, due partly to the congestion of the Ethereum network and high fees, some DeFi protocols are migrating to or developing on other blockchains, such as Binance Smart Chain, Solana, Polygon and Avalanche.

ASSET LAYER: CRYPTO-ASSETS

Certain crypto-assets, often referred to as a blockchain's "native" token, are minted through the consensus mechanism of a particular blockchain (e.g., mining or staking) and act generally as a reward to incentivize participation in that blockchain's consensus mechanism. Other crypto-assets, often referred to as "coins" or "tokens," are minted and managed by smart contracts running on a particular blockchain. Such smart contracts may themselves maintain a set of ledger entries that track blockchain addresses that control units of the crypto-asset they manage. Many of these crypto-assets are traded on or through centralized crypto-asset trading platforms, which provide other services such as lending, borrowing and custodial services. It is through these centralized crypto-asset trading platforms and the services they provide that participants acquire and trade crypto-assets used in DeFi protocols, and realize on profits from such DeFi activities.

DeFi protocols are able to facilitate transactions in crypto-assets that are compatible with the blockchain on which the protocol operates. Crypto-assets can take many forms, from those created and distributed by centralized participants, including fiat-based stablecoins, to those that are created and distributed through mining or by using smart contracts. Design decisions implemented in a blockchain's core code and in smart contracts define the features of each crypto-asset and how users interact with it, such as: the crypto-asset's total supply and how that supply is controlled (including issuance, circulation, and removal from circulation); types of transactions the crypto-asset is permitted to be a part of; whether assets are technologically "fungible" with other crypto-assets or are in some respects unique; and how users are incentivized to participate and interact with the crypto-asset. Because these features are set by the code or smart contract that is used to create the asset, these crypto-assets are often referred to as "programmable." Many different crypto-assets typically reside on the same blockchain. In addition, because different blockchains are not generally interoperable such that assets created on one cannot automatically be reflected on another, entire "cross-chain" or "bridge" protocols – discussed below – have been created to take an asset on one blockchain and create a synthetic version of it on another blockchain.

Smart contract code is typically viewable by the public once deployed to a blockchain and therefore is able to be copied or "forked" (copied with modifications). Open-source technical standards have emerged to aid developers in creating crypto-assets that behave in expected ways. For example, the ERC-20 standard outlines certain requirements that must be met for an Ethereum-based token to be considered "ERC-20 compliant." Typically, token standards ensure that tokens can transfer between addresses on the Ethereum blockchain and can interact in certain ways with other tokens. Standards are viewed positively by developers as a tool for saving development costs and reducing the risk of bugs or incompatibility. They

play an important role in determining what kinds of assets exist and what functionality is considered normal or expected.

For purposes of this technical discussion, crypto-assets can be grouped into three broad categories (although there are variations among crypto-assets in each category):[11]

- "Tokens" – These represent the vast array of crypto-assets, ranging from the "native" tokens that incentivize consensus activity on a blockchain (such as ETH on Ethereum) to smart contract-created tokens that entitle a holder to specified rights with respect to a protocol. In DeFi, newly minted tokens are obtained by a participant in different ways, including by "earning" them in exchange for participation in a protocol, voting or consensus mechanism. For example, a user may receive a token for depositing crypto-assets in a lending or trading system, which may give them an interest or a share of a pool. A user may receive a "governance token," which gives them certain voting rights on future aspects of the protocol. A user may be rewarded a native token for participating in mining. Many tokens serve multiple purposes, simultaneously being held for appreciation, invested in another protocol to obtain a return, or used for voting as part of the protocols. See "Products and Services".
- "Stablecoins" – These are a subset of crypto-assets that purport to have a stable value, as opposed to other crypto-assets, and that are generally linked or pegged to the value of some other asset or assets, including fiat and other crypto-assets. See "Role of Stablecoins in DeFi."[12]
- "Bridged" or "Wrapped" Tokens – These are a subset of crypto-assets created on a blockchain as a synthetic for a given token on another blockchain, thereby enabling the reference token to be used on a different blockchain. These tokens are often treated as if they are the equivalent of the original token, but they are technologically distinct and require either third-party custodians or the creation and operation of smart contracts on each blockchain. See "Products and Services".

SMART CONTRACT LAYER

Smart contracts are code deployed to and executed on a blockchain, which provide the underlying functionality for DeFi use cases such as crypto-asset exchange, lending and borrowing, derivatives, etc. Typically, any one of these use cases requires multiple smart contracts (and often auxiliary software) working together to form a specific protocol.

On blockchains that support smart contracts, such as Ethereum, the software code that makes up the contract is stored and executed on the blockchain. To prevent poorly written or abusive code, such as programs that loop infinitely and consume network resources until no transactions can be completed, Ethereum miners charge a fee (in ETH) for every transaction, including transactions that trigger smart contracts, and this fee is commonly referred to as "gas." Users include the ETH that they are willing to pay when they submit their transactions, which compensates the miners that contribute the computing and storage resources that are necessary to verify and write transactions to the blockchain. If a sufficient "gas" fee is not paid, a

---

11 There are millions of unique assets across all blockchains. Some are relatively simple, like those tokens created by the ERC-20 standard (ERC-20 tokens) that can be transferred through multiple DeFi projects. Newer entries – such as those created using the ERC-721 standard (NFTs) – have added new characteristics, including the ability for each token to be in some respects unique or "non-fungible." While NFTs are created using a different software standard, they may represent investment opportunities, as does any other type of crypto-asset depending on the facts and circumstances.

12 *See also*, IOSCO Global Stablecoin Initiatives Report (IOSCO Stablecoin Report), March 2020, available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD650.pdf.

transaction may fail or, depending on the blockchain, maybe delayed until the gas fee offered is attractive enough relative to others to be added to a subsequent block.

Once deployed to a blockchain, smart contracts obtain a unique address on the blockchain. Any transaction involving that smart contract will reference the address of the smart contract in the transaction. The source code of the deployed smart contract can be viewed and tested by anyone with access to the blockchain and the technical skills or resources to read or test the code. Smart contracts can remain deployed permanently unless specifically programmed with functionality describing how they can be destroyed (e.g., a "kill switch").

APPLICATION LAYER: USER INTERFACES AND DAPPS

While it is possible for sophisticated users to write code to interact directly with smart contracts on a blockchain, most users prefer to use a website or mobile app. The application layer includes graphical user interfaces (GUIs) and other components that enable and shape user interaction with DeFi. Notably, much of this functionality uses off-chain technologies, meaning that it does not operate on a blockchain but instead relies on traditional internet infrastructure. For example, graphical images and interaction code will often be hosted on centralized servers. Commercial, centralized services have also emerged that help accelerate DeFi software development by providing simplified application programming interface (API) access to underlying blockchains. Nonetheless, DeFi participants typically refer to applications that use smart contracts in some part of the application as "decentralized applications" or dApps.

As discussed under "Principal Participants" and "The Big Picture," apps enable retail investors to participate in DeFi. These apps may be all that an average user will see when interacting with a protocol and in some instances will provide users with a number of services. For example, they often:

- Solicit users and simplify the process by which users engage in DeFi transactions even if those users lack the technical ability or resources to interact directly with smart contracts. For example, centralized crypto-asset trading platforms have created software that allows their customers to engage with DeFi protocols.
- Provide interactive information, such as analytics, to assist users in making decisions about what DeFi transactions to engage in. For example, they may provide traders with candlestick charts and live-updated pricing information.
- Provide asset management services by allowing a user to deposit crypto-assets and invest them – either alone or through pooled transactions – into one or more DeFi protocols.

In DeFi currently, some of these apps are protocol-specific in that they allow a user to engage in transactions using one protocol's smart contracts. Other apps are protocol-agnostic (and are often referred to as "aggregators") in that they act across multiple protocols to identify transactions that meet certain parameters.

Beyond the broadly available apps designed for general users, sophisticated, well-capitalized entities may use specialized software exists to conduct automated trading involving DeFi products. This trading is fundamental to the operation of many protocols because it allows the protocol to adapt to market conditions. See "Products and Services".

OFF-CHAIN INTERACTION WITH DEFI

DeFi systems interact with "off-chain" systems in many ways. DeFi systems widely rely on centralized teams, companies and infrastructures. Even where a DeFi system uses on-chain smart contracts, users still

typically access DeFi products and services through an off-chain interface or interfaces, such as a website or mobile application. These resources in turn rely on URLs registered with a traditional DNS registrar, centralized file storage, and software supported by or hosted on traditional web servers or cloud services. However, protocols now exist in DeFi as an alternative for off-chain components (e.g., IPFS for file storage and web hosting, ENS for DNS-like routing). Some protocols already use one or more of these potentially decentralized infrastructure systems to reduce reliance on centralized infrastructure. Centralized crypto-asset trading platforms also play a central role in DeFi, including by providing trading, lending, and borrowing that facilitates participation, including on a highly leveraged basis, in DeFi protocols, and as the mechanism through which participants may realize on their trading and other DeFi activities.

Other ways in which DeFi protocols interact with the off-chain world is through their dependence on off-chain inputs:

- Protocols often require, or wish to use, information that does not exist on the blockchain (e.g., a crypto-asset's market price on a centralized crypto-asset trading platform, or the occurrence of an event, such as which team won a sports match). One popular source for such information is an "oracle." An oracle connects a smart contract to off-chain data that may be an input for that smart contract's functionality.
- Protocols often create methods for users to effect changes in how smart contracts and other aspects of protocols will operate in the future, including through altering smart contracts or, in the case of certain types of structures, determining how to spend assets an entity holds in "treasury" for purposes such as funding future development efforts. This is broadly referred to as "governance," which comes in various forms, including through administrative "keys," multi-signature accounts, "governance" tokens that provide certain voting rights to token holders, and "decentralized organizations" or "decentralized autonomous organizations" ("DAOs").[13] Each of these governance mechanisms can impact the degree to which a protocol, and any of its components, may be viewed as "decentralized." See "Governance Tokens" and "Decentralization".
- Many protocols currently rely on fiat- or asset-backed stablecoins as important crypto-assets being used in DeFi smart contracts and investments. See "Role of Stablecoins in DeFi".
- Other off-chain participants and activities that are needed or used in DeFi include those involving customer onboarding, digital wallets, blockchain analytics, market surveillance, and infrastructure, many or most of which are provided by centralized crypto-asset trading platforms.

PRODUCTS AND SERVICES

At the heart of DeFi are the range of products and services that generally state that they are open-source, decentralized, non-custodial, and enable investors and consumers to engage in crypto-asset transactions on a peer-to-peer or peer-to-contract basis. While many of the financial products and services arising from DeFi resemble traditional financial products and services, blockchain technology has supported the creation of entirely new financial products and services, such as "flash loans." It is important to recognize that DeFi does not exist wholly independent of traditional financial markets and entities (referred to as "TradFi" for

[13] Through these governance mechanisms, some DeFi projects have sought to create fully decentralized systems. Currently, however, claims about decentralization for many projects may not hold up to scrutiny of the technical reality of what can be changed in the system, who can be involved in the decisions, and who actually is involved.

purposes of this report) and centralized crypto-asset markets and entities (referred to as "CeFi" for purposes of this report) and there are important interlinkages.

BOX 1: DECENTRALIZATION

When evaluating DeFi products and services, one immediate consideration is to determine whether and to what extent something is decentralized. Decentralization is less a binary outcome and more a spectrum or a series of spectrums for each project. It is a term that can describe various aspects of a product and service, such as ownership of the enterprise, voting power over the enterprise or any aspect of it, control of user assets, network design of an underlying blockchain (settlement layer), or off-chain infrastructure such as web servers that provide application components, among others. In addition, there is no agreed definition of what causes a product or service to be considered decentralized, such that there is no concentration of ownership, voting power or control as to the product or service, enterprise or user assets. While a DeFi product or service may claim to be decentralized, some DeFi products and services may actually retain a level of centralization. For example, the founders or other participants may retain control or significant influence over aspects of the product or service. Even as to protocols and smart contracts that are subject to change through votes of governance tokens, ownership and voting control of governance tokens may be concentrated in the hands of a few and therefore there may continue to be controlled by centralized parties rather than protocols and smart contract designs. Most DeFi protocols rely on centralization in one or more areas, and there are protocols that have a hidden centralized authority and are decentralized in name only.

On a theoretical level, the extremes of the decentralization spectrum are explained as follows:

- Pure Decentralized Protocols – Governance decisions and administrative privileges over the smart contracts that sit behind a protocol are distributed to a dispersed network of independent users who have equal access to information and the ability to propose and vote to change any aspect of the protocol
- Pure Centralized Protocols – Governance decisions and administrative privileges are reserved for centralized operators

Using this theoretical framing, it is unlikely that most DeFi products and systems fall squarely into either extremity with most sitting somewhere between the two. When looking at a particular product or service from a decentralization standpoint, it is important to identify what features and activities do and do not involve central actors or parties. In analyzing the question of decentralization, it also is important to identify whether an individual participant's ability to make decisions impacts only their own choices and actions using the protocol or whether the participant has the ability to impact the protocol itself.

In using a protocol, participants may "self-custody" their crypto-assets, meaning that they alone can determine what is done with their assets without involving an intermediary. For example, they can transfer their crypto-assets away from the protocol at any time in full without a gatekeeper, and nobody has any rights, such as re-hypothecation rights, to their assets. While this type of custody may eliminate the need for certain intermediaries that may otherwise exist in CeFi or TradFi, self-custody alone does not affect or indicate whether the protocol has central or concentrated parties involved in protocol decision-making.

One area of focus is governance structures. Defi protocols may use various mechanisms to distribute governance roles, such as DAOs and governance tokens, in order to provide evidence of a greater degree

of decentralization. However, there are many different permutations of these governance arrangements and the role that they play within a protocol. The fact that elements of a DeFi protocol may be viewed as decentralized or subject to community vote does not mean that the protocol itself is fully decentralized. As discussed in "Governance Tokens," governance tokens currently may play a limited role in actually affecting the substance of smart contracts and play almost no role in managing or overseeing the entity and developers of the smart contracts and protocol at the "enterprise" level. Further, while DAOs are presented as a solution to provide for community governance, DAOs and their development are still in early stages. See "Governance Tokens" and "DAOs." Additionally, while a particular DeFi protocol may robustly mitigate instances of censorship or collusive control, there may still be an on-going dependency of protocol development and functionality on creators and foundational investors.

It should be noted that DeFi products and services may have the potential to become more decentralized over the course of their development as they often start out as centralized projects with decentralization as an end goal that they may develop towards incrementally. Because protocols vary tremendously, this analysis must be done on a case-by-case basis, and it is not a static assessment as these protocols can change considerably over time.

CRYPTO-ASSET USAGE

As noted above, central to DeFi are crypto-assets that can be created by and/or interact with code or a smart contract. A crypto-asset holder can use these assets to engage in DeFi trading, lending, borrowing and other activities. A crypto-asset holder's rights and interests by virtue of controlling a particular crypto-asset vary, as do the types of crypto-assets and the manner of their creation and distribution. Many of these crypto-assets also are traded on or through centralized crypto-asset trading platforms and may be the subject of CeFi lending and borrowing arrangements as well.

As discussed above, certain crypto-assets can be created by smart contracts and issued to participants in exchange for their participation in DeFi protocols, e.g., to represent financial exposures or returns. For example, DeFi systems can be structured in such a way that participants are rewarded for depositing (or "locking up") crypto-assets that can then be used by others for certain purposes, such as borrowing or trading. In such systems, the participant may receive another crypto-asset in return for participation in a protocol, often referred to as a "liquidity provider token" (or "LP token"), that may entitle the participant to a portion of transaction fees generated or some other type of return or interest created through the protocol.

Other crypto-assets can be structured to function as a stable value coin, or stablecoin, to provide its holder with a crypto-asset that is used essentially as a cash substitute in DeFi transactions, including to facilitate trading. Stablecoins are crypto-assets whose value is "pegged" or "linked" in some way to the value of a reference asset (e.g., fiat currency). Stablecoins, whether issued and maintained by or through a DeFi protocol or by a centralized arrangement, are critical to the functioning of DeFi as they are frequently used as one side of, or collateral for, a transaction. Because of their perceived stable value, they fuel transactions with more volatile assets. See "Role of Stablecoins in DeFi".

Another type of crypto-asset created and issued by platform or development entities or through smart contracts is what is referred to as a "governance token." These tokens enable their holders to participate in governance by voting, but they may also provide economic value as they may be held as a speculative investment, traded on trading platforms for profit and/or entitle their holders to additional distributions from the protocol's treasury. See "Governance Tokens".

LENDING AND BORROWING

Lending and borrowing protocols currently are two of the primary DeFi products currently available. Lending protocols allow holders of crypto-assets, often stablecoins, to earn a fixed or variable return on those assets by depositing them in a smart contract (or "lending pool") that simultaneously allows other participants to borrow those assets. Depositors typically receive a different crypto-asset from the protocol that represents that depositor's pro rata interest in the lending pool and that can be redeemed at any time for the original deposit and accrued interest. In many protocols, interest rates can vary and are set by algorithms or a protocol project team, or through certain governance voting to optimize utilization and mitigate liquidity risk.

Often, the determinative factor in the interest rate of a lending pool is the relationship between the crypto-assets in the lending pool, the amount that has been borrowed (the "utilization rate"), and the optimal utilization rate. Typically, the interest rate on the outstanding loans rises and falls with changes in the utilization rate. Because depositors can redeem crypto-assets at any time, the interest rate is programmed to rise with the utilization rate to attract more deposits and discourage borrowing. The interest rate, which gradually increases up to the optimal utilization rate, spikes if the utilization rate exceeds the optimal utilization rate. Conversely, the interest rate will decrease in response to a decreasing utilization rate to encourage borrowing.[14]

The same lending protocols also allow participants to borrow crypto-assets from the lending pool by depositing crypto-asset collateral in return for interest payments. The acceptability of collateral typically is measured against risk factors such as centralization risk (i.e., the degree to which there is centralized governance or control of the crypto-asset, such as most fiat- or asset-based stablecoins) and market risks (i.e., the liquidity, volatility, and market capitalization of the deposited crypto-asset). Loans can be for any amount, have no duration, and can usually be repaid at any time. Typically, there are no credit checks due to the pseudonymous nature of lending and borrowing protocols and, as a result, the lending and borrowing protocol seeks to mitigate risk and protect solvency by implementing risk parameters, such as loan-to-value ratios, liquidation ratios, liquidation bonuses (or penalties), and reserve factors that vary based on the crypto-asset used as collateral and its risks.

A loan-to-value ratio defines the size of a loan that can be obtained based on a specific amount of deposited collateral. Loans are generally required to be over-collateralized. The liquidation ratio, which is typically higher than the initial loan-to-value ratio, sets the maximum loan-to-value ratio, beyond which a liquidation process is initiated. At the outset of a loan, a collateral-to-borrow ratio (collateral factor) is set that determines how much collateral is required to be posted against a desired loan amount. Should this ratio drop below a set liquidation threshold (which can happen frequently given the volatility of tokens as collateral value) a borrower will automatically be considered in default and the supplied collateral is sold at a discounted rate to cover the loan. Thus, if the value of the collateral decreases or the value of the borrowed assets increases by an appreciable amount, the borrower might be at risk of liquidation unless more collateral is deposited, or the loan is repaid in part or in full. In this type of protocol, liquidation involves a third party acquiring a portion of the crypto-assets backing the loan in exchange for the borrowed crypto-assets, which ensures that the loan is sufficiently collateralized. In the event of a liquidation, the

[14] The fixed rate is higher than the variable rate because it is not subject to the ongoing mechanism described in this section. Nonetheless, the interest on a loan with a fixed rate is reset in either direction if certain other conditions are met. Such a change is likewise affected with a view to optimizing utilization and mitigating liquidity risk.

protocol rewards liquidators, and penalizes borrowers, by selling the deposited crypto-assets at a discount. The reserve factor is the portion of the interest paid by borrowers that goes to the protocol's "treasury" and is appropriated for the protection of depositors against borrower default or liquidation failure. Alternatively, if not over-collateralized, these arrangements may put restrictions on activities carried out with borrowed assets. One notable example is a flash loan where users are allowed to borrow without having to post collateral, but the duration is for one transaction that is instigated and settled simultaneously.

Lending protocols may distribute governance tokens in exchange for participation in these arrangements. As governance tokens typically have active trading and may provide other economic benefits, they may act as an incentive for borrowers to increase their borrowed position. This behavior has been characterized as borrowing and leveraging spirals,[15] both increasing the amount of liquidity in the arrangement and the risk of the borrower's collateral being liquidated. This behavior will continue if the cost of borrowing does not exceed the earnings from the governance tokens.

Lending protocols may also support "flash loans," which enable participants to borrow crypto-assets on an uncollateralized basis because the assets are borrowed and repaid within the same block of transactions. In other words, a flash loan is structured in such a way that borrowing, utilization of borrowed funds, and repayment constitute a series of steps in a single transaction. Thus, if the loan is not capable of being repaid in full within the same block, it is automatically canceled. Because flash loans do not involve default risk, borrowers are not required to deposit collateral, and the interest paid to the pool from which the crypto-assets were borrowed is fixed at a low rate.

There also are protocols that enable participants to post collateral to obtain a new crypto-asset (often a stablecoin) instead of taking assets from a lending pool. See "Role of Stablecoins in DeFi".

COMPARISON TO TRADITIONAL LENDING AND BORROWING ACTIVITY

*TradFi***:** Lending and borrowing are fundamental mechanisms in any financial system. At a basic level this involves lenders providing funds to borrowers in return for interest and is an activity that is typically facilitated by a centralized third party, most commonly a bank, which will utilize customer deposits to lend to others.

*DeFi***:** Within DeFi, as noted, there are various lending and borrowing services. The key differences with TradFi lending/borrowing arrangements include:

- Instead of being deposited with a central party, users deposit crypto-assets to a smart contract on a distributed ledger which automatically manages the ratio of liquidity between supplied and borrowed assets, a ratio which in turn will also determine the interest rates paid by borrowers and received by lenders.
- As noted above, credit assessments typically are not required for borrower loan approvals. Instead, DeFi arrangements may rely on over-collateralization (i.e., tokens supplied by the borrower will be worth more than the amount borrowed).

[15] A borrowing spiral is the process of re-depositing borrowed funds as collateral in order to receive governance tokens as a reward. A leverage spiral is similar but carried out by more sophisticated investors who take long positions on an asset/market to maximize their long exposure to a crypto-asset that is expected to appreciate.

DERIVATIVES/SYNTHETICS

DeFi protocols have enabled the growth of blockchain or smart contract-based derivatives and synthetic exposures. A large portion of derivative DeFi protocols currently available allow participants to create synthetic crypto-assets whose value derives from the performance of an underlying reference asset ("asset-based") or the outcome or occurrence of some event ("event-based"). The reference asset or event could be virtually anything, such as securities, commodities, currencies, or the failure or hack of another DeFi protocol (see "Insurance"). For example, a person could create a synthetic crypto-asset whose value tracks the price performance of ETH relative to BTC, such that any increase in the price of ETH relative to BTC would cause the value of the synthetic crypto-asset to increase. The creator of such a synthetic crypto-asset often sells it to others (e.g., through an automated market maker) and thus takes the other side of the trade, meaning that they profit if the price of ETH relative to BTC decreases.

Like with lending protocols, a creator of a synthetic crypto-asset typically must deposit collateral in an amount that is greater than the value of the reference asset, as well as set an expiration date in some cases. This over-collateralization ratio must be maintained for the duration of the contract to avoid liquidation by holders of the synthetic crypto-asset or by others, who are rewarded for such service. A synthetic crypto-asset typically is redeemable for the collateral that was used to create it in an amount that equals the extent to which the price of the reference asset has increased or decreased, as the case may be. The price can be determined and settled through various means, including oracles.

Another type of synthetic crypto-asset that is increasingly being used in DeFi is a so-called "bridged" or "wrapped token." These tokens effectively serve as a bridge between one blockchain and another and require a person to transfer the underlying crypto-asset to the address of a centralized third party or a smart contract on the blockchain supporting that crypto-asset, which in turn issues, through a smart contract, a crypto-asset representing the underlying crypto-asset on a different blockchain. As the wrapped token purportedly is backed by the underlying crypto-asset on a 1:1 basis and can be redeemed for the underlying crypto-asset at any time, it is designed to be the economic equivalent of that asset. Wrapped bitcoin ("wBTC") is a prominent example as it gives holders of BTC the ability to participate in DeFi protocols running on other blockchains, such as Ethereum, through a process that locks up their BTC holdings (for so long as the wBTC is outstanding) but does not require them to sell the tokens. Wrapped ether ("wETH") is another token that is increasingly being used as, among other things, a bridge to Ethereum-compatible networks that enable faster and cheaper transaction execution (e.g., a Layer 2 network). These types of bridged or wrapped tokens, as synthetic exposures to the referenced crypto-asset, are affected by events involving the underlying crypto-asset, including volatility, as well as by events affecting the bridging blockchain.

Beyond DeFi protocols designed to offer synthetic exposure to an asset or event, there are also derivative DeFi protocols that are economically the same as or similar to traditional derivatives such as options, swaps, and more complex structured products.

COMPARISON TO TRADITIONAL DERIVATIVES ACTIVITY

TradFi: TradFi derivatives markets involve both centrally cleared and over the counter derivatives transactions. These may be derivatives on any type of asset, financial instrument or underlying reference, including securities, commodities, currencies, and events. These markets are subject to regulation globally, including with respect to regulation of intermediaries, trade reporting, clearing, platform trading and margin issues. Regulators globally have established additional standards, laws and regulations for

over-the-counter derivatives transactions, including centrally clearing to mitigate systemic risk, improve transparency in the over-the-counter derivatives markets, and protect against market abuse. Jurisdictions have long recognized the value of derivatives to financial markets and the wider economy due to their role in enabling market participants to manage their risks, improving the pricing of risk, and adding to liquidity. Regulation of derivatives has been the subject of a number of international reports particularly since the 2008 financial crisis.[16]

DeFi: DeFi protocols may enable participants to create and trade the same or similar synthetic economic exposures, some of which may be based on or reference any type of asset or event, and currently are subject to derivatives regulation in many jurisdictions.

TRADING

Another key product and service in DeFi involves various trading protocols, which can involve both the deposit of crypto-assets into the protocol as well as trading activities through use of the protocol. The investor returns from these protocols may arise from their trading activities directly as well as from commission-like income generated as a result of their deposit of assets into the protocol. Crypto-asset trading protocols in DeFi are often called decentralized exchanges or "DEXs."

DEXs often facilitate the exchange of crypto-assets through smart contracts rather than through centralized trading platforms, which require traders to deposit their crypto-assets with the trading platform operator. While DEXs rely on smart contracts for trade execution, they can differ in the extent to which components of a transaction are conducted on-chain. Two types of prominent DEXs are "order book exchanges" and "automated market makers" ("AMMs").

The most popular type of DEX order book exchange includes both on-chain and off-chain components, where order books are maintained by centralized operators and the blockchain primarily serves as a settlement layer. Users interested in buying or selling a particular crypto-asset at a certain price ("makers") will communicate that order to the operator, who will in turn publish the order for the use of others who might be interested in matching the order ("takers"). Once there is a match, the taker submits the order to the protocol, which executes a peer-to-peer exchange of the crypto-assets. Unlike in the centralized trading platform context, the operator may never have control of the users' crypto-assets and may serve as a "relayer" of information that is necessary for the trade to be executed and settled on the blockchain. The operator collects fees from makers and takers for providing this service. In addition, takers typically pay a protocol fee on each trade, a portion of which may go to makers to reward them for providing liquidity.

AMMs can exist entirely on-chain and rely on participants to deposit two or more crypto-assets in a smart contract (or "liquidity pool"), which then is available to trade with participants who want to exchange one of those assets for another. The depositors, who are generally referred to as "liquidity providers," typically deposit a number of crypto-asset pairs into the AMM and receive a crypto-asset that represents their pro rata interest in the liquidity pool and is redeemable at any time for their slice of the pool, including accrued trading fees. Typically, participants who trade with a liquidity pool deposit a certain number of crypto-asset A and receive a certain number of crypto-asset B. The exchange rate is automatically determined according to a formula that is essentially based on the ratio of assets held by the pool. Thus, as the ratio of crypto-asset A to crypto-asset B increases, the liquidity pool price of crypto-asset A decreases and the price of

[16] *See, e.g.*, IOSCO Principles for the Regulation and Supervision of Commodity Derivatives Markets Consultation Report (November 2021), available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD689.pdf ("IOSCO 2021 Derivatives Report").

crypto-asset B increases. The degree to which the price of each of the assets moves generally depends on the size of the trade and the pool's liquidity. AMMs are substantially dependent on arbitrage traders, typically employing "bots", who buy or sell the crypto-asset, as the case may be, until its liquidity pool price converges with the average market price.

CeFi crypto-asset trading platforms play a central role in the growth of DeFi. These platforms provide trading, lending and borrowing activities that facilitate participation in and deposit of crypto-assets in DeFi products and enable DeFi market participants to realize on their DeFi products through dispositions or other activities on or through these centralized crypto-asset trading platforms. CeFi crypto-asset trading platforms, in turn, have interconnectivity with TradFi through, for example, bank accounts. The dependence of DeFi market participants on a limited number of centralized crypto-asset trading platforms gives rise to concentration, interdependence and interconnectivity risks that can impact the broader markets.

ROLE OF BOTS

As noted above, there is specialized software that allows for automated, and often high-speed, trading – often by sophisticated, well-capitalized entities. This trading is fundamental to the operation of many protocols because they allow the protocol to adapt to market conditions. For example, the protocols that mint crypto-asset collateralized stablecoins often rely on auctions to liquidate the deposited collateral whose value has dropped, and AMMs rely on "bot" arbitrage to adjust the AMM pool's holdings (and thus its trading price) if the smart contract deviates from market prices.

Algorithmic trading is common in the DeFi space, and bots are employed to run various trading strategies or identify arbitrage opportunities. Bots may be used to automate trading decisions based on certain pre-determined triggers, whether based on mean reversion, momentum, or some other strategy. They may also be used to automate portfolio allocation decisions. Bots are also deployed by miners and others to position transactions favorably on the blockchain to, for example, front-run or back-run transactions sitting in what is called the "mempool." The mempool consists of transactions that are awaiting processing by the blockchain's consensus mechanism. The strategy to front-run transactions often entails paying higher gas prices to prioritize a trade earlier in a block. Back-running may entail early detection of large trades that could move prices and subsequently submitting trades to be included in the same block before prices are updated by oracles.[17] Other bot strategies include arbitrage between DEXs, and identification of liquidation opportunities on lending protocols. Activities of miners to increase the gas price could impact blockchain settlement of DeFi transactions.

Other strategies continue to emerge to profit from inefficiencies within the DeFi ecosystem. Overall, bots have the potential to create more efficient markets, though many are gas-intensive (thus raising the cost of transacting for other users) and can result in worse execution of trades and higher slippage for other users.

AGGREGATORS

In addition to DEXs and bots, there are other software-based products that enable various trading activities. Such products, called "aggregators," play an essential role as portals to a variety of protocols. They are designed to optimize liquidity or yield-generating opportunities for their users by scanning across protocols and then routing transactions to fulfill desired user parameters. One type is referred to as "DEX aggregators."

[17] "Miner extractable value" ("MEV") is a measure of the profit that a miner can derive from strategically including, excluding, and changing the order of transactions in a block.

DEX aggregators query a range of trading protocols for the purpose of finding the best terms for a trade, including the trading price, trading fee and "slippage" (i.e., probability that the deal terms will change over time). These aggregators can divide a single trade transaction among multiple trading protocols to ensure that the trade, in its totality, is executed at the best rate. They may also function as an aggregator of aggregators; such that various DEX aggregators are scanned for the best rate instead. DEX aggregators may charge a fee for this service, which would be added to the fee(s) that are otherwise charged by the trading protocols from which they source transaction information.

COMPARISON TO TRADITIONAL EXCHANGE AND CENTRALIZED AND DECENTRALIZED TRADING PLATFORM ACTIVITY

*TradFi***:** Traditional exchanges typically are markets that bring together multiple buyers and sellers of financial instruments. Traditional exchanges are operated by a centralized party or may be operated by financial intermediaries such as broker dealers as alternative trading systems.

CeFi: Many crypto-asset trading platforms permit the exchange of crypto-assets for other crypto-assets or for fiat currency. Most CeFi crypto-asset trading platforms engage in activities beyond traditional exchange activity. Typically, these platforms enable both institutional and retail trading and offer a variety of additional services, such as trading, lending, borrowing and custody. These platforms typically maintain custody of user assets, match buy and sell orders between their customers in real time and thereby control the throughput of transactions on their platforms via internal records that are maintained off-chain. These crypto-asset trading platforms are connected to DeFi and DEX activity through their activities in trading, lending, and borrowing crypto-assets used or received in DeFi transactions.

DeFi: As noted, certain DEXs facilitate permissionless, pseudonymous, non-custodial, direct crypto-asset exchanges between users. For example, an AMM protocol operates a series of peer-to-contract mechanisms whereby users (liquidity providers) deposit tokens into a liquidity pool managed by a smart contract that is then traded against by other users (liquidity takers), with the price determined by the ratio of assets in the pool. Typically, the AMM algorithmically adjusts prices according to a constant product formula in responses to trades which add to or deplete liquidity.

There are a variety of DEXs in operation that exhibit not only a range of different features but also a range of different crypto-assets they support for trading. For applications on the Ethereum blockchain, these typically include any ERC-20 compliant token, certain stablecoins, certain wrapped tokens (e.g., wBTC and wETH), and other tokens, including derivatives and synthetics and even perpetual swaps.[18] Much like most other applications within DeFi, and in contrast to most traditional trading markets, there is little or no on-boarding AML/CFT requirements, pre-trade or creditworthiness checks nor is there a uniform approach to decision-making around the degree of leverage that users can assume as part of these trades.

BOX 2: ROLE OF STABLECOINS IN DEFI

Stablecoins are a key component of DeFi and have contributed to the exponential and continuing growth of DeFi, facilitating the transfer of assets between and among CeFi and DeFi platforms and protocols, and fuelling the development of DeFi products and services, such as those involving trading, lending and borrowing, insurance, and derivatives or synthetics. Stablecoins are designed to be a less volatile alternative to other crypto-assets, and, because of their perceived stability, they have become DeFi's

[18] Perpetuals markets rely on an underlying funding rate that is calculated over a specific time period and will require the long to make payments to the short depending on the market price of the underlying relative to the perpetual price.

substitute for fiat currency, acting as the "stable" leg in trading transactions involving more or highly volatile crypto-assets or as the "collateral" for lending and borrowing. Stablecoins facilitate the instantaneous transfer of crypto-assets across the globe on a 24/7 basis and enable investors globally to "plug into" DeFi.

Stablecoin is a broad term encompassing a variety of crypto-assets, including those that may be considered securities in certain jurisdictions. There is no universally agreed-upon definition of the term, but most seek to create a store of value and means of exchange that is global, efficient and accessible. While stablecoins seek to achieve a particular characteristic (i.e., price stability), they are not technologically different from other types of blockchain created crypto-assets. Stablecoins could be pegged or linked to particular assets ("reference asset"), algorithmically controlled, or their value can float freely. An algorithmically controlled stablecoin is one that is based on an algorithm designed to maintain price stability by adjusting the supply of tokens to match demand, thereby affecting the quantity of tokens held by any given user while maintaining its value/market share.

Despite common claims by stablecoin initiatives that they are "backed" or "collateralized" by reference assets, it should be noted that several currently traded stablecoins are not in fact "backed" or "collateralized" by reference assets and stablecoin holders are not entitled to redemption (at face value).

A stablecoin can take many forms and can reference one or more of the following asset types:

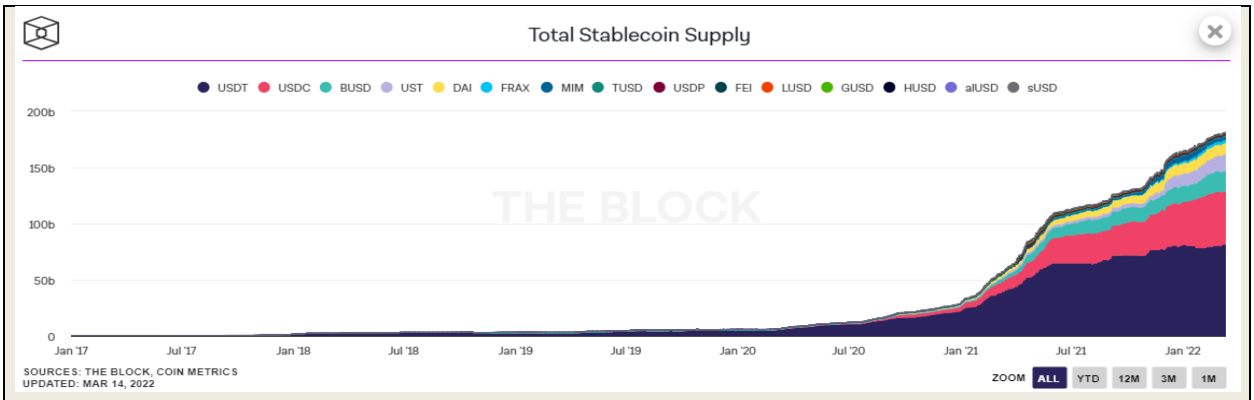
1) **Fiat currencies**. A stablecoin can reference one or more fiat currencies. The fiat currencies, or assets with equivalent fair value, may or may not be safeguarded by a custodian.
2) **Other real-world assets.** A stablecoin can reference other real-world assets such as securities, commodities, derivatives, real-estate, and/or other financial instruments and assets.
3) **Other crypto-assets.** A stablecoin can reference one or more other crypto-assets.

There are a number of public reports addressing stablecoins and the issues and risks they present broadly.[19] The following discussion focuses on stablecoins in the context of DeFi.

Stablecoins Role in DeFi Growth

DeFi participants, including institutional market participants, view stablecoins as crypto-assets with sufficient liquidity and price stability to allow users to benefit from the functionality of DeFi applications without the unpredictability created by price volatility. Stablecoins are viewed as, and used by, DeFi participants as a substitute for fiat currency, and many applications are operating outside of and/or in non-compliance with regulatory frameworks, including AML/CFT checks. The use of stablecoins to facilitate transactions involving trading, lending and borrowing, between and among platforms and protocols, has enabled DeFi to become the fastest growing sector in the crypto industry in 2020 and into 2022.

[19] *See* Committee on Payments and Market Infrastructure Consultative Report on Application of the Principles for Financial Market Infrastructures to Stablecoin Arrangements, October 2021, available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD685.pdf ("CPMI/IOSCO 2021 Stablecoin Report"); Financial Stability Board Report on Regulation, Supervision and Oversight of "Global Stablecoin Arrangements," October 2020, available at https://www.fsb.org/wp-content/uploads/P131020-3.pdf ("FSB 2021 Stablecoin Report"); IOSCO Global Stablecoin Initiatives Report (IOSCO Stablecoin Report), March 2020, available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD650.pdf; President's Working Group on Financial Markets Report on Stablecoins, November 2021, available at: https://home.treasury.gov/system/files/136/StableCoinReport_Nov_1508.pdf ("PWG 2021 Stablecoin Report").

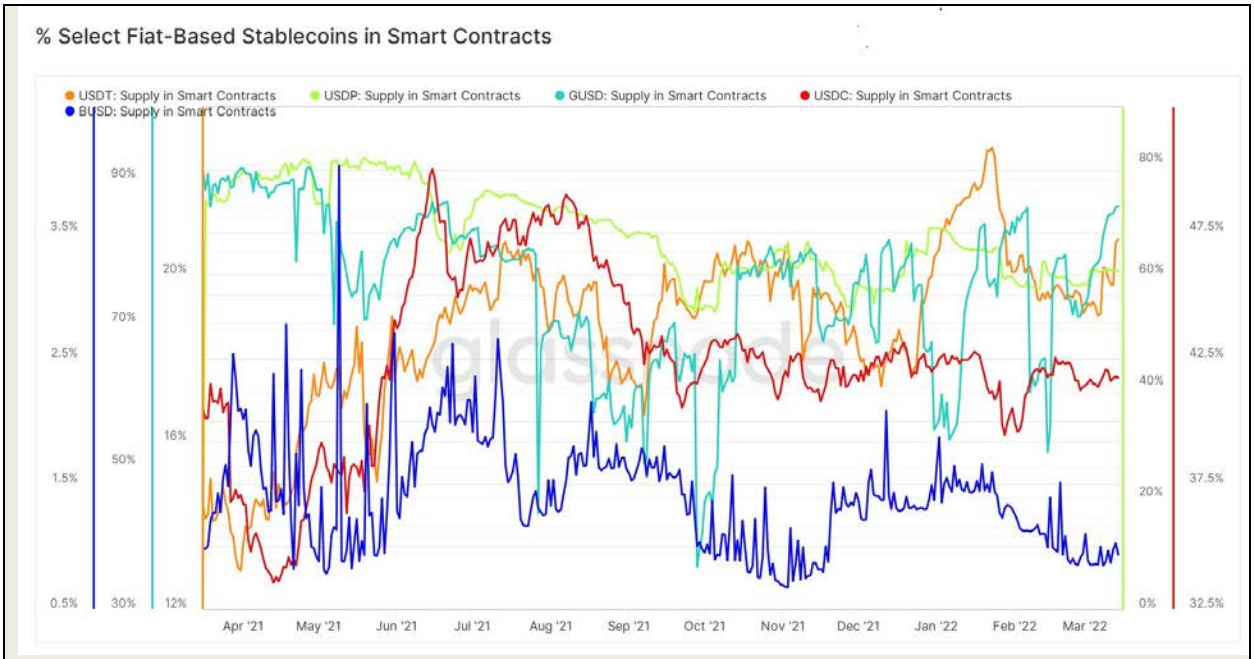


Types and Amount of Stablecoins Used in DeFi

Stablecoins that reference a fiat currency (fiat-based stablecoins) (also called off-chain collateralized stablecoins) may be the most used to date. Currently the most prominent ones are issued by a centralized issuer who claims to hold and disclose the referenced fiat currency, or assets with equivalent fair value, in reserves. Fiat-based stablecoins are marketed as providing a price-stable crypto-asset that crypto-asset investors can use to generate yield in the DeFi ecosystem through different blockchain networks. Fiat-based stablecoins have the objective to provide a stable value while maintaining the characteristics of a crypto-asset that is interoperable with the technological ecosystem. For example, a user can convert USD to a fiat-based stablecoin through a centralized crypto-asset trading platform (or in rare cases with the stablecoin issuer), and then use the fiat-based stablecoin to participate in DeFi activities.

While the market share of particular USD pegged fiat-based stablecoins changes, a limited number of predominant USD pegged fiat-based stablecoins currently account for a significant share of liquidity for the major DeFi protocols. Among the top DeFi protocols in terms of USD-equivalent amount of crypto-assets supplied are MakerDAO, Curve, Uniswap, Aave, and Compound. They collectively host a significant portion of stablecoins in circulation.

The chart below indicates the percentage of select fiat-based stablecoins in smart contracts. The Y-axis is a different scale for each stablecoin presented.



Source: Glassnode

Stablecoins that reference another crypto-asset (crypto-asset-based stablecoins) (also called on-chain collateralized stablecoins), such as DAI, have become a backbone of the DeFi ecosystem. DAI is backed by an over-collateralized amount of another crypto-asset and its value is soft pegged with economic mechanisms that incentivize supply and demand to drive the price to $1 DAI, through an autonomous system of smart contracts on the Ethereum blockchain. DAI and other on-chain collateralized stablecoins are promoted as seeking to create a "decentralized" version of a stablecoin.

Stablecoins Role in DeFi Applications

Stablecoins have a number of uses in DeFi. They are used as a "stable leg" in a trade against a more volatile crypto-asset. For example, stablecoins often are one asset in a pair of crypto-assets used in an AMM. The AMM creates liquidity for others seeking to effectuate trades. Stablecoins also are used as "collateral" to finance such activities such as liquidity mining, yield-farming, lending and borrowing. For example, stablecoins are frequently "locked" in DeFi arrangements in order to garner yield from interest payments paid by others borrowing those stablecoins from the arrangement to engage in for leveraged trading or other activities. Stablecoins reportedly are among the most highly traded assets as a percentage of total volume on several large venues that enable the trading of crypto-assets.[20]

Risks of Using Stablecoins in DeFi

Fiat-based stablecoins have significant risks, as earlier reports have clearly noted, including risks relating to issuer viability and performance, conflicts of interest among issuers and distributors, verifiability and liquidity of reserves to support payment on redemption of outstanding stablecoins, and risks of centralized crypto-asset trading platforms who play a key role in the distribution, trading, and redemption of stablecoins. These risks arise in DeFi applications as well as in centralized crypto-asset trading platforms and activities. For example, the failure of a stablecoin issuer or crypto-asset trading platform

[20] *See* https://www.theblockcrypto.com/data/crypto-markets/spot.

primarily involved in a particular stablecoin would eliminate the stability, give rise to significant volatility in these assets and thereby impair the collateral and liquidity that is at the heart of DeFi. Centralized crypto-asset trading platforms, and their role in trading, lending and borrowing stablecoins as well as other crypto-assets, also present significant risks, including those involving high leverage and concentration, among others.

Unlike fiat-based stablecoins that have a central issuing entity, crypto-asset-based stablecoins typically are more decentralized and are over-collateralized; however, their scalability tends to be limited. To mint more of the stablecoin, a user must necessarily back the issuance by an over-collateralized debt position. In some cases, there is even a debt ceiling that further limits the supply growth. In addition, depending on the type of collateral used, there may be exposure to third-party liabilities and interdependence with traditional finance. Additionally, with most crypto-assets used as collateral in a particular stablecoin protocol, there is significant downside volatility risk that a crypto-asset based stablecoin holder is subject to. To the extent the collateral is a fiat-based stablecoin, there are additional risks that may impact the crypto-asset-based stablecoin value. As discussed above, these risks may differ depending on the collateralization levels and mechanisms in a particular crypto-asset based stablecoin.

Stablecoins issued by a private entity and used for trading, lending or borrowing purposes have unique risks associated with the issuer. Additionally, risks arise from secondary market activity and market participants beyond the stablecoin issuer itself. Stablecoin arrangements generally require a mechanism for distribution to end-users and a mechanism for repurchase or conversion of the stablecoins into national currency. These activities are often undertaken by market participants other than the stablecoin issuer. For example, rather than mint or redeem stablecoins through the issuer, most market participants rely on crypto-asset trading platforms to exchange between stablecoins and national currencies (or even other stablecoins).

INSURANCE OR RISK PROTECTION

As with other financial markets, investors may have a strong interest in hedging their exposures and protecting against certain risks. While traditional insurance may normally play a role in addressing these types of risks, in DeFi, traditional insurance is significantly limited, and smart contract-based insurance and risk protection protocols aimed at providing the same or similar protection as exists in traditional insurance markets are only now developing. DeFi or smart contract insurance or risk protection protocols that currently exist enable participants to obtain protection against a certain event (e.g., the hack or failure of a particular DeFi protocol or centralized trading platform with which they have crypto-assets on deposit or locked up, a stablecoin price crash, etc.) in exchange for a fee (or "premium"), which goes to the participants who assume the risk of the event coming to pass by depositing the crypto-assets that would be used to cover a claim. Although they are likened to traditional insurance, the smart contracts underlying these arrangements are essentially shared risk pools that offer and sell event contracts, which might be a type of derivative depending on the jurisdiction. In essence, these shared risk pools protect crypto-assets that are deposited in a protocol or held by a custodian.

In the DeFi risk protection protocols, typically anybody can participate in providing protection by funding the risk pools that will pay for accepted claims by depositing crypto-assets in return for fees (collectively becoming a liquidity provider). Coverage providers choose the risk events they are willing to cover, and fees vary depending on the protocol insured and the amount of risk. Participants who purchase protection can submit a claim if they believe they have lost crypto-assets as a result of a covered event. Claims can be paid based on either a vote of token holders or automatically by a smart control that relies on some oracles

that determine the existence or non-existence of the "insured" event. The protocols depend on the existence of economic incentives that deter dishonest behavior in claim submissions and claim assessments, as well as risk parameters that ensure that the protocol as a whole is not overly exposed to any type of risk that might be systemic in nature.

ASSET MANAGEMENT AND ADVISORY ACTIVITY

DeFi asset-management and advisory protocols can take various forms. In some cases, where smart contracts automate investment strategies, users can deposit assets into a protocol and have them transferred to, pooled with or otherwise used by another protocol that pays a return. DeFi protocols set the parameters for portfolio management such as fees, asset weighting, asset types and the number of positions. These protocols often issue a separate token, which can be used for governance votes and that can be used to pay transaction costs or management fees. Once the asset pool is set up, other investors can invest in the pool, typically through a website interface to the given protocol. On certain asset management-like protocols, custody of invested crypto-assets remains in the hands of the investor within their wallet, negating the need for a third-party custodian.

Currently, investments in asset management DeFi protocols are in crypto-assets, including crypto-assets that provide derivative/synthetic exposure to real-world assets. As real-world securities and assets are tokenized, they can be included within such a DeFi asset pool.

Pooled assets on DeFi protocols can fall into the traditional categories of being either actively or passively managed. Some actively-managed DeFi asset pools put all investment decision-making in the hands of an entity that acts as a portfolio manager, who has discretion over investments. Other protocols allow users to invest in pools that rely on smart contracts to automatically balance the investments – using algorithms to ensure the pool meets the investment objectives and parameters.

In addition, there are protocols that operate to pool investors' crypto-assets for trading, lending and borrowing purposes, referred to in this report as yield-farming aggregators or pools. Yield-farming aggregators or pools provides a type of asset management which has similar characteristics to robo-advisory service for DeFi participants. Yield-farming typically involves participation in various DeFi protocols, such as AMMs and liquidity pools, to attain greater yield. While participants can engage in yield-farming independently, they often use yield-farming aggregators or pools as they can earn yields that likely would not otherwise be attainable independently. Yield-farming aggregators or pools can constantly rebalance as opportunities in the DeFi space shift in accordance with strategies coded into smart contracts. Participants deposit crypto-assets in the associated yield-farming protocol and receive a crypto-asset representing their pro rata share of the asset management pool, which is redeemable at any time. The protocol charges fees for this service, most of which are contingent on performance (i.e., whether the smart contract has generated yield). While yield-farming aggregators or pools use smart contracts, the creators or developers of these smart contracts often retain the ability to modify the smart contracts and algorithms.

As DeFi asset management protocols are based on blockchains and smart contracts, investors in the protocols are promised full transparency regarding all activities, such as trading and investment decisions; however, analyzing blockchain data requires a level of technical expertise.

COMPARISON TO TRADITIONAL ASSET MANAGEMENT AND ADVISORY SERVICES

TradFi: Investors use asset management and advisory services to enhance their risk and return profile by gaining advice on and access to markets, assets or strategies (including passive strategies) they may otherwise be unable to replicate effectively if investing individually. Generally, management fees are

charged based on a percentage of the assets under management (AUM) or advice, and some managers may also charge an additional performance fee.

Where funds are pooled, asset management clients are afforded economies of scale as firms undertake investment activity on behalf of a large pool of underlying investors. Assets will usually be held by a third-party custodian, with fund administration also being carried out by a separate entity.

Asset managers will continually rebalance a given portfolio based on investor flows and their overarching investment strategy (investing/divesting as necessary). In the case of passive strategies, portfolio managers will have to regularly trade underlying investments to ensure that they meet the correct weights as represented in the benchmark or index.

DeFi: In DeFi, there are protocols that appear to offer services similar traditional asset-management services. Often, the DeFi protocol will claim to identify the best yield-generating investment strategies available to investors and to use smart contracts that automate those investment strategies. These activities often are not engaged in with regulated intermediaries or regulated asset managers.

CLEARANCE AND SETTLEMENT ACTIVITY

As many DeFi activities and products rely on the blockchain to transfer ownership or interact with a smart contract, there is a dependence on the relevant blockchain for clearance and settlement to occur.

COMPARISON TO TRADITIONAL CLEARANCE AND SETTLEMENT ACTIVITY

TradFi: Financial markets and activities are supported by infrastructures responsible for clearance and settlement activities. These infrastructures are highly interconnected with institutions and systemically important to the proper functioning of financial systems, facilitating netting activities between counterparties, providing a mechanism to safely transfer ownership of assets and move value between parties.

DeFi: Certain activities in DeFi are captured directly on the blockchain, where the exchange of assets can occur "atomically," i.e., simultaneously. However, depending on the DeFi arrangement and the consensus mechanism used by the blockchain, there could be questions about settlement finality. Also, as an increasing number of DeFi products and services develop on a particular underlying blockchain and transactions inevitably compete for processing by the consensus mechanism, scalability becomes an increasing challenge, leading to slower settlement times and increased transaction fees. This impacts accessibility as only larger players/participants will be able to afford to pay transaction fees.

Solutions to this scaling challenge are being considered, including various "Layer 2" mechanisms, such as lightning networks and roll-ups, involving off-chain activity which enables the execution of multiple transactions where the net of those transactions will be represented as a single block on the blockchain, allowing for multiple transaction to be processed at once.

In addition to DeFi activities on a blockchain, there are other DeFi related activities involving centralized crypto-asset trading platforms and other service providers, where transfers and settlement of crypto-asset transactions, including those involving stablecoins, occur off-chain. These activities, in most cases, are reflected only on the internal books and records of the centralized crypto-asset trading platform or service provider.

CUSTODY AND CUSTODIANS

In some DeFi protocols, custody of assets is said to be retained by users. However, when interacting with certain DeFi products and services, users may "deposit" or "lock-up" their assets in smart contracts -

handing over management of those assets to the smart contract. In some cases, an individual, group of individuals, or entity will retain an "administrative key" to that smart contract and, as such, may have control over participant assets. In some cases, a participant can connect a self-custodial wallet to a DeFi product or service. Thus, users can have full control of the private keys that allow them to access their crypto-assets.

COMPARISON TO TRADITIONAL CUSTODY AND CUSTODIAN ACTIVITY

TradFi: Regulated firms will take custody of securities and fund holdings on behalf of investors for safekeeping and administration of assets, preventing and mitigating instances where assets are subject to theft or loss.

DeFi: In DeFi, some protocols may allow users to self-custody through their own wallets. The retention of the crypto-asset by a user will depend, however, on the type of DeFi protocol the participant is engaging with. In some protocols, users may be required to deposit or lock up their digital assets in a smart contract, thus subjecting them to the risk of theft, hacks or other cyber vulnerabilities that may allow others access to users' crypto-assets. Even for users who self-custody their crypto-assets in their own wallet, there exists the risk that their private keys will be lost or compromised, and crypto-assets as a result may be forever lost or stolen.

PRINCIPAL PARTICIPANTS

Key to the ongoing development and operation of DeFi, and all of its products, services, arrangements and activities, are the various DeFi market participants. There are a number of primary participants in the DeFi market as discussed below. These include entities undertaking the creation and development of protocols, their financial backers, and users of the protocols once they are deployed. DeFi aspires to decentralize ownership and governance of financial services, such that a dispersed community of users make relevant decisions regarding the maintenance and growth of the financial service, instead of a centralized financial intermediary.

PROTOCOL CREATORS AND DEVELOPERS

In DeFi, as in other crypto-asset markets, there are entities that create and introduce software through which DeFi operates. These entities often obtain funding for their development efforts in traditional capital raising as well as through crypto-asset offerings. As protocols are developed, developers often create a reserve or "treasury" to hold fiat or crypto-assets for purposes of funding future refinements and development of the protocol. These entities may either retain these reserves themselves or may create a different organization that takes on the responsibility to manage the reserve or treasury. The specific organizational forms that create and launch protocols and those that are responsible for ongoing activities can vary. These key types of entities include traditional corporate entities, foundations that often hire contractors to work on the protocol, and DAOs.

DAOs

DeFi market participants continually experiment with new organizational structures in an attempt to achieve more decentralized systems. A DAO is a relatively new type of organizational structure that focuses on community, as compared to centralized, governance. There is no agreed definition of what constitutes a DAO.[21] In general, participants who promote DAOs claim to organize around a mission, or set of missions,

[21] There are various types of DAOs, each formed by different types of like-minded community members with different intents at their core. This is not intended as an exhaustive list but covers many of those that exist today in the market:

and coordinate their growth through a shared set of rules enforced via mechanisms built on a blockchain. They state that, in lieu of a management committee or board of directors, holders of the DAO's "governance" token act as a decentralized governance body to vote on the direction of the protocol or for resetting specific parameters (e.g., the level of collateral needed for borrowing).[22]

Generally speaking, a DAO seeks to emulate the operation of a corporate entity through code. While the governance, operations, rules, bylaws, and policies of a corporate entity are set forth in its corporate organizational documentation pursuant to applicable law, DAOs are designed, ideally, to automate operation according to a blockchain-based form of governance with all aspects written as participatory code represented in smart contracts. Typically, a DAO's governance is effectuated through voting by governance token holders. DAOs claim that there is no central authority or ownership and governance is said to be distributed by design to the community of users. Furthermore, the manner in which a DAO conducts itself is stated to be entirely transparent, as one could theoretically check how a DAO is operating by viewing its blockchain address where all transactions are recorded. However, whether the governance is actually decentralized, including what voting proposals are put forth and how voting is implemented (as well as how the approved proposal is affected) depends upon the facts and circumstances. For example, depending on the facts of any particular DAO, there may be concentrations of governance token holders, managing entities overseeing voting and implementation of votes, or other circumstances that, in reality, show that a DAO is in fact centralized. DAOs also may rely on social media tools, e.g., permissioned communication channels, that may give rise to information asymmetry and governance influence over DAO activity.

While DAOs are a novel structure, they are not without drawbacks. DAOs are typically not recognized as corporate entities and therefore do not have the same legal definitions and protections as other structures (such as a limited liability corporation). DAOs also may lack the ability to make fast decisions due to the need to corral voting consensus amongst such a broad governance community. Governance token holders may also show apathy towards more 'mundane' proposals up for vote, leading to low voter turnout and/or cases where votes are delegated to concentrated stakes holders.

COMPARISON TO TRADITIONAL CAPITAL RAISING

*TradFi***:** An organization looking to raise capital typically faces a choice between two well-understood financing routes: debt and equity. Both require the involvement of a centralized party that is raising funds in return for an equity share in the entity or interest payments on a loan. The organization will quite often rely on the services of other centralized third parties (e.g., investment banks, broker-dealers, underwriters) in the process and pay fees for those services.

*DeFi***:** Although fundraising is still being done through centralized token distributions, recently more projects in DeFi have experimented with fundraising through DAOs. While the operation of a DAO over

Protocol DAOs (exist to build a protocol); Social DAOs (exist to build communities); Service DAOs (exist to bring together and coordinate individuals for certain projects); Investment DAOs (exist to pool capital to deploy into investments); Grant DAOs (exist to patronize and support early-stage protocols); Collector DAOs (exist to own certain assets); and Treasury DAOs (exist to maintain funds raised).

[22] Users can join a DAO by connecting their wallet addresses and, in some cases, they may be required to commit upfront capital to participate. Such contributions, combined with any additional profits from protocol activities and capital appreciation of their governance token are just some of the ways that DAOs have been able to accumulate substantial treasuries which they can use as befits the intent of the DAO or as determined by code or voting by members or contributors.

the long term may reduce centralization, initial organization and fundraising by a DAO likely still involves centralized actors.

BOX 3: GOVERNANCE TOKENS

Some DeFi proponents view the advent of governance tokens as the solution for eliminating central actors in DeFi products and services. Here one can again draw distinctions between those products or services that can exercise more centralized governance (e.g., through administrative keys) and those that assert to exercise more decentralized governance (e.g., through, in theory, governance tokens). It is important to recognize that concentrated ownership of governance tokens or voting rights would weigh against viewing governance tokens existence as a measure of decentralization, either of a smart contract or of a protocol more generally.

The issuance of governance tokens to users has become an increasingly common approach to distributing decision-making regarding protocols and smart contracts and stands in contrast to "admin keys," which provide holders with a backdoor to unilaterally amend and update the underlying smart contract infrastructure as they see fit. Governance tokens are not confined to a particular token standard, such as ERC-20 or ERC-721, meaning that at a technical level, they vary in practice according to how a particular protocol has issued its governance token. While governance tokens have been presented as offering community decision making without central actors, in reality for typical DeFi protocols today, there continues to be central actors with concentrated ownership and voting.

Governance tokens are tied to a specific DeFi protocol and purport to provide holders with economic rights and/or with voting rights on future changes to certain features of a protocol. They do not, however, provide control over the protocol at the enterprise level and in most cases the entity behind the protocol. Potentially in the future, including through the development of a truly decentralized DAOs, governance tokens may in fact transfer agency, responsibility and control of protocols to their users allowing them to determine how to allocate treasury funds, who to hire, and how to operate the business. To date, however, while there are many examples where a quorum of votes by governance token holders have led to certain changes being implemented, some voting proposals are still controlled by central parties through control of, for example, communication channels. Similarly, while in some cases a voter-approved decision can be automatically executed on-chain, in other cases central parties and developers control the actual implementation of a voter-approved software change.

In many cases, governance involves both off-chain and on-chain activity. Off-chain applications (e.g., Snapshot) may enable the community to, among other things, "test the waters" with respect to a proposal before putting it to a vote and implementing it on-chain. Other off-chain applications (e.g., Discord) provide communication channels for discussing proposals.

Typically, a single governance token will entitle the holder to a single vote, and votes can also be delegated by those holders who do not wish to participate in voting. Though they can be designed to be user-inclusive, these governance voting systems have been criticized for encouraging plutocratic decision-making (as the amount of tokens one has determines how much voting power one wields).

When looking at token-based governance systems it is useful to consider:

- Governance tokens vary and do not typically endow unilateral control on holders as they operate within hard-coded parameters set at issuance.

- Governance tokens may not have an intrinsic value like common stock, but they have become commonly used as a speculative investment instrument and are often tradable on centralized crypto-asset trading platforms. This means that the corresponding voting rights often are not utilized or are delegated to parties who act as centralized voting entities.
- Governance token ownership distribution may be concentrated. There are instances where governance tokens are either pre-mined and thus more heavily concentrated in the hands of earlier investors and developers, or otherwise have become concentrated in the hands of investors and others with the resources required to actively participate in voting. In some cases, voting rights can be delegated. In such instances, where a large proportion of governance tokens or voting rights rests with a small group, governance becomes effectively centralized or vulnerable to being influenced (in the same way as might happen in TradFi with activist hedge funds).
- Token based governance structures differ among DeFi products and services.

DEFI INVESTORS

Central to DeFi are investors who have been observed fulfilling two primary roles. First, in some cases, investors, primarily institutional investors such as venture capital funds and private equity funds, provide capital for the protocol creators and developers to fund the development and deployment of the protocol. Second, in some cases, investors play a key role in protocol activity by engaging in and investing in the DeFi products and services of the protocol. These may be institutions and a significantly growing number of retail investors. The following discusses the types of investors and the ways in which they participate in DeFi. DeFi has attracted different types of sophisticated investors including traditional institutional investors, hedge funds, and venture capital funds.

VENTURE CAPITAL FIRMS

The primary participants to date in funding DeFi development are venture capital firms and investors. In 2021, about 25% of all venture firm funding for crypto projects involved DeFi (the largest sector allocation), with over 420 deals raising more than $1.9b.[23] These investments typically involved purchases of equity in a DeFi-based business, usually with rights to receive governance tokens. Such investments helped fuel the growth of DeFi, often sustaining protocols from the ideation through deployment of complete protocols. VCs benefit in the short term, as these protocols can start monetizing on their idea immediately after launch. Importantly, VCs look to the receipt of governance or other tokens traded on centralized crypto-asset trading platforms for immediate liquidity to monetize a return on their investments and, for some, giving them the rights to significant voting power and governance.

HEDGE FUNDS

Hedge funds (private funds) engaging with DeFi appear to invest in relatively liquid assets for complex trading strategies across yield-farming, staking, and lending/borrowing protocols. In addition, they routinely trade on DeFi trading platforms. DeFi hedge funds generally employ two types of strategies: 1) analyzing fundamentals to find investment opportunities, and 2) algorithmic trading. In either case, much of the DeFi trading activity by hedge funds centers on taking advantage of short-term market-neutral arbitrage opportunities, which may exist between different DEXs or borrowing/lending markets.

[23] See The Block Research, 2022 Digital Asset Outlook, available at https://www.tbstat.com/wp/uploads/2021/12/The-Block-Research-2022-Digital-Asset-Outlook.v2.pdf.

TRADITIONAL INSTITUTIONAL INVESTORS

Until very recently, institutional investors largely appear to have limited their participation in DeFi protocols, which they have indicated are due to issues around DeFi protocols' compliance with applicable jurisdictional regulations as well as the institutional investors' ability to ensure compliance with their own internal or regulatory requirements. However, this past year saw the launch of multiple vendor products and services that were aimed at institutional investors, including those involving trading, best execution, and custody, which appears to have encouraged more institutional firms to commence DeFi activity. In addition, the DeFi infrastructure recently began offering institutional firms potentially safer access points to DeFi, such as permissioned lending pools (for KYC/whitelisting), trading systems resistant to miner extractable value (MEV), and decentralized identity management. Institutional investors are attracted to the potential for yield they perceive as being available through the DeFi market. There is an increasing interest from certain fund managers to build investment strategies based on DeFi, including investing in protocols across a number of different blockchains to access potential additional yield from lending, liquidity pools, farming and staking in the DeFi ecosystem.

Many large multi-national banks and asset managers recently publicized their interest in crypto-assets broadly, both for themselves and their clients, and DeFi specifically. Services beginning to be offered by these institutions include custody, active investing in governance tokens, staking, and asset tokenizations.

RETAIL INVESTOR PARTICIPATION

The growth of DeFi protocols (and interfaces that do not require technological sophistication) and the development of pooled investment structures has led to a dramatic increase in retail participation in DeFi and access to DeFi products and services. This involvement is facilitated by the increasing use of social media and celebrity endorsements of DeFi investment opportunities.

Retail investors are often drawn by descriptions of investing opportunities or crypto-assets through social media. They are drawn by profit-making opportunities, including rates of return or types of investments that they cannot access in the traditional market. Participants talk about their non-financial gains from participating in protocols. They discuss the value of contributing to projects and being part of communities that reflect their personal values.

Innovative technologies on the blockchain have led to the proliferation of hedge fund-type activities in DeFi, including by enabling retail participation by investors who are otherwise unable to engage in these activities in traditional markets. For example, "vaults" are a mechanism for smaller-ticket investors to participate in on-chain "hedge funds" by deploying capital into single or multi-strategy pools run by smart contracts. Similarly, products such as yield-farming aggregators or pools enable greater retail participation in DeFi. Other DLT-centric innovations include on-chain (via smart contracts) services such as custodianship, fund administration, accounting, trading, and risk management, which has reduced start-up costs associated with launching a traditional hedge fund off-chain.

As with other investment products, DeFi has attracted individuals and entities who engage in promotional and marketing activities for various protocols. Marketing firms and freelance promoters provide services for product promotion and media outreach, especially for website design, search engine optimizations, and social media campaigns. Some act as consultants, advising protocols on how to scale faster, attract new users, and increase their capitalization and liquidity. A subset also assists with other aspects of DeFi, including audit, legal consulting, white paper writing, financial modeling, product development (including the economic uses and incentives for tokens, called tokenomics), and token distributions and offerings.

Novel fundraising techniques also have emerged in the DeFi ecosystem, some or all of which may implicate securities frameworks or other regulatory frameworks in some jurisdictions. As with Initial Coin Offerings ("ICOs"), depending on the jurisdictions, these more recent types of funding activities may not necessarily have been conducted in compliance with applicable securities laws or may not currently be subject to securities laws in certain jurisdictions.

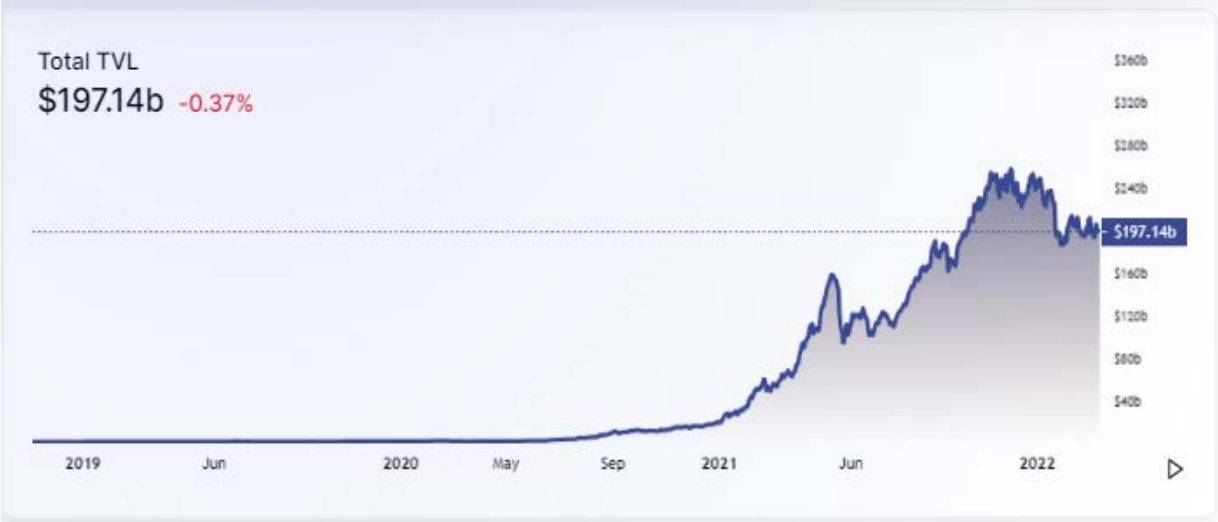
THE "BIG PICTURE" WHY DEFI GROWTH HAS OCCURRED

The reasons for the recent growth in DeFi are multifaceted, and there are multiple underlying incentive mechanisms that have helped fuel participation. DeFi relies on the contributions of various stakeholders, each of whom has an important role to play in making the system work and expects to earn a profit through participation. These stakeholders include creators and developers of a DeFi protocol (the "protocol development group"); investors in the protocol development group and/or protocol; protocol users; service providers; and blockchain networks.

First, early investors have recognized the opportunity to allocate capital to nascent technologies with venture-type return (and risk) profiles. Second, crypto-asset holders have recognized a market thirsty for liquidity and so they perform market-maker and related services to DeFi protocols. Third, TradFi and CeFi market participants have sought to diversify their activities and to seek yield in DeFi as an alternative platform with the potential for diversified higher returns. Fourth, blockchain communities have encouraged the proliferation of DeFi projects on their platform, as they are aware that their network can only scale with its adoption. Fifth, early adopters and proponents of crypto-assets have seen DeFi as a place where they can invest in products and services that align with their general outlook for this industry. These primary factors, and likely others, have fueled the growth of DeFi.

Industry measures for the size of DeFi participation, although unverified, include identifying the USD value of crypto-assets that are "locked" in smart contracts on a particular blockchain. The chart below, from an industry source, shows the growth in DeFi across blockchains, as measured in "Total Value Locked" (TVL).

Total value of assets locked in DeFi transactions



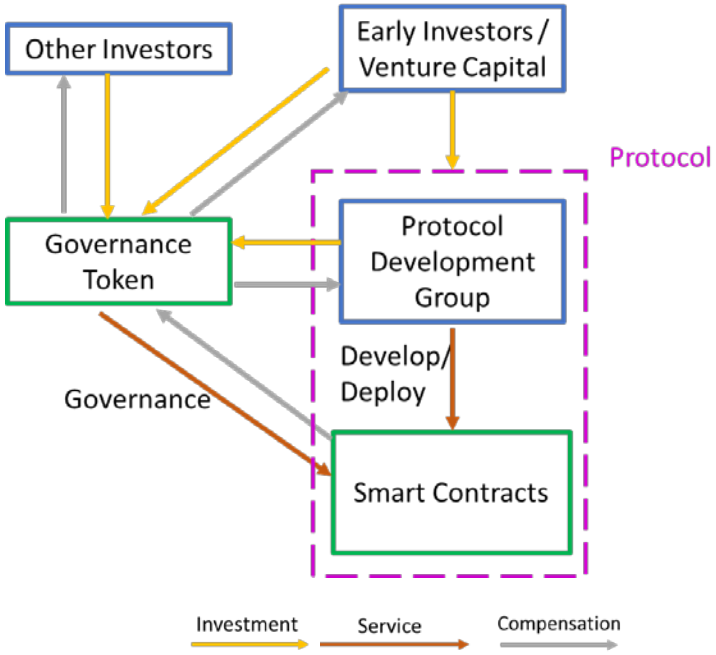
Total value locked in US$ (billions)

Source: defillama

The "Big Picture" of DeFi can be broken down in terms of three primary components: capital formation, development and deployment; use and investment; and settlement.

CAPITAL FORMATION, DEVELOPMENT, AND DEPLOYMENT

To execute their business plans, protocol development groups typically rely on venture capital firms and other institutional investors, who contribute capital and provide advice in exchange for an economic stake in the protocol development group and/or the protocol. All projects need capital for expenditures and growth, which they store in their respective treasuries until needed. During the pre-deployment stage, protocol developers typically raise capital from angel investors and venture capital funds in order to fund the protocol's development and the creation and maintenance of apps that bring user participation to the protocol via user interfaces. Early investors may obtain equity in the company developing a protocol as well as the right to receive future tokens, including governance tokens of the protocol, once the protocol is launched and deployed to a blockchain. The protocol development group, as well as its founders and employees, also may receive an allocation of governance or other tokens upon the launch of the protocol as compensation for their efforts. These parties also often continue to be involved in the project through participation in a DAO or foundation as well as by developing apps for the protocol. These activities may involve, for example, promoting the protocol and operating a website or mobile app that facilitates use of the protocol.

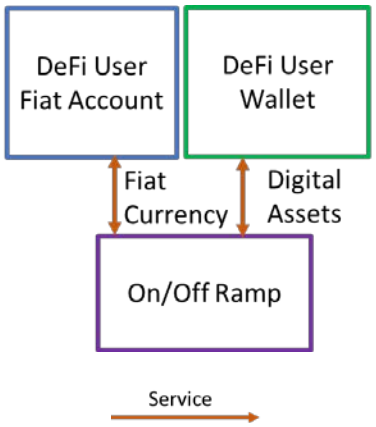


Following launch, in some cases control of the protocol, including code changes and project funding from retained capital or from unsold governance tokens (referred to as treasury) may be transferred to a separate group or entity (e.g., a foundation or DAO). In addition, code changes in smart contracts and in protocols as well as decisions on spending the treasury may, depending on the protocol, be subject to governance token holder voting. Depending on the particular DeFi arrangement, the developers, early investors, and others holding material amounts of governance tokens may continue to influence the development and maintenance of the protocol. The ongoing development group, whether a DAO, a foundation, or a corporate entity, may use governance tokens it holds to raise additional capital in trading activities on centralized crypto-asset trading platforms. These participants also may use CeFi and DeFi products to raise capital, such as by selling governance tokens to other investors through, for example, a centralized crypto-asset trading platform or a DEX. The governance tokens afford early investors and others the opportunity to not only influence the direction of a DeFi protocol but also experience venture-type returns (and risks) as they are tradable on both CeFi and DeFi trading platforms. The factors driving the economic value of governance tokens can vary. It could be driven by speculation, real economic rights and interests (e.g., distributions of fees generated by the protocol), or both.

Once the protocol is deployed, it may contain a treasury consisting mostly of its own governance token. A project's pathway to decentralization may include a distribution of governance tokens to early adopters (sometimes accomplished through "airdrops"), protocol users and liquidity providers, engineers that evolve and improve the code, purchasers of the tokens in the secondary market, and third-party service providers (e.g., auditing firms) that are paid in tokens for their services. It may be the expectation of those who are compensated in governance tokens for investment, usage, or service that these governance tokens will appreciate over time due to increased demand in the secondary market and/or fees paid by the protocol to token holders.

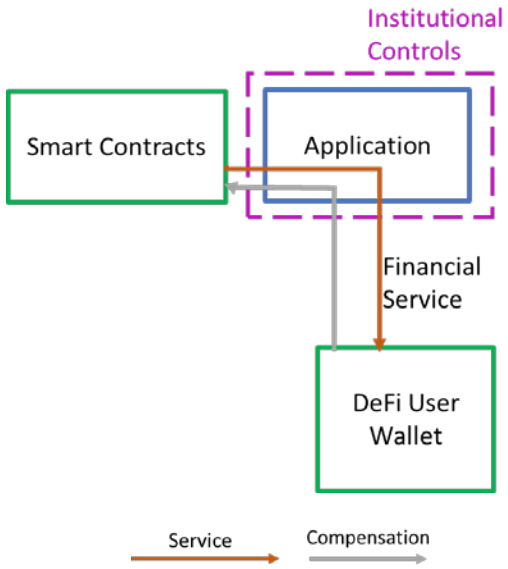
USE AND INVESTMENT

DeFi protocols enable disintermediated transactions between providers of capital and users of capital. Nonetheless, to use DeFi protocols, participants on both sides of a transaction need crypto-assets, which they generally acquire and, in many cases, hold through certain intermediaries for a fee. TradFi and CeFi service providers, such as centralized crypto-asset trading platforms working with banks or other financial institutions, are integral to DeFi as they serve as the fiat currency on- and off-ramps and provide custody and other solutions that enable participants to hold and use their crypto-assets. Individuals and institutions typically go to a crypto-asset trading platform or kiosk (e.g., crypto-asset ATM) operated by a centralized entity to convert fiat currency into crypto-assets. As noted above, centralized crypto-asset trading platforms play a key role in the issuance, trading, and redemption of many fiat-based stablecoins.

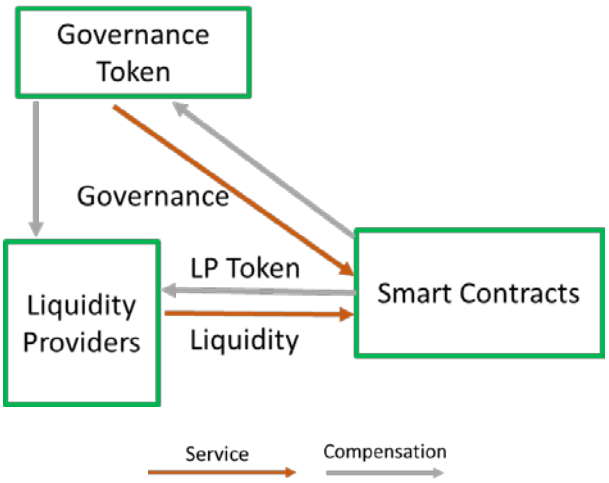


Many DeFi protocols create their own crypto-assets, which are sometimes used in transactions, and which sometimes become tradable on secondary markets. In the most-practical example, participants deposit or lock up their assets in a protocol, and the protocol's smart contract issues them a token that represents their financial exposure. Participants hold those tokens and then return them to the smart contract to close out their transaction and realize their profits or losses, for example removing their assets from a liquidity pool or a lending pool.

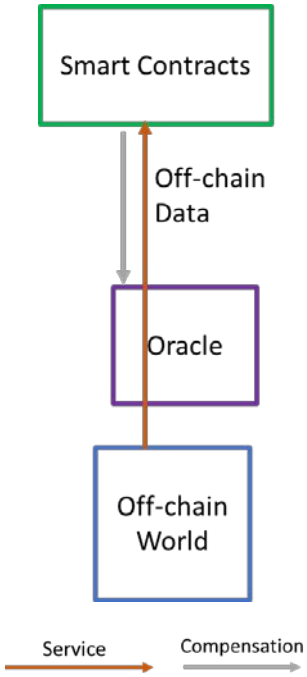
Retail investors and consumers typically use the services of a self-hosted wallet provider to access DeFi protocols, which involves transferring crypto-assets from their account with a centralized entity to their own wallet. Institutional investors typically prefer or require a different set of controls that enable them to engage in DeFi transactions while keeping their crypto-assets in the custody of a centralized entity. While many individuals prefer to retain control of their crypto-assets while engaging in DeFi transactions, they may also access DeFi opportunities through their accounts with TradFi and CeFi entities insofar as those entities have integrated their platforms with DeFi. In sum, these service providers are critical to the functioning of DeFi as they are needed to enter, use, and/or exit the space.



Through participation in various DeFi products and services, DeFi participants are able to use their crypto-assets in a multitude of ways to earn additional returns, including by providing capital and investment to developing DeFi projects. These economics hold true in DeFi as well, where there is a need for the virtuous cycle of attracting capital to attract users to attract more capital, etc. Current holders of crypto-assets, therefore, see an opportunity to put these assets to work by 'locking' them in a single protocol in exchange for LP tokens and/or governance tokens, or by yield-farming or liquidity mining across multiple protocols to dynamically maximize their yield. The highest yields are offered by protocols with the lowest liquidity, thereby incentivizing liquidity to be well distributed across the DeFi ecosystem. In addition to seeking to profit by becoming early investors in DeFi protocols and using the functionality of the protocols, some institutional investors (e.g., hedge funds) use their capital and other resources to develop sophisticated systems for the identification of other yield-generating opportunities. One example of this is the development and use of bots to identify arbitrage opportunities across DEXs or opportunities to buy collateral from a lending protocol at a discount. These advanced trading strategies essentially take advantage of inefficiencies in the system and may involve the use of novel products like flash loans. For retail investors who connect through social media primarily, those communication channels are especially important to build the network effects crucial to most protocols. Importantly this means the limits of these systems (ecochambers, closed ecosystems etc.) are imported into the use of DeFi offerings. As well as the aspects around developing a social movement towards certain (perhaps only claimed) goals. There is also the aspect that though this is socially driven as something 'new' many in the community choose to program what already exists (e.g., existing financial products in economic terms).



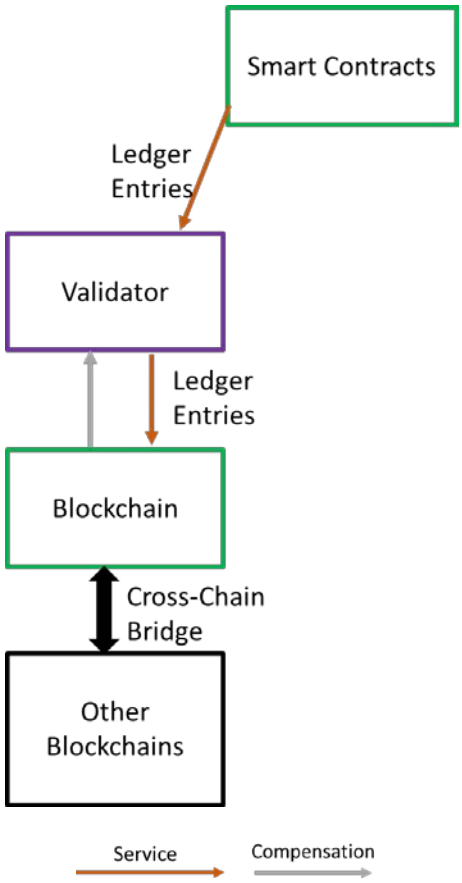
DeFi has a burgeoning market for service providers that also profit from the growth and adoption of this ecosystem. For example, oracles get compensated by protocols for acting as the data provider for off-chain information such as stock prices, off-chain collateral value, or election results. Wallet service providers, while not typically paid directly from protocols, enjoy growth in their user base from DeFi users signing up for wallets for the purpose of accessing DeFi services. Additionally, custody and KYC/AML service providers are increasingly partnering with protocols to bring "institutional quality" to DeFi for those participants that require it for their own compliance needs.

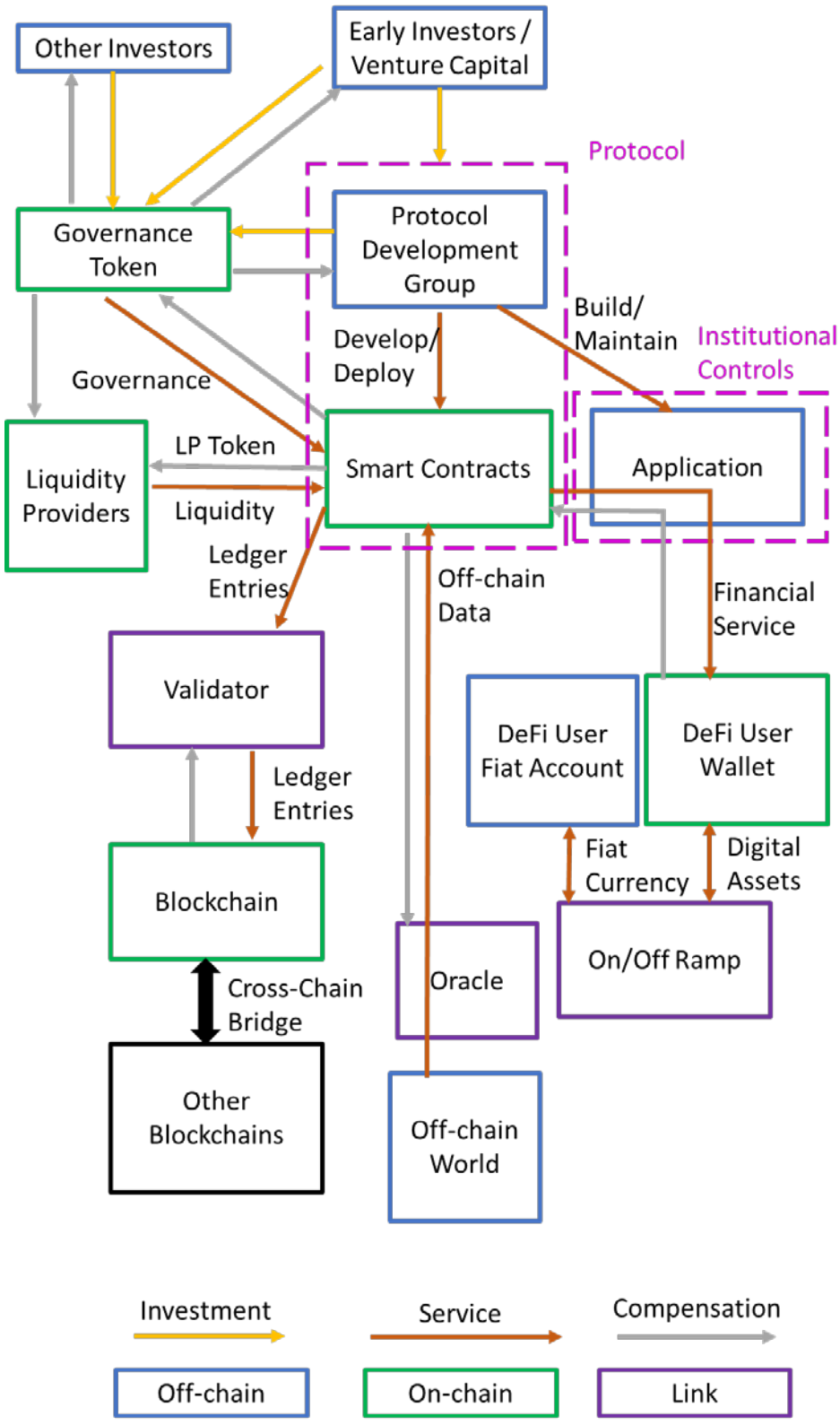


SETTLEMENT

DeFi protocols rely on a blockchain for transaction execution and settlement. The strength of a public permissionless blockchain network depends on the number of nodes that actively participate in mining and/or validating transactions. These network participants require compensation for their work and are incentivized by receiving a "block reward" and/or fees that are paid by protocol users for transaction

settlement. Both forms of compensation typically are paid in the native crypto-asset of the blockchain, whose value generally correlates with the amount of activity occurring on the blockchain. Further, a higher value incentivizes more nodes to join the network and validate transactions, thereby creating a stronger and more resilient network. Given these dynamics, blockchain networks are actively seeking to attract DeFi protocols to deploy on their blockchains. Blockchains compete based on a number of measures, including the speed and cost of transaction settlement, and they may engage in such promotional activities as distributing their native crypto-assets to DeFi protocol users to increase use and engagement on their platforms. DeFi protocols may run on multiple blockchains, in which case cross-chain bridges are relied upon.





DEFI: THE BIG PICTURE

KEY RISKS AND CONSIDERATIONS

At its core, DeFi seeks to obviate traditional intermediaries between parties to transactions. Although it is argued that disintermediation allows for faster, cheaper and more efficient execution of transactions, it also eliminates market participants that have traditionally acted as gatekeepers, performing central roles of ensuring investor protection and market integrity. Some intermediaries, for example, provide investment advice to assist investors in understanding the potential benefits and risks of a particular investment. Others provide real-time information about investment products, companies and markets to reduce information asymmetries and allow investors to research potential investments. Intermediaries also impose structural constraints upon users, such as capital and liquidity controls, AML/CFT protections and compliance, and targeted financial sanctions monitoring. They also can provide protections against losses as a result of bankruptcy and theft. These are important investor and market protections that seek to minimize fraud, reduce systemic risk and contribute to fair, efficient and equitable markets. Absent these intermediaries – and without appropriate substitute mechanisms – the risk for investor and market harm may be exacerbated.

Although DeFi has been presented as providing certain benefits, it also presents numerous risks to participants, including to investors and the markets, currently and as it develops. The DeFi market and its participants in many respects have operated to date either outside the scope of existing regulatory frameworks or, in some jurisdictions, in non-compliance with applicable regulations. The below discussion addresses the primary risks that DeFi presents to investors and markets. It is not an exhaustive list.

ASYMMETRY AND FRAUD RISKS

DeFi allows investment in a variety of products and services – including risky speculative trading, lending and borrowing activities – often on a cross-border basis and with 24/7 availability. Relatedly, DeFi can pose significant potential for investor harm.

Retail investors in DeFi projects typically form part of an online community or otherwise are brought into DeFi through influencers, social media, and other forms of digital engagement and promotional activities, which can be a prominent avenue to gain more traction. Misinformation and inappropriate advertising using these promotional channels present well-understood risks to investors.[24]

Many DeFi products and systems fail to provide important disclosures. Although blockchain data and smart contract code is transparent for all to see, understanding this data and code requires technical capability and knowledge. Without basic regulatory safeguards, including those that are the purpose of traditional financial services regulation, such as requirements for the disclosure of material information about a product, service or the individuals and underlying entities, investors may not necessarily receive sufficient information to make informed investment decisions. Some DeFi products and systems may require certain technical or other expertise that not all investors have and, as a result, may be unsuitable for some investors. There may be hidden informational or technological advantages sophisticated participants have over retail investors that make for an uneven playing field. Even absent fraud or misconduct, investors may lose some, if not all, of their investment due to these asymmetries.

There are key risks to retail investors participating in secondary markets, separate from fraud and market risks discussed below. Specifically, although some DeFi participants may strive to afford greater financial inclusion for products and systems, certain participants have designed DeFi products and systems in a way that may concentrate the cost of failure on individual investors, as opposed to protocol creators and

[24] *See, e.g.*, IOSCO Report on Retail Distribution and Digitalisation (Jan. 2022), available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD695.pdf.

institutional investors. For example, certain projects have raised money through venture capital firms or other large investors who monetize their investment as retail investors later invest. Creators and large investors may have structured capital raising using DAOs, governance tokens, and other mechanisms, as a way to make a profit while avoiding financial responsibility for the failure of a project. In some cases, this has resulted in the asymmetric concentration of risk.

Increased activity in DeFi has also increased the likelihood of and opportunity for bad actors to perpetrate fraudulent schemes and engage in illicit activities and other misconduct. There have been numerous reports of DeFi fraud schemes in the form of exit scams and rug pulls (orchestrated by developers and/or influencers who promote a project and, ultimately, escape with the money at an agreed time), Ponzi schemes and other types of fraud and misconduct, such as the theft of private keys. DeFi can facilitate a swift, anonymous and often untraceable exit, leaving those defrauded with little, if any, recourse.

MARKET INTEGRITY RISKS

DeFi systems and products largely involve speculative trading, lending and borrowing, sometimes involving highly-levered strategies. Thus, risks analogous to those in traditional markets also exist. These risks include those caused by trading and price misinformation or manipulation and conflicts of interest. DeFi also introduces risks that are somewhat unique to DeFi, such as those discussed below.

FRONT-RUNNING (OR SIMILAR FRAUDS)

On certain blockchains, miners are able to profit by using their ability to re-order or censor transactions that have been submitted to the blockchain. This has been referred to as MEV. This can occur when blockchain validators or anyone with first-hand information of transactions in the queue for validation uses this information and advanced technical skills to maximize their own profits. One type of activity involves front-running or trading ahead of transactions in the queue of transactions to be validated in order to gain advantage. Typically, a front-runner can re-order transactions in the queue by paying a higher gas fee to place the front-running transaction in front of others in the queue. Usually, the faster the blockchain, the harder it is to front-run transactions. Generally, the Ethereum blockchain, upon which most DeFi apps are built, has been vulnerable to front-running as perpetrators have had sufficient time to re-order transactions in a favorable way. Front-running can result in users with transactions that have been re-ordered obtaining less favorable transaction terms. If enough front-running occurs on any particular blockchain, it can result in stale transactions, faulty consensus and an ultimate loss of confidence in the ability of the blockchain to process transactions and achieve settlement finality.

FLASH LOANS

As discussed above, a flash loan is a type of uncollateralized lending that has been seen on DeFi protocols on the Ethereum network. Flash loans use smart contracts that do not permit the exchange of funds unless the borrower can repay the loan before the transaction ends, otherwise the smart contract cancels the transaction. Typically, the flash loan uses other smart contracts in a trading strategy designed to make a profit. A common use for flash loans is to execute a trading strategy around an arbitrage opportunity. As long as the strategy can be executed instantaneously and yield sufficient profit to pay back the loan plus interest and any fees, individuals can use the flash loan to gain access to large amounts of capital with no up-front collateral in order to execute the strategy.

However, flash loan protocols can facilitate the rapid exploitation of a vulnerability, such as a coding error in a smart contract. In other cases, a flash loan could be used to facilitate manipulative conduct. For

example, some AMM prices are prone to manipulation through the creation of an imbalance in the pool, resulting in slippage and arbitrage opportunities.

MARKET DEPENDENCIES

For DeFi protocols to function properly, the participation of certain actors may be required. These can include diverse actors such as validators on the underlying blockchain, arbitrage traders, liquidity providers, oracles, etc. Although incentive structures exist to promote that participation, mainly through what is coined "tokenomics," arbitrage opportunities, fees, and other profit-making mechanisms, these structures may fail, causing a protocol ultimately to fail. In traditional markets, participation by key participants may be supplied or augmented by regulated entities that currently are not acting to support the DeFi ecosystem.

As a specific example, various DeFi protocols are highly reliant on a few fiat-backed stablecoins as critical sources of liquidity. These protocols are, therefore, highly dependent on the continued viability and existence of these stablecoins. To the extent that there is any event, whether from a regulatory action, issuer default, or some other factor, that impacts the value of the stablecoin, the collateral and liquidity that is the engine for these DeFi protocols would be significantly impaired, potentially resulting in systemic failures of these DeFi protocols. See "Role of Stablecoins in DeFi."

USE OF LEVERAGE

Many DeFi products and systems offer the use of leverage. For example, crypto-assets borrowed from one lending protocol can be used as collateral in another, thereby using the same underlying assets to build an increasing number of positions. This can exacerbate liquidation risks if they were to materialize. Leverage is also seen in the trading of derivatives in DeFi protocols, which often offer high margin levels.[25]

ILLICIT ACTIVITY RISKS

Although some industry participants are beginning to explore the use of AML/CFT tools with their protocols, many products and services in DeFi have no requirements for AML/CFT measures, presenting potentially significant anti-money laundering and terrorist financing (AML/TF) risks. Further, illicit actors are using sophisticated anonymity-enhancing technologies, such as anonymity-enhanced cryptocurrencies (AECs), mixers, tumblers and other technologies, to obfuscate the details of financial transactions. The result is that, under the cloak of anonymity, illicit actors can easily circumvent traditional AML/CFT frameworks and similar supervisory regimes and store proceeds of crime, elude sanctions and launder money. There are significant risks for those transacting in DeFi to engage with a sanctioned counterparty or with crypto-assets sourced through illicit activity.

OPERATIONAL AND TECHNOLOGY-BASED RISKS

Operational risk refers to the risk that deficiencies in information systems or processes, human errors, management failures, or disruptions from internal and external events will result in the reduction, deterioration or breakdown of products and services. DeFi seeks to shift trust from traditional intermediaries to technology and, therefore, presents inherent technology-based risks.

Blockchains

DeFi applications generally rely on public blockchains for settlement and contract resolution. However, the operation of a blockchain is not always seamless and blockchains differ significantly in their

[25] For a discussion of the procyclical effects and destabilizing impact of leverage in DeFi, *see* Aramonte, Huang & Schrimpf, DeFi Risks and the Decentralization Illusion, BIS Quarterly Review, December 2021, available at: https://www.bis.org/publ/qtrpdf/r_qt2112b.htm.

implementation and network health at any given time. Recognizing the existing risk of the potential for intermediary failures in traditional finance, unlike in traditional finance where, for example, information systems and processes are governed by an intermediary, in blockchain, this responsibility lies with validators, who typically are economically incentivized to participate in a non-malicious manner. If the incentive structure does not sufficiently motivate a validator to participate or does not deter malicious behavior, the network could be compromised. As DeFi is blockchain-based, any disruption or manipulation of a blockchain that underpins a particular DeFi product or service -- including any forks, attacks or nefarious activity -- likely will directly impact the operation of a DeFi product or service.

Once a blockchain protocol vulnerability has surfaced or been exploited, addressing that vulnerability may require coordination of and consensus by the blockchain's validators to adopt a new version of the protocol (e.g., create a hard fork). There could be uncertainty and delay caused by this process and the need for community activity to galvanize decision-making. While this process occurs, there may be interference in normal blockchain settlement processes, calling into question transaction settlement finality.

Some blockchains are prone to validator concentration. If this occurs, the blockchain is susceptible to centralization of control over the consensus mechanism and the risk of self-interested or malicious behavior of validators.

Although DeFi activity is increasing on other blockchains, to date, almost all DeFi activity has taken place on the Ethereum blockchain. The reliance on Ethereum poses potential failure risks. High gas fees, congestion and transactional limitations on Ethereum impact the costs to investors and the efficiency of transactions. These conditions are exacerbated as more activity takes place on the Ethereum blockchain.

It bears mention that blockchains rely upon internet infrastructure, and that protocols may also rely on off-chain technology, such as cloud-based services and oracles. Therefore, any risks posed by the use of these technologies translate to DeFi as well.

Smart Contracts

Smart contracts are software that exist for the most part on public permissionless blockchains. While this open access can facilitate financial innovation, there are no technological restrictions on developers, including no required professional or licensing qualifications that govern who may deploy, manage, or engage with smart contracts. While participants do engage in efforts to test and vet code (e.g., through "bug bounty" programs), there are no formal code auditing requirements. Thus, anyone can develop, deploy and engage with new smart contracts that could subject DeFi participants to code vulnerabilities, fraud, theft and other significant risks. Many projects launch through copying another developer's code. While open sourcing of good code has certain advantages and efficiencies, the propagation of bad code can have adverse consequences. Further, since DeFi products and systems generally must be upgraded, there will be continuing risk of coding error.

Smart contracts are what determine a crypto-assets' technological features and any vulnerability or bug in the smart contract code that controls or engages with a crypto-asset, if it surfaces or is exploited, could adversely impact any crypto-asset issued, tracked or held by the smart contract, and could permanently impair the crypto-asset's function and value.

In addition to risks to assets and protocols impacted by smart contracts, there are additional vulnerabilities that arise due to the composability feature of many smart contracts. Smart contracts typically are designed to be composible, i.e., they may interact with other smart contracts in that they may essentially be "daisy

chained" together to compose new products and systems. It is difficult to anticipate all potential issues that may arise through this daisy chaining.

Further, the ability to modify or upgrade a smart contract, once deployed, may be limited, unless and to the extent that the smart contracts was created with the ability to delete or alter the contract after creation. Thus, a smart contract can essentially operate in perpetuity on a blockchain, regardless of administrator or user behavior. Some will exist even if administrators or users wish to disable them. For other smart contracts, administrators may have retained an "administrative key" allowing them to delete or alter the contract after creation.

Oracles

Oracles – and the off-chain information that they supply to smart contracts – are a crucial aspect to the operation of many protocols, including those that rely on oracles to supply the current value of assets held as collateral. Risks can arise from the use of oracles. Centralized oracles, for example, are vulnerable to malicious behavior of the oracle provider, as well as to coding errors, attack or manipulation by others. More decentralized oracles may still be open to these vulnerabilities. Bad actors have employed oracle attacks to profit, for example by triggering liquidations based on faulty information. Even absent error or misconduct, the provision of certain information by an oracle can be delayed, which can cause stale information to be delivered to a smart contract and, in turn, create adverse consequences for those using the smart contract if market conditions have moved against them during the time delay.

CYBERSECURITY

Cybersecurity risk management policies and procedures are core elements of a traditional securities and capital markets regulatory framework. Perhaps due to the nascent and permissionless nature of DeFi, protocols and smart contracts have been susceptible to cybersecurity attack, and particularly hacking. As of the end of 2021, the total amount of money lost due to smart contract, software and crypto wallet hacking was reported at more than $10 billion, with more than $2 billion stolen in 2021 from DeFi alone, representing an increase in loss value of over 1300% from 2020.[26] Hacks can result in the leak of sensitive information and the loss of funds, often with no recourse. An industry has started to form around smart contract "auditing," but standards and in some cases legal accountabilities are not yet established. DeFi projects regularly use bug bounties and appeals to open source software principles (such as using template code and technical standards such as ERC-20) to further mitigate cybersecurity risk, but hacks remain common.

---

[26] *See* https://www.cnbc.com/2021/11/19/over-10-billion-lost-to-defi-scams-and-thefts-in-2021.html; https://www.elliptic.co/resources/defi-risk-regulation-and-the-rise-of-decrime; Chainalysis, "The 2022 Crypto Crime Report; Original data and research into cryptocurrency-based crime," February 2022 ("Chainalysis Report"), available at: https://go.chainalysis.com/2022-Crypto-Crime-Report.html. According to the Chainalysis Report, "[i]n 2020, just under $162 million worth of cryptocurrency was stolen from DeFi platforms, which was 31% of the year's total amount stolen. That alone represented a 335% increase over the total stolen from DeFi platforms in 2019. In 2021, that figure rose another 1,330%. In other words, as DeFi has continued to grow, so too has its issue with stolen funds. … [M]ost instances of theft from DeFi protocols can be traced back to errors in the smart contract code governing those protocols, which hackers exploit to steal funds, similar to the errors that allow rug pulls to occur." Id at 6.

NASCENT STAGE OF DEVELOPMENT

Blockchain technology and DeFi are nascent and developing. Although innovations may hold promise for certain applications, at present, DeFi naturally faces several early-stage challenges that may not be readily apparent to retail users.

Comprehensibility – DeFi products and systems lack the traditional interfaces with which investors are accustomed to interacting. DeFi investor interfaces and other channels of engagement may be difficult to understand and use, including those relating to the opening and funding of accounts, terms and conditions of use, transacting, monitoring, and closing accounts.

Scalability – DeFi products and services have been limited in their ability to scale to process more transactions without compromising function and user experience. As currently operating, users can experience slow transaction speeds and low throughput with high transaction costs and gas fees.

Supportability – Certain DeFi products and systems have not been maintained and supported sufficiently to ensure sustainability.

Reliability – DeFi products and services shift trust from intermediaries to protocols and code, which can be subject to error, vulnerability, and attack. If compromised, this can result in errors in transactions, lack of dispute mechanisms and lack of redress or remedy.

GOVERNANCE RISKS

Though many DeFi applications purport to be decentralized, there are DeFi protocols that retain the discretion for governance teams or other entities, such as select professional investors or venture capitalists, to exercise voting rights, have a say on governance issues, or retain some ultimate control, including terminating the protocol. A set of unique risks arise relating to governance over DeFi protocols and smart contracts. Two primary areas where these risks arise is in the control of administrative keys and the functioning of protocol governance structures. If there is no disclosure of material information about these governance arrangements to potential investors, they are deprived of information that could have a substantial impact on the performance of the product or system.

Retention by an entity or individual of an administrative key permits the disabling or alteration of a smart contract or protocol. This may present advantages for maintaining the code. However, the retention of an administrative key also poses risks. In some instances, the holder of the administrative key has unilateral control of users' funds held in a smart contract or protocol. Risks arise, such as key loss or theft, insider theft of crypto-assets held in the smart contract or protocol, and other cybersecurity concerns (such as ransom or hacks from outside parties). There is also the risk that the smart contract or protocol will be disabled or altered unexpectedly by the administrator.

Certain DeFi products or systems claim to be governed by governance tokens. While in theory governance tokens are intended to grant decision making regarding the protocol and smart contracts to a dispersed community of users, in many products and systems there is highly concentrated voting control and governance token ownership. See "Governance Tokens."

Also, there could be misalignment of incentives as between holders of governance tokens and holders of other tokens issued by the protocol, which ultimately present risks to the protocol. Governance token holders, although having the ability to vote on certain aspects of the protocol, may be incentivized to sell the token on centralized crypto-asset trading platforms for short-term profit taking while holders of other tokens issued by the protocol may be looking for more long-term use of the protocol. Further, a governance

token holder may only hold the governance token through a vote and thereby influence the protocol without any interest in the long-term prospects of the protocol. Further, if governance token holders have access to information that other users of the protocol do not, risks relating to information asymmetries, such as non-disclosure of material information to investors and insider trading, also arise.

Certain activities can permit actors to gain a large influence over a protocol. For example, some protocols allow for the delegation of voting rights to others, who could acquire large concentrations of voting rights. Moreover, in many cases governance token holders transfer or delegate their voting rights to concentrated groups or entities, while retaining the economic benefits. This bifurcation may undercut assertions of decentralization. Information about these voting transfers and delegations may not be available to the market and purchasers of governance tokens in secondary market trades. In a technique known as a "Sybil attack," certain individuals with advanced knowledge of a governance token "airdrop" by a protocol can generated multiple pseudonymous addresses to obtain control over a concentration of airdropped tokens and gain a large influence over a system.

SPILL-OVER OF RISKS TO CENTRALIZED/TRADITIONAL MARKETS

Centralized Crypto-asset Trading Platforms

The ability of retail investors to participate in DeFi has been enhanced by the participation of centralized crypto-asset trading platforms as a pathway into DeFi protocols and smart contracts. For example, many of these centralized crypto-asset trading platforms serve as interfaces for DeFi protocols. Users of centralized crypto-asset trading platforms often can "loan" their crypto-assets to the platform for a return. Similarly, these platforms may be engaging in lending activities of crypto-assets enabling participation, including on a highly leveraged basis, in DeFi products. The platform may also be using those crypto-assets in speculative DeFi trading, lending and borrowing protocols. These platforms often offer highly leveraged exposures, including through the use of stablecoins. Further, users may also purchase tokens generated by DeFi platforms, including governance tokens on or through these platforms, and similarly, through trading activities, may use centralized crypto-asset trading platforms to realize on DeFi investments. Thus, through these centralized crypto-asset trading platforms, retail investors may be subject to the aforementioned risks of DeFi. Centralized crypto-asset trading platforms are at the heart of crypto-asset trading and, as a result, DeFi. Risks of these crypto-asset trading platforms could directly affect DeFi. As centralized crypto-asset trading platforms offer a full range of services, including trading, lending and borrowing, and custody of crypto-assets, they are subject to significant risks including potential conflicts of interest, economic exposures, and concentration risks relating to crypto-asset control through custody, leverage, and trading risks.

Traditional Financial Institutions

To date, the interconnectedness of DeFi to traditional financial institutions may be limited, but it is growing. Banks have made loans and investments into DeFi projects. They may hold assets of a stablecoin's reserve. They may have banking relationships with centralized crypto-asset trading platforms through which individuals can on-ramp into DeFi. Private funds may also be investing into DeFi projects and may be engaging in DeFi activities. To the extent traditional financial institutions are becoming involved in DeFi projects or transactions, or activities that support stablecoin business, this activity may present risks to the traditional businesses and their operations which, if they grow, may become material to their business operations. The use of DeFi to create derivatives or synthetics of existing equity or debt also may pose risks to traditional markets for those equity and debt instruments.

CONCLUSION

This report is based on currently available information as of the date of publication. The purpose of this report is to provide a general understanding of DeFi, including some areas of potential regulatory concern. The descriptions contained in this report are meant to describe typical features of DeFi protocols currently available. Actual features of any particular DeFi protocol in existence may vary. This report acknowledges that DeFi is a continuously evolving area and IOSCO will continue to examine this area and its implications for market regulators.

IOSCO welcomes input from the public, including crypto-asset market and DeFi participants and from any other interested party, on the presentation of information in this report, as well as on any other crypto-asset or DeFi related matter.